TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

HEARINGS

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

NINETY-SEVENTH CONGRESS

SECOND SESSION

MAY 4, 5, 6, 11, AND 12, 1982

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

95-929 O WASHINGTON : 1982

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

S401-60

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, JR., Delaware, *Chairman*

CHARLES H. PERCY, Illinois
TED STEVENS, Alaska
CHARLES McC. MATHIAS, JR., Maryland
JOHN C. DANFORTH, Missouri
WILLIAM S. COHEN, Maine
DAVID DURENBERGER, Minnesota
MACK MATTINGLY, Georgia
WARREN B. RUDMAN, New Hampshire
HARRISON H. SCHMITT, New Mexico

THOMAS F. EAGLETON, Missouri
HENRY M. JACKSON, Washington
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio
JIM SASSER, Tennessee
DAVID PRYOR, Arkansas
CARL LEVIN, Michigan

JOAN M. MCENTEE, *Staff Director*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

WILLIAM V. ROTH, JR., Delaware, *Chairman*
WARREN B. RUDMAN, New Hampshire, *Vice Chairman*

CHARLES H. PERCY, Illinois
CHARLES McC. MATHIAS, JR., Maryland
JOHN C. DANFORTH, Missouri
WILLIAM S. COHEN, Maine

SAM NUNN, Georgia
HENRY M. JACKSON, Washington
LAWTON CHILES, Florida
JOHN GLENN, Ohio
JIM SASSER, Tennessee

S. CASS WEILAND, *Chief Counsel*
MICHAEL C. EBERHARDT, *Deputy Chief Counsel*
ELEANORE J. HILL, *Chief Counsel to the Minority*
KATHERINE BIDDEN, *Chief Clerk*

CONTENTS

Testimony of— Page

Arkov, Joseph, (assumed name for former Soviet engineer) 27
Asselin, Fred, staff investigator, Permanent Subcommittee on Investigations 82
Baker, Dr. Lara H., Jr., assistant office leader, International Technology Office, Los Alamos National Laboratory, University of California 54
Bell, William H., prisoner; accompanied by Robert L. Kirste, attorney 37
Brady, J. Lawrence, Assistant Secretary of Commerce for Trade Administration, Department of Commerce 262
Bryant, Clyde, Chief, Support Services Division, Office of Munitions Control, State Department 156
Bryen, Dr. Stephen D., Deputy Assistant Secretary of Defense, International Economics, Trade and Security Policy, Department of Defense 249
Buckley, James L., Under Secretary of State for Security Assistance, Science and Technology, Department of State 156
Corcoran, George G., Assistance Commissioner (Border Operations), U.S. Customs Service 193
Fry, Glenn W., staff investigator, Permanent Subcommittee on Investigations 74, 82
Greenberg, Theodore, assistant U.S. attorney, Eastern District of Virginia 129
Inman, Adm. Bobby R., Deputy Director, Central Intelligence Agency 235
Johnston, Ernest, Deputy Assistant Secretary of State for Economic and Business Affairs 156
Kapper, Dr. Frank, Director of Military Technology Sharing 218
Lecht, Charles, former president and chairman of the board, Advanced Computer Techniques Corp 229
Lomacky, Dr. Oles, Director of the Office of Technology Trade 218
Lorenzo, Michael, Deputy Under Secretary of Defense, International Programs and Technology, Department of Defense 218
Maguire, John, president, Software AG of North America, Inc 121
Marshall, John D., businessman, Santa Clara, California 71
Martin, John L., Criminal Division, U.S. Department of Justice 129
O'Brien, Patrick, Director, General Investigations, U.S. Customs Service 193
O'Malley, Edward J., Assistant Director, Intelligence Division, Federal Bureau of Investigation 168
Southard, Douglas, deputy district attorney, County of Santa Clara, California 143
Van Cook, Arthur, Director of Information Security, Department of Defense, and chairman, National Disclosure Policy Committee 181
Von Raab, William, Commissioner, U.S. Customs Service 193
Vorona, Dr. Jack, Director, Scientific and Technical Information, Defense Intelligence Agency, Department of Defense 110

EXHIBITS

	Introduced on page	Appears on page
1. Assessment of the technology transfer problem regarding diversions to the Soviet Union	6	7
2. Public Law 96-72, 96th Congress, September 29, 1979, Export Administration Act of 1979	97	*
3. Testimony of William V. Skidmore, Director, Office of Export Administration, Department of Commerce, before the Subcommittee on International Economic Policy and Trade of the House Committee on Foreign Affairs, March 26, April 14, 28, and May 13, 1981, Export Administration Amendments Act of 1981	97	*
4. Export Administration report to Congress, October 1978–March 1979, issued by the Industry and Trade Administration, Department of Commerce; Export Administration report to Congress, April 1979–September 1979; issued by the Industry and Trade Administration, Department of Commerce; Export Administration annual report fiscal year 1980, issued February 1981, by International Trade Administration, Department of Commerce; Export Administration annual report fiscal year 1981, issued February 1982, by the International Trade Administration, Department of Commerce	97	*
5. Memorandum from Sharon R. Connelly, Director, Compliance Division, to William V. Skidmore, Director, Office of Export Administration, on "Administrative Enforcement Activity in the Compliance Division in Fiscal Year 1981 Compared to Prior Years," October 5, 1981	97	*
6. 198L summary of work of Facilitations Branch of Compliance Division	97	*
7. S. 206, 96th Congress, Office of Strategic Trade Act of 1980, introduced on April 24, 1980, by Senator Garn; floor remarks of Senator Garn; and May 8, 1980, "Dear Colleague letter" regarding legislation	97	*
8. Letter to the Speaker of the House and the President of the Senate transmitting a report from President Carter, "Shipments of Agricultural Commodities to the Soviet Union," January 2, 1980	97	*
9. Report by the Comptroller General of the United States, "Lessons To Be Learned From Offsetting The Impact Of The Soviet Grain Sales Suspension," July 27, 1981, U.S. General Accounting Office	97	*
10. Memorandum from William Green, Deputy Assistant Commissioner for Border Operations, Customs Service, to Robert L. Kench, Associate Deputy Attorney General and Chairman of Inter-agency Working Group on Export Control, October 20, 1980	97	97–99
11. Los Angeles Times article, "4 Accused of Exports for Soviet Bloc Nations," August 20, 1981, p. 1	97	*
12. Indictment, *United States* v. *Werner J. Bruchhausen, Anatoli Tony Maluta, Sabina Dorn Tittel; and Dietmar Ulrichshofer;* U.S. District Court for the Central District of California	97	*
13. Information, *United States* v. *Anatoli Tony Maluta*, U.S. District Court, Central District of California	97	*
14. Stipulation of Facts and Exhibits re: trial of Anatoli Tony Maluta, *United States* v. *Anatoli Tony Maluta*, October 27, 1981, U.S. District Court, Central District of California	97	*
15. Memorandum re: Sentencing; Exhibits; Declaration of Theodore W. Wu, *United States* v. *Anatoli T. Maluta and Sabina D. Tittel*, U.S. District Court, Central District of California	97	*
16. Commerce Department press release of April 3, 1981, announcing that the Department had denied all U.S. export privileges to Anatoli Maluta, Sabina Dorn Tittel; and Werner J. Bruchhausen and three firms associated with them; and 16 more Commerce Department press releases relating to actions taken in connection with alleged violations of export laws and regulations in 1980 and 1981	97	*

EXHIBITS—Continued

	Introduced on page	Appears on page
17. Commerce Department press release of September 8, 1980 in which Commerce Secretary Philip M. Klutznick and Attorney General Benjamin Civiletti announced that President Carter had directed formation of an interagency working group chaired by the Justice Department "to examine ways to improve compliance with the export control laws."	97	*
18. Commerce Department press release of January 11, 1980, announcing, "Commerce Secretary Denies $1 Billion Plus In Export Licenses for Soviet Union"	97	*
19. Volumes 4, 7, 8, and 11, reporter's transcript, *U.S.* v. *Spawr, Optical Research, Inc., Walter J. Spawr, Frances Spawr*, November 13, 24 and 25 and December 3, 1980, U.S. District Court, Central District of California	97	*
20. Qualification standards and position discriptions on GS-1811 Federal criminal investigation issued by the Office of Personnel Management	97	*
21. Speech by Senator Henry M. Jackson on "Technology Transfer Policy—The High Stakes," in Senate, February 11, 1982	97	*
22. Congressional Research Service report entitled, "Foreign Espionage and U.S. Technology," prepared at the request of the Senate Permanent Subcommittee on Investigations by Mark M. Lowenthal, Foreign Affairs and National Defense Division; and George Holliday and Lawrence Evans, both of the Economics Division; August 12, 1980	97	*
23. Statements of Lawrence J. Brady, Assistant Secretary of Commerce for Trade Administration, before House Subcommittees on Science, Research and Technology and on Investigation and Oversight, March 29, 1982; and before Senate Subcommittee on International Finance and Monetary Affairs, April 14, 1982	97	*
24. Commerce Department April 1982 biography of William V. Skidmore, Director, Office of Anti-Boycott Compliance; and Acting Director, Compliance Division	97	*
25. New York Times editorial, "Smothered By A Security Blanket," April 12, 1982	97	*
26. Letter from Frank Carlucci, Deputy Secretary of Defense to William D. Carey, Executive Officer and Publisher of *Science* magazine, printed under the heading, "Scientific Exchanges and U.S. National Security," in January 8, 1982 issue	97	*
27. *Soviet Military Power*, Department of Defense publication	97	*
28. Letters from Chairman Roth and Senator Nunn to Commerce and Treasury Departments requesting specific information on export controls, September 21, 1981; April 14 and 16, 1982	97	*
29. Sworn affidavit of John Rennish	277	278
30. Sworn affidavit of Michael Dolphin	277	283
31. Sworn statement of Charles McLeod	277	287
32. Freedom of Information Act (S. 1751), and a section by section analysis, submitted by Mr. Van Cook	191	*
33. Briefing on duel-use technology prepared by Col. Kenneth Evans, U.S. Army	296	*
34. Statement prepared for the subcommittee by the American Society for Industrial Security	296	*
35. Prepared statement submitted to the subcommittee by the Computer & Business Equipment Manufacturers Association	296	*
36. Prepared statement submitted by the Electronics Industries Association	296	*
37. Prepared statement submitted by the Scientific Apparatus Makers Association	296	*
38. Court exhibits, documents and related material	296	*

APPENDIX

Asselin, Fred, investigator, Permanent Subcommittee on Investigations. Prepared statement, including a summary written by Mr. Asselin on the CTC case ..... Page 366
Baker, Dr. Lara H., Jr., assistant office leader, Los Alamos National Laboratory. "Talking Notes" of Dr. Baker; his submitted résumé; a memorandum dated April 16, 1982, which contains Dr. Baker's response to the Customs Bureau regarding the CTC case 338
Brady, Lawrence, Assistant Secretary of Commerce for Trade Administration, Department of Commerce, prepared statement 596
Bryen, Dr. Stephen D., Deputy Assistant Secretary of Defense, International Economics, Trade and Security Policy, Department of Defense, prepared statement 583
Buckley, James L., Under Secretary of State for Security Assistance, Science and Technology, Department of State, statement with related material and attachments 533
Cohen, Senator William S., prepared statement 313
Fry, Glenn W., staff investigator, Permanent Subcommittee on Investigations, prepared statement 426
Greenberg, Theodore, assistant U.S. attorney, Eastern District of Virginia, prepared statement 432
Inman, Adm. Robert R., Deputy Director, Central Intelligence Agency, prepared statement 577
Jackson, Senator Henry M., prepared statement; letters to President Reagan dated March 8, 1982, and November 14, 1980, relating to the subcommittee's investigation; a newsletter by Senator Jackson dated February 11, 1982, on the subject matter 315
Lecht, Charles, former president and chairman of the board, Advanced Computer Techniques Corp., statement 570
Lorenzo, Michael, Deputy Under Secretary of Defense, International Programs and Technology, Department of Defense, prepared statement; copy of speech dated March 11, 1982, to the George Washington University on Military Transfer Technology 552
Southard, Douglas, deputy district attorney, county of Santa Clara, Calif., prepared statement 475
U.S. Department of Commerce: Inspector General's Report of Inspection of the Export Administration's Compliance Division 606
Wu, Theodore Wai, assistant U.S. attorney, Criminal Division, Central District of California, prepared statement (did not testify) 510

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

TUESDAY, MAY 4, 1982

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met at 10:10 a.m., pursuant to call, in room 3302, Dirksen Senate Office Building, under authority of Senate Resolution 361, dated March 5, 1980, Hon. William V. Roth, Jr., presiding.

Members of the subcommittee present: Senator William V. Roth, Jr., Republican, Delaware; Senator William S. Cohen, Republican, Maine; Senator Warren B. Rudman, Republican, New Hampshire; Senator Henry M. Jackson, Democrat, Washington; Senator Lawton Chiles, Democrat, Florida; and Senator Sam Nunn, Democrat, Georgia.

Members of the professional staff present: S. Cass Weiland, chief counsel; Michael C. Eberhardt, deputy chief counsel; Katherine Bidden, chief clerk; Eleanore J. Hill, chief counsel to the minority; Gregory Baldwin, assistant counsel to the minority; Jack Key, Glenn Fry and Fred Asselin, staff investigators to the minority; and Kathleen Dias, executive secretary to the minority chief counsel.

[Members of the subcommittee present at convening: Senators Roth, Nunn, Jackson, Cohen, Chiles, and Rudman.]

Chairman ROTH. Today the Permanent Subcommittee on Investigations opens 5 days of in-depth hearings into the loss of U.S. technology to the Soviet Bloc countries. At the very outset, I want to congratulate you, Senator Nunn, and your staff for the excellent work in putting together this series of very important hearings.

As chairman I am, of course, cognizant of the accomplishments of the subcommittee under you, Senator Jackson, on this subject during the mid-seventies and fully support the type of investigation that has led to the presentation of evidence we will begin to hear today.

The issues that will be addressed here in the next two weeks are of great concern to me and should be fully understood so that the American people can better appreciate the extent to which our sensitive technology is finding its way into the Soviet Union and its bloc nations. There is no question that the Soviets have undertaken a massive, well-financed, expertly coordinated program to systematically acquire as much as our high technology as they can steal, purchase through middlemen or otherwise appropriate. And all because they are unable to produce that technology themselves. So they are left to copy ours and use it, not to make life more comfortable for their citizens, but to advance their numerous weapons systems and overall military capabilities.

It is of the utmost importance, therefore, that our Federal law enforcement and intelligence agencies work closely with representatives of private industry in identifying and protecting those sensitive items and processes which are the targets of Soviet operatives. But in so doing we must remain committed to our great tradition of American competition in the world marketplace. A balance must be struck between our legitimate effort to curtail any assistance to Soviet military buildup on one hand, and our promotion of free enterprise in the world market on the other hand.

This is no easy balance to strike, but hopefully our hearings will identify the issues that we must address if we are to succeed in both of these goals.

One key factor to success will be the assurance that our Federal intelligence agencies are interacting with Federal enforcement agencies to identify those types of sensitive technology most desired by the Soviet Union. This is where our emphasis on control must lie, not with items of little or no priority to the Soviets.

Furthermore, much of the technology developed here in the United States is also being developed by other Western nations for sale overseas, while our allies readily trade away sensitive information to the Soviet bloc. We must, therefore, work together with our friendly neighbors to establish carefully conceived important programs aimed at specific types of technology.

Clearly, effectiveness depends on multilateral enforcement. Where that cooperation is lacking, we must build incentives to achieve them; and where there are presently treaties in effect, we must insure that there is a sufficient commitment to their vigorous enforcement.

I look forward to the next several days of hearings and again want to thank Senator Nunn for his efforts.

Senator Nunn.

OPENING STATEMENT OF SENATOR NUNN

Senator NUNN. Thank you very much, Mr. Chairman. I want to thank you, Mr. Chairman, and the entire majority staff for your splendid cooperation during the course of this investigation and in plans for these hearings. We have had the minority staff working on this problem now for about 15 months and during the entire course of that investigation, we have had splendid and total cooperation from the majority, which we appreciate very much.

The subcommittee today begins its evaluation of the effectiveness of the executive branch in enforcing export controls, particularly with regard to transfer of technology to the Soviet Union and other Warsaw Pact nations.

The subcommittee has received information indicating that the executive branch has devoted insufficient attention and resources to enforcing export controls on high technology. When I say the executive branch during the course of these hearings, I want to make it absolutely plain I am talking about the executive branch that exists now and the one that existed before. This is a bipartisan thing and this is not aimed at any particular administration. This problem transcends any administration or any leadership.

For this Nation to neglect export controls is to assist the Soviets in carrying out their global designs. They have stated often their goal to achieve superiority in science and technology. We are mistaken not to take them at their word.

Since the end of World War II, the Soviets have made great strides in building their military prowess. Our own security analysts admit to the increased level of deployed Soviet military technology. We have relied on our technological superiority to offset the Soviet Union's commitment to have more of everything, more men in arms, more armor, more aircraft, more ships at sea. However, the United States' advantage in basic military technology is being challenged. Today the Soviets have more of most things military. They are also closing the gap technologically in many fields.

In modernizing their military capabilities, the Soviets first had to modernize their industry. In that pursuit, they relied to an important extent on technology from the United States.

According to American defense analysts, the United States has been the source of much of the Soviet Union's electronic and computer technology and advanced manufacturing capability. Some of this expertise was given or sold to the Soviets willingly. Some of it the Soviets obtained illegally.

The Soviets have come to view our technology as their technology, to be obtained whenever they need it. As a consequence, we are in the position of supporting our own costly national security apparatus, and indirectly helping them to build theirs.

Since 1970, the Western democracies and Japan have supplied the Soviet industrial sector with millions of dollars' worth of efficient machine tools, chemical plants, precision instrumentation, and associated technologies. Western goods and technologies have played a major role in the modernization and expansion of Soviet industry. The use of the technology embodied in the Western equipment has enabled the Soviet Union and the Warsaw Pact countries to achieve industrial growth at a faster rate than would have been possible with their own resources.

Our purpose in these hearings is to identify the principal vehicles the Soviets use to obtain high technology from the United States and to examine our ability to halt the technological drain.

Imagine for a moment an office in the Kremlin where senior Soviet officials decide what kind of technology they need from us and then devise their efforts to obtain it.

The Kremlin office, a composite of several Soviet departments, responds to the law of supply and demand. The demand is reflected in the needs of military and industrial planners. The planners give the "Technology Transfer Office" a shopping list of desired high technology components and knowledge. The composite Soviet officers in charge of obtaining American technology surveys his resources.

Generally speaking, he has seven basic approaches he can utilize.

First, there are the KGB and the GRU, the spy organizations which practice traditional hand-in-the-safe information gathering crafts. Their tactics range from bribery to blackmail to extortion.

Second, the Soviets rely on information published by the U.S. Government and made available by Federal agencies.

The subcommittee will examine information indicating that too much data about our military programs may be being made public. The Soviets draw heavily on the Government's public documents.

Third, the Soviets promptly translate U.S. technical journals and distribute them among their scientists and engineers. There is nothing the United States can do to stop that. However, the subcommittee will examine the procedures with which the Government decides to make heretofore sensitive information available.

Fourth, the Soviets promote information exchanges as ways to establish improved relations between the two countries. But information exchanges may serve the Soviets in other ways.

The subcommittee will examine information indicating that the Soviets exploited such exchanges for their own benefit and the United States gives up more information than it receives.

Similarly, the subcommittee will examine information indicating that the Soviets exploit the so-called student exchange program with the United States. Sources indicate that the Soviets send to American universities established scientists to learn at our Nation's centers of high technology studies. In return, the United States usually is represented by college-age students whose interests are literature, art, or history.

Fifth, the Soviets and their surrogates form marketing and manufacturing companies in this country which serve two purposes for them. They buy high technology and munitions for illicit export to the Soviet Union. Second, they use their facilities in the United States as havens for spies. Both these techniques will be examined in the hearings.

Sixth, the Soviets turn to agreements in which American companies and consortiums build factories in the U.S.S.R.

Seventh, the Soviets employ business intermediaries in the United States and foreign countries. Using false shipping documentation and other illegal practices, business intermediaries buy high technology components and knowledge and send them to the Soviet sphere.

It is important to note that in these hearings we have special interest in so-called "dual-use" technology; that is to say, technology developed or manufactured in this country primarily by the private sector and primarily for commercial purposes. It is termed "dual use" because in the hands of the Soviets or another adversary, the technology can have military applications that can be used against the United States.

Such technology cannot be exported legally without a validated license from the U.S. Department of Commerce.

The Commerce Department's Office of Export Administration, known as OEA, has the responsibility of enforcing export controls under the Export Administration Act. Investigation of alleged violations is conducted by OEA's Compliance Division.

Our preliminary investigation has raised serious questions about the ability of the Commerce Department to enforce effectively those U.S. export laws governing technology transfer.

The subcommittee will examine carefully allegations that from as early as 1963, the Compliance Division has been undermanned and undertrained as a law enforcement organization. By contrast, the

Soviets have become increasingly adept in their ability to secure our high technology.

In that context, the subcommittee intends to examine the mechanisms both on the statutory and agency levels, which the United States has developed to implement a strong policy aimed at halting the technology drain. We will weigh the testimony and evidence to determine what can be done to improve the ability of the executive branch to enforce export controls.

The transfer of technology to the Soviet Union is one of our most important national security problems. It is a national security issue that deserves the most responsible and thoughtful scrutiny.

I want to stress that a primary consideration of this subcommittee's inquiry is to enable the private sector of our economy the opportunity to export with as few regulations and controls as possible. One point has come through clearly in the preliminary investigation. It is that the way high technology export controls are administered now, too many items are controlled, and because the Government tries to control too many commodities, it fails to keep track of those products the Soviets desire most. So, in the effort to broaden and have a comprehensive list, we end up uncovering more and more. An improved system of export regulations would focus on those high technology items the Soviets must have.

This so-called Soviet shopping list, based on sound intelligence estimates, will enable our Government to safeguard the most critical aspect of our technology and we hope also eliminate some of the regulations and controls that cause American businessmen to complain bitterly about wasteful Government redtape.

The result, if it can be implemented, will be an improved enforcement effort and an improved balance of trade.

What Chairman Roth pointed out at the beginning of these hearings is very important. It is extremely difficult for an open society to have restrictions on technology transfer. We have to arrive at a balance. The openness of our society is one of the strengths that we have in developing new technologies. It is also apparent that the Soviet Union has a distinct advantage in developing technology because they have a closed society. So we certainly have to keep that balance in mind.

Mr. Chairman, I think it is appropriate at this point to express my respect and admiration for our colleague on this subcommittee, Senator Jackson, who was one of the first to speak out on the importance of the technology transfer issue.

As early as 1974, Senator Jackson, then chairman of this subcommittee, convened hearings on this subject and helped focus needed attention on a subject that was much in need of congressional oversight.

Senator Jackson's work in this area provided an accurate and comprehensive foundation for the investigation we launch today. So I want to commend you, Senator Jackson, for your longstanding leadership in this field and as I have said so many times in the past, you know and understand national security matters very well—with one or two possible exceptions that we can discuss later on.

In addition, Mr. Chairman, I want to point out that in this preliminary investigation, the minority staff has coordinated its efforts with the staff of the Senate Select Committee on Intelligence. We have re-

ceived complete cooperation and assistance from select committee staff and I myself have benefited greatly from the generous guidance of my distinguished colleagues, Senator Goldwater, the chairman of the select committee, and Senator Moynihan, the vice chairman.

Our staff has provided thorough briefings to the select committee staff and I have kept members of the select committee advised of our progress as well.

In concluding my opening statement, Mr. Chairman, I request that you order printed in the record at this point an assessment of the technology transfer problem regarding diversions to the Soviet Union. The assessment prepared by national security specialists in the executive branch was made available to me through established procedures.

Chairman ROTH. Without objection, it will be so printed.

[The document referred to was marked "Exhibit No. 1," for reference and follows:]

EXHIBIT NO. 1

Soviet Acquisition of Western Technology

Contents

	Page
Introduction	1
Soviet Acquisition of Western Technology: A National-Level Program	1
Soviet Mechanisms for Acquiring Western Technology	2
Soviet Acquisitions and Benefits	5
Outlook for the 1980s	11

Appendix

Projected Soviet Technological Needs and Acquisition Targets Through the 1980s	13

Soviet Acquisition of Western Technology

Introduction

The United States and its Allies traditionally have relied on the technological superiority of their weapons to preserve a credible counterforce to the quantitative superiority of the Warsaw Pact. But that technical superiority is eroding as the Soviet Union and its Allies introduce more and more sophisticated weaponry—weapons that all too often are manufactured with the direct help of Western technology.[1] Stopping the Soviets' extensive acquisition of military-related Western technology—in ways that are both effective and appropriate in our open society—is one of the most complex and urgent issues facing the Free World today.

This report describes the Soviet program to acquire US and Western technology, the acquisition mechanisms used, the spectrum of Western acquisitions that have contributed to Soviet military might, the projected Soviet priority needs for Western technology, and the problems of effectively stemming the transfer of Western technology that could someday find application in weapons used to threaten the West.

Soviet Acquisition of Western Technology: A National-Level Program

Since at least the 1930s, the Soviet Union has devoted vast amounts of its financial and manpower resources to the acquisition of Western technology that would enhance its military power and improve the efficiency of its military manufacturing technology. Today this Soviet effort is massive, well planned, and well managed—a national-level program approved at the highest party and governmental levels.

[1] While there are numerous interpretations of "technology" for weapons, it is defined in this report as the application of scientific knowledge, technical information, know-how, critical materials, keystone manufacturing and test equipment, and end products which are essential to the research and development as well as the series manufacture of modern high-quality weapons and military equipment. Western technology is defined as that technology developed by the Free World.

This program accords top priority to the military and military-related industry, and major attention is also given to the civilian sectors of Soviet industry that support military production.

The Soviets and their Warsaw Pact allies have obtained vast amounts of militarily significant Western technology and equipment through legal and illegal means. They have succeeded in acquiring the most advanced Western technology by using, in part, their scientific and technological agreements with the West to facilitate access to the new technologies that are emerging from the Free World's applied scientific research efforts; by spending their scarce hard currency to illegally purchase controlled equipment, as well as to legally purchase uncontrolled advanced Western technologies having military industrial applications; and by tasking their intelligence services to acquire illegally those US and Western technologies that are classified and export controlled.

The Soviets have been very successful in acquiring Western technology by blending acquisitions legally and illegally acquired by different government organizations. The Soviet intelligence services—the Soviet Committee for State Security (KGB) and the Chief Intelligence Directorate of the Soviet General Staff (GRU)—have the primary responsibility for collecting Western classified, export-controlled, and proprietary technology, using both clandestine and overt collection methods. They in turn make extensive use of many of the East European Intelligence Services (see inset, p. 2); for their efforts in acquiring Western technology, these countries are paid in part with Soviet military equipment and weapons.

Clandestine acquisition of the West's most advanced military-related equipment and know-how by the KGB and GRU is a major and growing problem.

East European Intelligence Services Acquire Technologies for the Soviet Union

In the late 1970s a former East European intelligence officer revealed organizational and targeting details related to Soviet-directed acquisitions of Western technology by East European intelligence services, particularly military-industrial manufacturing-related technologies that were given the highest priority for collection by at least one East European intelligence service. Many technologies were acquired through dummy firms established in Western Europe that were successful in securing some of the most advanced technologies in the West, including computer, microelectronic, nuclear, and chemical technologies.

In microelectronics, for example, many US firms were targeted through their affiliates in Western Europe; scientists, technicians, and commercial representatives also were successfully recruited to provide information during their trips to Europe. Although most of the military and defense-industrial information acquired by East European intelligence services went to the Soviets, much of it was used by the East Europeans themselves to benefit their military and civilian industries. The computer, microelectronic, and photographic areas were priority targets. The East European countries benefited considerably from microelectronic acquisitions, and could not have achieved the present level of development in their computer industry without illegal acquisitions of Western technology.

These intelligence organizations have been so successful at acquiring Western technology that the manpower levels they allocate to this effort have increased significantly since the 1970s to the point where there are now several thousand technology collection officers at work. These personnel, under various covers ranging from diplomats to journalists to trade officials, are assigned throughout the world.

Soviet foreign trade organizations, or enterprises, although quasi-independent entities, are partially subordinated to the Ministry of Foreign Trade, and their activities are closely coordinated by this Ministry. They have major responsibilities for both legal and illegal acquisitions and purchases; they work closely with the KGB and GRU in arranging trade diversions. East European trade companies assist them in clandestine and illegal acquisition operations

Official Soviet and East European science and technology (S&T) organizations also play a major role in both open and clandestine acquisition of Western technology. The Soviet State Committee for Science and Technology (GKNT) is the key player in arranging government-to-government science and technology agreements to facilitate access to and the acquisition of established as well as new technologies, including those just emerging from Western universities, laboratories, and high-technology firms. It is the GKNT that oversees the allocation of scarce Soviet hard currency for the legal purchase by various Soviet organizations of selected Western technology for Soviet military purposes. If the GKNT is unable to acquire the necessary technology by open or legal means, it tasks Soviet intelligence to clandestinely acquire the technology.

It is the well-organized and well-coordinated use of all these organizations that has made the Soviet program to acquire Western technology so successful. As a result, the Soviets have acquired militarily significant technologies and critically important industrial Western technologies that have benefited every major Soviet industry engaged in the research, development, and production of weapon systems.

Soviet Mechanisms for Acquiring Western Technology

Soviet acquisition mechanisms include: *legal means* through open literature, through legal trade channels, and through student scientific and technological exchanges and conferences; *illegal means* through trade channels that evade US and Western (i.e. CoCom)[2] export controls, including acquisitions by their intelligence services through recruited agents and industrial

[2] The Coordinating Committee (CoCom) was established in 1949 to serve as the forum for Western efforts to develop a system of strategic export controls. It is composed of the United States, the United Kingdom, Turkey, Portugal, Norway, the Netherlands, Luxembourg, Japan, Italy, Greece, France, the Federal Republic of Germany, Denmark, Canada, and Belgium.

espionage. While a large volume of technology is acquired by nonintelligence personnel, the overwhelming majority of what the United States considers to be militarily significant technology acquired by and for the Soviets was obtained by the Soviet intelligence services and their surrogates among the East European intelligence services. However, legal acquisitions by other Soviet organizations are important since it is often the combination of legally and illegally acquired technologies that gives the Soviets the complete military or industrial capability they need.

Because of the priority accorded to the military over the civilian sectors of the Soviet economy, Western dual-use technology—i.e., technology with both military and civilian applications—almost always finds its first into military industries, and subsequently the civilian sectors of industries that support military production. Thus, Soviet assurances that legally purchased dual-use technology will be used solely for civilian applications can seldom be accepted at face value.

Legal acquisitions generally have their greatest impact on the Soviets' broad industrial base, and thus affect military technology on a relatively long-term basis. The Soviet Kama Truck Plant, for example, was built over some seven years with massive imports of more than $1.5 billion worth of US and West European automotive production equipment and technology. Large numbers of military-specification trucks produced there in 1981 are now being used by Soviet forces in Afghanistan and by Soviet military units in Eastern Europe opposite NATO forces. Similarly, large Soviet purchases of printed circuit board technology and numerically controlled machine tools from the West already have benefited military manufacturing sectors.

The Soviets give priority to those purchases that meet the direct needs of the Soviet military-industrial complex by paying for them in hard currency. Over the past 10 years, the Soviets legally and illegally purchased large quantities of Western high-technology microelectronics equipment that has enabled them to build their own military microelectronics industry in a short time. This acquired capability in microelectronics is the critical basis for the present wide-ranging enhancements of Soviet military systems and for their continuing sophistication.

Acquisitions through illegal trade channels often have both industrial and military applications, and thus are important in the near term. Illegal acquisitions of technology fall into two general categories, both of which are extremely difficult to detect and monitor. One is the diversion of controlled technology from legitimate trade channels to proscribed destinations. This is done through US and foreign firms that are willing to engage in profitable impropriety; through agents-in-place in US or foreign firms or foreign subsidiaries of US firms; through Soviet- and East European—owned firms locally chartered in the West; and through foreign purchasing agents (including arms dealers). For instance, to evade the US embargo on microelectronic technology exports to the Soviet Union, the Soviets and their surrogates have set up dummy corporations in the West that purchase sophisticated microelectronics manufacturing equipment. This equipment is then shipped and reshipped, sometimes with the knowledge of individuals in the companies, to disguise its ultimate destination—the Soviet Union or Eastern Europe. Both the Soviet and Warsaw Pact intelligence services are in the mainstream of this illegal technology trade flow. The other type of diversion is an in-place diversion, in which legally acquired technology and equipment—in the computer area, for example—are put to military end uses not authorized in export license applications.

The acquisitions that most directly affect Soviet military development have come from intelligence collection and related illegal trade diversions. Soviet Bloc intelligence services have concentrated their effort in the United States, Western Europe, and Japan. These services target defense contractors and high-technology firms working on advanced technology (both classified and unclassified), foreign firms and subsidiaries of US firms abroad, and international organizations with access to advanced and/or proprietary technology, including access to computer data base networks throughout the world.

95-929 O - 82 - 2

Table 1

Major Fields of Technology of Interest to Soviet and East European Visitors to the United States

Computers	Architecture Automatic Control CAD (Computer-Aided Design) Cybernetics/Artificial Intelligence Data Bases Image Processing Design Image Processing/Retrieval	Memories N/C (Numerically Controlled) Units Networks Pattern Recognition Programming Robots Software
Materials	Amorphous CAD Composites Cryogenics Deformation	Metallurgy N/C Machine Tools Powder Metals Superconductors Testing/NDT (Non-Destructive)
Semiconductors	CAD Circuits Defects Devices	Design Ion Implantation Production Technology SAW (Surface Acoustic Wave) Devices
Communications, Navigation, and Control	Antennas Microwave/Millimeter Waves Radio Wave Propagation	Satellite Communications Signal Processing Telecommunications
Vehicular/Transportation	Marine Systems	Shipbuilding
Laser and Optics	Fiber Optics Gas Lasers	Optics Tunable Lasers
Nuclear Physics	Cryogenics Fusion Materials MHD (Magnetohydrodynamics)	Reactors Structural Designs Superconductors
Microbiology	Genetic Engineering	

Both legal and illegal acquisitions of US and Western technology and equipment are coordinated with information obtained through the complex network of international governmental scientific and technical agreements and exchanges that the USSR maintains with the advanced industrial nations. These include know-how, equipment, and computer data base collection activities of Soviet scientists and engineers who participate in academic, commercial, and official S&T exchanges. Visiting Soviet and East European technical and student delegations to the United States generally consist of expert scientists, many of whom are connected with classified work in their home countries. Such was the case with the Soviet scientist who managed to get assigned to fuel-air explosives work. When he finished his US study programs, he almost certainly returned to the USSR to work on related weapons. Other Soviet and East European scientists have come to the United States to work in the aerohydrodynamic, cryogenic, optic, laser, computer, magnetic bubble computer memory, nuclear, microelectronic, and structural and electronic material areas. Given the military importance of these fields to the Soviet Union, it appears likely that a high percentage of these scientists will work on military-related programs in these areas after they return home.

From the beginning, Soviet candidates in various academic and scientific exchange programs have nearly always proposed research activities involving technologies in areas that have direct military applications and in which the Soviets are technologically deficient. Table 1 provides a list of the key high-technology fields that Soviet and East European

visitors come to the United States to study, research, or discuss, many of which are on the US Militarily Critical Technology List today. In each of the past two years, more than a third of the 50 program proposals offered under the Graduate Student/Young Faculty Program of the International Research and Exchanges Board (IREX) has been completely unacceptable in terms of prospective technology loss, and many other programs needed to be modified or have access constrained before the exchanges could be allowed.

The Soviets correctly view the United States and several other Western countries as a continuing source of important and openly available scientific and technical information, which they take every opportunity to obtain access to. Some of the unclassified documents so acquired are previously classified materials which had been downgraded to unclassified through US procedures providing for automatic declassification after a stipulated period. When collected on a massive scale and centrally processed by the Soviets, this information becomes significant because it is collectively used by Soviet weapons designers and weapons countermeasure experts.

The Soviets also regularly attend high-technology trade shows, and attempt to visit commercial firms in the West, particularly small and medium-sized firms that are active in developing new technologies. These apparent trade promotion efforts often mask Soviet attempts to acquire emerging Western technological know-how before its military uses have been identified and government security controls have been applied. Emerging technologies are particularly vulnerable to foreign collection efforts of this type.

Soviet intelligence continues to place a high priority on the collection of S&T information on genetic engineering and futuristic weapons such as lasers and particle beam weapons. The Soviets have been stepping up their efforts to acquire new and emerging technologies such as very-high-speed integrated-circuit (VHSIC) and very-large-scale integration (VLSI) technology from Western universities and commercial laboratories for both military and commercial applications.

Over the past few years there has been an increased use of Soviet- and East European-owned firms locally chartered in the United States and abroad to exploit Western-controlled and military-related technology. There are more than twenty Soviet- and East European-owned firms in the United States, and near the end of the 1970s there were more than 300 similar firms in Western Europe. In addition to the United States, heavy concentrations are in the United Kingdom, Sweden, the Netherlands, Italy, the Federal Republic of Germany, France, Canada, Belgium, and Austria. These firms are avenues for Soviet acquisition of advanced Western technologies, as was shown when the US engineer arrested in late 1981 was charged with selling US secret documents to an East European intelligence officer employed by a Polish-owned firm chartered in Illinois (see inset, p. 6). Furthermore, firms chartered in the United States can legally purchase controlled US technology and study it without actually violating US export controls unless they attempt to export the equipment or related technical data from the United States without a license.

Soviet Acquisitions and Benefits

Today's recognition of the crucial role of Western technology in the development and production of Soviet weapon systems and related military equipment is not unique. Soviet dependence on Western technology was visible and clear-cut in the years immediately after World War II, when the Soviets stole Western nuclear secrets leading to their development of a nuclear weapon capability, and copied a US bomber in its entirety leading to production of their TU-4. To achieve major improvements in their military capability quickly, they exploited captured scientists and industrial plants and resorted to a combination of espionage, stealing, and copying Western systems.

Since that early period of near-complete reliance in the 1950s, the Soviets' dependence on Western technology to develop their weapons has decreased. Nevertheless, despite several decades of Soviet priorities focused on science, technology, and weapon systems, the Soviets, because of their inability to be innovative

US Radar Expert Passes Over 20 Significant Classified Reports on Future US Weapon Systems to Intelligence Agent

William H. Bell, a radar project engineer for a high-technology US defense firm was recruited by an intelligence officer who operated under cover as a vice president of the Polish firm called Polamco. This firm is a subsidiary of the Polish Government Corporation and is incorporated in Illinois and Delaware. It began as an importer/exporter of machinery, parts and tools and as a consultant to firms exporting these products to Poland. The recruitment began as a simple friendship between neighbors with mutual sporting interests, grew quickly to include their families, then to proving Bell's credentials by showing a classified document to the agent, and then to passing microfilm copies of classified reports at meeting places in the US, Switzerland, and Austria. Mr. Bell was in financial straits and was easily influenced by the cash proffered—a total of $110,000 over a three-year period. In all, over 20 highly classified reports on advanced future US weapon systems or their components were passed to the Polish Intelligence Service and probably eventually to the Soviet Intelligence Service.

Among the classified reports, those of prime importance to the West included: the F-15 look-down-shoot-down radar system, the quiet radar system for the B1 and Stealth bombers, an all-weather radar system for tanks, an experimental radar system for the US Navy, the Phoenix air-to-air missile, a ship-borne surveillance radar, the Patriot surface-to-air missile, a towed-array submarine sonar system, a new air-to-air missile, the improved HAWK surface-to-air missile, and a NATO air-defense system. The information in these documents put in jeopardy existing weapons and advanced future weapon systems of the United States and its Allies. The acquisition of this information will save the Polish and Soviet Governments hundreds of millions of dollars in R&D efforts by permitting them to implement proven designs developed by the United States and by fielding operational counterpart systems in a much shorter time period. Specifications on current and future US weapon systems will enable them to develop defensive countermeasure systems.

and effectively apply new technology to weapons developments, still depend on Western technology and equipment to develop and manufacture some of their advanced weapon systems more quickly.

Today, Soviet military designers carefully choose the Western designs, engineering approaches, and equipment most appropriate to their deficiencies and needs. These needs are still substantial and pervade almost every area of weapons technology and related manufacturing equipment. Table 2 lists classes of Western technology acquired by the Soviets and East Europeans and illustrates the wide range of Soviet military technology needs. In the following paragraphs of this section, Soviet Bloc acquisitions have been grouped according to their likely applications: strategic systems, aircraft systems, naval systems, and tactical systems. Also cited are acquisitions in the microelectronic and computer areas that have broad application to military and industrial programs. In certain of these areas, notably the development of microelectronics, the Soviets would have been incapable of achieving their present technical level without the acquisition of Western technology. In other areas, acquisitions have allowed the Soviets to reduce the indigenous effort they would otherwise have had to expend.

The Soviets' strategic weapons program has benefited substantially from the acquisition of Western technology. The striking similarities between the US Minuteman silo and the Soviet SS-13 silo very likely resulted from acquisition of US documents and expedited deployment of this, the first Soviet solid-propellant ICBM. The Soviets' ballistic missile systems in particular have, over the past decade, demonstrated qualitative improvements that probably would not have been achieved without Western acquisitions of ballistic missile guidance and control technology. The most striking example of this is the marked improvement in accuracy of the latest generation of Soviet ICBMs—an improvement which, given the level of relevant Soviet technologies a decade ago, appears almost certainly to have been speeded by the acquisition of Western technology. Their improved accuracy has been achieved through the exploitation and development of good-quality guidance components—such

Table 2

Selected Soviet and East European Legal and Illegal Acquisitions From the West Affecting Key Areas of Soviet Military Technology

Key Technology Area	Notable Success
Computers	Purchases and acquisitions of complete systems designs, concepts, hardware and software, including a wide variety of Western general purpose computers and minicomputers, for military applications.
Microelectronics	Complete industrial processes and semiconductor manufacturing equipment capable of meeting all Soviet military requirements, if acquisitions were combined.
Signal Processing	Acquisitions of processing equipment and know-how.
Manufacturing	Acquisitions of automated and precision manufacturing equipment for electronics, materials, and optical and future laser weapons technology; acquisition of information on manufacturing technology related to weapons, ammunition, and aircraft parts including turbine blades, computers, and electronic components; acquisition of machine tools for cutting large gears for ship propulsion systems.
Communications	Acquisitions of low-power, low-noise, high-sensitivity receivers.
Lasers	Acquisitions of optical, pulsed power source, and other laser-related components, including special optical mirrors and mirror technology suitable for future laser weapons.
Guidance and Navigation	Acquisitions of marine and other navigation receivers, advanced inertial-guidance components, including miniature and laser gyros; acquisitions of missile guidance subsystems; acquisitions of precision machinery for ball bearing production for missile and other applications; acquisition of missile test range instrumentation systems and documentation and precision cinetheodolites for collecting data critical to postflight ballistic missile analysis.
Structural Materials	Purchases and acquisitions of Western titanium alloys, welding equipment, and furnaces for producing titanium plate of large size applicable to submarine construction.
Propulsion	Missile technology; some ground propulsion technology (diesels, turbines, and rotaries); purchases and acquisitions of advanced jet engine fabrication technology and jet engine design information.
Acoustical Sensors	Acquisitions of underwater navigation and direction-finding equipment.
Electro-optical Sensors	Acquisition of information on satellite technology, laser rangefinders, and underwater low-light-level television cameras and systems for remote operation.
Radars	Acquisitions and exploitations of air defense radars and antenna designs for missile systems.

as gyroscopes and accelerometers. The quality of these instruments, in turn, depends to a considerable degree on the quality of the small, precision, high-speed bearings used.

Through the 1950s and into the 1960s, the Soviet precision bearing industry lagged significantly behind that of the West. However, through legal trade purchases in the 1970s, the Soviet Union acquired US precision grinding machines for the production of small, high-precision bearings. Similar grinding machines, having lower production-rate capabilities, were available from several foreign countries. Only a few of these machines, either US or foreign, would have been sufficient to supply Soviet missile designers with all the quality bearings they needed. These purchases provided the Soviets with the capability to manufacture precision bearings in large volume sooner than would have been likely through indigenous development. The Soviets probably could have used indigenous grinding machines and produced the required quality of bearings over a long period by having an abnormally high rejection rate.

While some of the Soviet acquisition in the aircraft area appears directed toward the development of countermeasures against Western systems, the Soviets appear to target data on Western aircraft primarily to acquire the technology. Furthermore, while the Soviets have acquired a large amount of hardware and data from planes downed or captured in Vietnam and elsewhere, they continue to attempt to acquire the most advanced technologies through both legal and illegal transactions with the West. Assimilation of

Western technology has been of great benefit to both their military and commercial aircraft development programs—to the extent that aircraft from certain Soviet military design bureaus are to a significant degree copies of aircraft of Western design. Soviet military aircraft designers have "ordered" documents on Western aircraft and gotten them within a few months, including plans and drawings for the US C-5A giant transport aircraft early in its development cycle; these plans, although dated now, have contributed to current Soviet development of a new strategic military cargo plane. Designers were in particular need of data on US technological advances, but more importantly, they needed information on aerospace manufacturing techniques.

Soviet aircraft designers have been interested in US military transports and wide-body jets and probably have managed to accelerate the development programs for their IL-76 Candid and IL-86 transports. The IL-86 looks much like the Boeing 747 and the IL-76 resembles the C-141. Neither system is an identical copy.

The IL-76 also is used by the Soviets as the platform for their new AWACS (Airborne Warning And Control System), which is expected to be operational in the mid-1980s. This system will provide the Soviets with a major improvement in attacking low-flying missiles and bombers. The Soviet AWACS is strikingly similar in many ways to the US AWACS, and is a major improvement over their old AWACS.

The Soviets' acquisition effort in the naval systems area reflects well the two major factors that motivate their requirements: the acquisition of technology not readily available to them—yet critical to their programs—and the acquisition of equipment which, while producible in the Soviet Union, allows them to divert resources to more pressing naval programs. The Soviets appear to have concentrated their acquisitions in areas related to aircraft carriers, deep sea diving capabilities, sensor systems for antisubmarine warfare and navigation, and ship maintenance facilities. In the maintenance area, two huge floating drydocks purchased from the West for civilian use by the Soviets have been diverted to military use. Drydocks are critical for both routine and fast repair of ships damaged in warfare. In 1978, when the Soviets took possession of one of the drydocks, they diverted it to the Pacific Naval Fleet. The other was sent to the Northern Fleet in 1981.

These drydocks are so large that they can carry several naval ships. More importantly, they are the only drydock facilities in either of the two major Soviet fleet areas—Northern or Pacific—capable of servicing the new Kiev-class V/STOL aircraft carriers. Soviet advanced submarines carrying ballistic missiles, Soviet Kiev aircraft carriers, and Soviet destroyers were among the first ships repaired in these drydocks. It is important to note that the drydocks themselves are so large that no Soviet shipyard would have been capable of accommodating their construction without major facility modifications, associated capital expenditures, and interruptions in present weapons programs. Their importance will be even more pronounced when the Soviets construct the still-larger carriers (for high-performance aircraft) projected for the 1990s. The Soviets even have acquired Western aircraft carrier catapult equipment and documentation for this larger carrier; catapult technology, though relatively common in the West, is outside the Soviet experience.

Within the past few years, the USSR also has contracted for or purchased foreign-built oceanographic survey ships equipped with some of the most modern Western-manufactured equipment. In place of US equipment that was embargoed, other Western equipment has been installed on the ships. This modernization of what is the world's largest oceanographic fleet with Western technology will help support the development of Soviet weapon system programs and antisubmarine systems against the West.

Although the Soviets have a strong indigenous technology base that could support the development of much of their tactical weapons systems, this does not prevent them from maintaining an ambitious program for acquiring and benefiting from Western technology in this area. In some cases, their acquisitions satisfy deficiencies in Soviet technology; smart weapons technology and electro-optical technology are examples of

Table 3

Microelectronic Equipment and Technology Legally and Illegally Acquired by the Soviet Bloc

Equipment or Technology	Comments
Process Technology for Microelectronic Wafer Preparation	The Soviets have acquired hundreds of specific pieces of equipment related to wafer preparation, including epitaxial growth furnaces, crystal pullers, rinsers/dryers, slicers, and lapping and polishing units.
Process Technology for Producing Circuit Masks	Many acquisitions in this area include computer-aided design software, pattern generators and compilers, digital plotters, photorepeaters, contact printers, mask comparators, electron-beam generators, and ion milling equipment.
Equipment for Device Fabrication	Many hundreds of acquisitions in this area have provided the Soviets with mask aligners, diffusion furnaces, ion implanters, coaters, etchers, and photochemical process lines.
Assembly and Test Equipment	Hundreds of items of Western equipment, including scribers, bonders, probe testers, and final test equipment have been acquired by the Soviets.

this. Signal and information-processing technology, particularly for Soviet air defense systems, is another. More often, however, technology is exploited to speed up a developmental program or to improve upon original Western designs in an expeditious manner. The Soviets appear to have concentrated their tactical systems acquisitions on Western tank, antitank, and air defense-related technology and equipment in order to derive concepts and know-how to benefit their weapons programs and to design countermeasures to the Western systems. The Soviet SA-7 heat-seeking, shoulder-fired antiaircraft missile contains many features of the US Redeye missile. Such acquisitions have enabled the Soviets to obtain advanced tactical weapon capabilities sooner than otherwise would have been possible.

Western equipment and technology have played a very important, if not crucial, role in the advancement of Soviet microelectronic production capabilities. This advancement comes as a result of over 10 years of successful acquisitions—through illegal, including clandestine, means—of hundreds of pieces of Western microelectronic equipment worth hundreds of millions of dollars to equip their military-related manufacturing facilities. These acquisitions have permitted the Soviets to systematically build a modern microelectronics industry which will be the critical basis for enhancing the sophistication of future Soviet military systems for decades. The acquired equipment and know-how, if combined, could meet 100 percent of the Soviets' high-quality microelectronic needs for military purposes, or 50 percent of all their microelectronic needs.

Table 3 identifies the microelectronic production-related equipment that has been acquired by the Soviet Bloc. These acquisitions have been grouped into areas related to the four steps required to produce a microchip: wafer preparation, circuit-mask making, device fabrication, and assembly and testing.

Soviet computer technology has long been limited by fabrication and production technology problems and by difficulties in software development. Since 1969 the USSR and East European countries have been developing a family of general purpose computers known as the Ryad series. These computers, which make up virtually the total Soviet and East European effort in large general purpose computers, have been and will continue to be used in a wide variety of civil and military applications. Western technology has been important to development of the Ryad series by providing proven design directions both at the system and component levels. The architectural designs of the

Ryad computers, for example, are patterned after those of the highly successful mass produced IBM 360 and 370 series, computers that are used in a wide range of applications and are highly serviceable in the field.

With this approach, the Soviets and East Europeans eliminated many of the risks involved in undertaking the development and production of a new series of general purpose computers, and saved considerable amounts of manpower and time. Since the early 1970s the Soviets and East Europeans have legally purchased more than 3,000 minicomputers, some of which are now being used in military-related organizations. Furthermore, they are also developing minicomputers that are direct copies of Western models. Soviet and East European development of computer systems has been aided by all available means—legal and illegal, including clandestine—for acquiring the needed technical know-how.

Thus, the Soviets and their Warsaw Pact allies have derived significant military gains from their acquisitions of Western technology, particularly in the strategic, aircraft, naval, tactical, microelectronics, and computer areas. This multifaceted Soviet acquisitions program has allowed the Soviets to:

- Save hundreds of millions of dollars in R&D costs, and years in R&D development lead time (see inset).
- Modernize critical sectors of their military industry and reduce engineering risks by following or copying proven Western designs, thereby limiting the rise in their military production costs.
- Achieve greater weapons performance than if they had to rely solely on their own technology.
- Incorporate countermeasures to Western weapons early in the development of their own weapon programs.

These gains are evident in all areas of military weapons systems. While difficult to quantify, it is clear that the Western military expenditures needed to overcome or defend against the military capabilities derived by the acquisition of Western technology far outweigh the West's earnings from the legal sales to the Soviets of its equipment and technology.

Soviet Intelligence Officer Reveals Technology Acquisition Saved Soviet Military Hundreds of Millions of Rubles

A former Soviet intelligence officer revealed that information on Western military-related technology acquired by the Soviet intelligence services saved the Soviet military industry hundreds of millions of rubles. The acquisition of Western technology operationally was assigned the highest priority for collection by local residencies in key West European countries because of the relatively easy access to much US and Western technology in Europe and the praise being received by the services for their acquisition efforts.

These acquisitions were directed by the military manufacturing industries under the Council of Ministers, and there was intense competition between the intelligence services to acquire Western technology needed for weapons development programs. Of particular need by Soviet weapons designers has been the acquisition of knowledge on special materials, notably the weaving of carbon filaments in a three dimensional configuration which the services were tasked to acquire. The end products from this 3-D carbon-carbon weaving technology are useful for ablative heat shields for high velocity reentry vehicles (the warhead part of ICBMs and SLBMs) and for other portions of rocket motors for large missiles. The Soviet acquisition of some of this technology is likely to enable them to eventually gain a capability for increased military options against the West—a capability that otherwise would have taken them several additional years to develop themselves. The intelligence services also worked closely with scientists from the Soviet military manufacturing industries and even planned joint operations against Western Trade and Equipment Fairs in order to acquire needed Western technology.

Outlook for the 1980s

The Soviets' military R&D and weapon test-and-evaluation efforts are continuing at a rapid pace. Several hundred development projects for weapons systems and major system elements are now under way, and it is expected that through the 1980s the number of new or modified advanced Soviet weapon systems emerging from these projects into production and deployment will remain at the high levels of the last two decades—some 200 weapon systems per decade.

Soviet military manufacturing capacity increased by a significant 80 percent during the 1960s and 1970s, and new plant expansion now under way at one-fourth of their key weapons manufacturing facilities will add considerably to their capabilities. These new facilities will be ready to produce weapons in the next four to 10 years. Plant expansion is in the following areas: ground warfare vehicles, including new tanks; aviation, including facilities for a new B-1-type bomber and a new long-range military transport aircraft having strategic airlift capabilities; naval shipbuilding, including submarines for ballistic missiles and cruise missiles, as well as full-size aircraft carriers for high-performance aircraft capable of competing with the United States in global operations; and electronic and microelectronic manufacturing facilities throughout the USSR. The development and production of new Soviet weapons at these facilities is sure to be more complex and costly than during the 1970s.

All of this military development and plant expansion activity, however, is taking place at a time when the Soviet economy has reached its lowest level of growth since World War II. Soviet annual GNP growth may well be limited to an average of 1 to 2 percent by the mid-1980s. Stagnation in industrial sectors that are key to both the civilian and the military sectors will make it increasingly difficult for the Soviets to satisfy the needs of both. Thus, Soviet leaders will have to make tough choices among defense, investment, and consumption; the competition among rival claimants for resources will become intense. Under these conditions, it may be impossible for the Soviets to maintain current growth in military production without hurting the civilian economy.

Despite these economic difficulties, there are no signs that the Soviets are shifting resources away from the military sector or slowing down development of weapon systems that will be entering the production stage by mid-decade. New generations of Warsaw Pact weapons will require selected critical component and modern manufacturing technologies. It is in these areas that Soviet illegal acquisitions of Western technology, complemented by legal acquisitions, are most likely to be concentrated over the next five to 10 years.

Among the more important technologies are microelectronics, computers, and signal processing. Microelectronics will play a very significant role in advances in computers and signal processing, and all of these technologies will be important in developing advanced Soviet missile, aircraft, naval, and tactical weapon systems, and associated detection systems. Additional projected Soviet technological needs related to such systems are presented in the appendix.

As the result of both tactical and strategic force modernizations, Soviet and Warsaw Pact military manufacturers are increasingly pressed by large-scale production requirements and the related need to control manufacturing and materials costs. Thus, particularly critical for the 1980s are Soviet needs to improve their manufacturing capability. To a large extent, the level of manufacturing technology in Soviet plants determines the Soviets' capability to move new technology from R&D into military applications. Manufacturing technologies play a significant role not only in the development of advanced component technologies, such as microelectronics and computers, but also in the actual production of modern military systems.

Future Soviet and Warsaw Pact acquisition efforts—including acquisitions by their intelligence services—are likely to concentrate on the sources of such component and manufacturing technologies, including:

- Defense contractors in the United States, Western Europe, and Japan who are the repositories of military development and manufacturing technologies.

- General producers of military-related auxiliary manufacturing equipment in the United States, Western Europe, and Japan.

- Small and medium-size firms and research centers that develop advanced component technology and designs, including advanced civil technologies with future military applications.

The combination of past Soviet acquisition practices and projected Soviet military needs indicates that the United States and its Allies are likely to experience serious counterintelligence and related industrial security and export control problems over the next five to 10 years.

The task of stopping Soviet Bloc intelligence operations aimed at Western military and industrial technologies already poses a formidable counterintelligence problem, both in the United States and abroad. But that task is likely to become even more difficult in the future as several trends identified in the 1970s continue into the 1980s:

- First, since the early 1970s, the Soviets and their surrogates among the East Europeans have been increasingly using their national intelligence services to acquire Western civilian technologies—for example, automobile, energy, chemicals, and even consumer electronics.

- Second, since the mid-1970s, Soviet and East European intelligence services have been emphasizing the collection of manufacturing-related technology, in addition to weapons technology.

- Third, since the late 1970s, there has been increased emphasis by these intelligence services on the acquisition of new Western technologies emerging from universities and research centers.

The combined effect of these trends is a heavy focus by Soviet Bloc intelligence on the commercial sectors in the West—sectors that are not normally protected from hostile intelligence services. In addition, the security provided by commercial firms is no match for the human penetration operations of such foreign intelligence services. But the most alarming aspect of this commercial focus by Soviet Bloc intelligence services is that as a result of these operations the Soviets have gained, and continue to gain, access to those advanced technologies that are likely to be used by the West in its own future weapons systems.

The Soviet intelligence effort against Western defense contractor firms poses a serious problem in itself. With more than 11,000 such firms in the United States and hundreds of subsidiaries abroad, US counterintelligence efforts are stretched thin. Protection of US firms abroad from hostile intelligence threats is the responsibility of host governments, but they too are feeling the burden of well-orchestrated Soviet Bloc efforts. The Soviet intelligence threat and the illegal trade problem appear to be severe in Japan. It appears that Western industrial security—both defense and commercial—will be severely tested by the Soviet intelligence services and their surrogates among the East European intelligence services during the 1980s.

Western industrial nations also can expect increased Soviet Bloc intelligence activities directed at the acquisition of their key industrial technologies. Western export controls are presently being updated and broadened; the CoCom allies have recently agreed to strengthen controls and to enhance their enforcement. Moreover, serious hard currency shortages, along with generally increased restrictions on Soviet S&T visitors to the United States, will make the Soviets even more dependent on intelligence and other illegal efforts to acquire the goods and equipment they will need.

The massive, well-planned, and well-coordinated Soviet program to acquire Western technology through combined legal and illegal means poses a serious and growing threat to the mutual security interests of the United States and its Allies. In response, the West will need to organize more effectively than it has in the past to protect its military, industrial, commercial, and scientific communities.

Appendix

Projected Soviet Technological Needs and Acquisition Targets Through the 1980s

Given the dynamic nature of their collection program, it is expected that the Soviets will continue their attempts to acquire a broad range of Western technologies. Certain areas, however, represent priority collection targets for them; these areas are critical to the Soviets' enhancement of their weapons capability.

Over the past decade, the Soviets' most pronounced improvements in strategic weaponry have been in the development of a MIRV ballistic missile capability and a significant improvement in the accuracy of their ICBMs. The former capability was made possible largely through the introduction of onboard digital computers and the latter through the improvement in the quality of the missile guidance systems and the procedures used to calibrate them. Technology acquisitions from the West contributed significantly to these improved capabilities.

The Soviets probably will continue to make their highest priority the acquisition of Western microelectronics and computer technology for in-flight guidance computers. This acquisition effort will be motivated by a desire to overcome reliability problems and also to provide the on-board processing capability required for the development of new guidance options with the potential for extremely high accuracies.

The Soviets will also give top priority to acquiring information on the latest generation of US-inertial components upon which the MX ICBM and the Trident SLBM guidance systems are based. Despite the past accuracy improvements of Soviet ICBMs, these two US systems incorporate technologies beyond present Soviet technological capabilities. Moreover, their SLBM accuracies are significantly behind those of US systems. In addition to information on hardware, the Soviets are expected to seek calibration software algorithms which, as the guidance instruments themselves reach their practical performance limit, would allow for continued improvement in weapon system accuracy.

Western solid rocket propulsion technology also will be a high-priority Soviet acquisition target in the 1980s. While the Soviets have vast experience with the liquid-propellant systems which represent the bulk of their ballistic missile force, they are shifting their emphasis to solid propulsion systems, which have practical advantages over liquid systems in a variety of applications. At the same time, the Soviets have had only limited success with the progress of their solid-propulsion program. They probably will pursue the acquisition of information on solid-propellant production procedures, and propellant grain design, motor case, and rocket nozzle technologies.

The Soviets' ABM R&D effort has continued apace since the 1960s. As a result, they have gained considerable expertise in the development of large fixed-site radars for early warning, tracking, and engagement, and their interceptor technology has also improved substantially over the years. Areas remain, however, in which the Soviets will still seek and would benefit from sophisticated Western ABM technology. These include signal processing for detection, discrimination, target assignment, and sensor technology, particularly in the long-wave infrared portion of the electromagnetic spectrum applicable toward improving their launch detection capability.

Priority Soviet targets in the aircraft area will include Western materials technology, particularly composite materials to allow weight-efficient designs. The Soviets would also benefit from the acquisition of certain engine technologies, in particular those critical to the development of high-bypass turbofans for large strategic airlift type of aircraft. While, in general, Soviet avionics technology appear adequate, the Soviets have yet to demonstrate a capability to deploy reliable, accurate airborne inertial navigation systems for long-range navigation and weapons delivery. Thus, while long used in the West, these systems are still prime candidates for acquisition.

Very high priority probably will be given to the acquisition of computer-aided aircraft design technology, an area in which the Soviets are clearly impressed by US progress. In general, they also will continue to benefit from the acquisition of efficient aircraft production technology from the West to reduce costs.

While the Soviets have a strong indigenous air defense radar and missile technology, their general lag in microelectronics and microprocessing will direct them to attempt wherever possible in the West the acquisition of advanced signal-processing hardware and software.

The Soviets will continue to emphasize the acquisition of naval-related technologies applicable to improving their antisubmarine warfare capabilities, an area in which much Western technology is superior to theirs. Thus, a significant effort to acquire acoustic sensor technology can be expected, in particular that technology applicable to the development of large towed acoustic arrays that would assist the localization of Western submarines in open waters. They probably will also target the acquisition of Western signal-processing hardware and software required to fully exploit the detection capabilities of these sensors.

Another critical problem area to which the Soviets will direct acquisition is that of submarine quieting. Here also the Soviets lag the West significantly. As a result, not only are their submarines more vulnerable to detection, but the self-generated noise reduces the effectiveness of their own acoustic sensors.

An area in which the Soviets have historically lagged behind the West is precision submarine navigation—in particular, in the development of submarine inertial navigation systems. The need for improvements here will become more pressing as the Soviets develop long-range cruise missiles for land attack which require precise knowledge of launch location.

The Soviets also will continue to target technologies related to the design and construction of large aircraft carriers (for high-performance aircraft) to reduce the likelihood of poor design choices that would arise in what is for them an entirely new type of construction program.

Much of the Soviet acquisition effort in the area of tactical weapons is likely to be targeted against seeker and sensor technology for tactical missiles and precision-guided munitions. The Soviets will apply considerable effort in particular to acquiring advanced Western electro-optical technology including that related to antitank weapons. As in other weapons areas, the signal processing and microelectronics technologies supporting tactical weapon systems will also be priority acquisition targets. Technical documentation on entire weapon systems, if obtained, will be used to develop countermeasures.

In the microelectronics area the USSR is now at the stage of implementing its LSI (large-scale integration) technology to high-volume production. Despite the large acquisitions of Western technology and production equipment over the past 10 years which have brought them to the LSI level, additional acquisitions from the West are needed for the more sophisticated weapons projects of the future. Ever-increasing needs for higher precision Western equipment will extend at least through the 1980s.

In addition, the Soviets will require considerable expansion of their microelectronic material base to support continued expansion of integrated-circuit production. In this regard, the USSR is seeking Western help to build two or three poly-silicon plants that will more than double current Soviet capacity for military applications. Also, with increasing advances in the technology, the USSR already will be seeking additional Western assistance in key complementary technologies such as packaging and printed circuit board production.

The USSR is expected to focus its future acquisitions efforts on the emerging technologies related to very-high-speed integrated circuits (VHSIC) and very-large-scale integration (VLSI). It is important to note that, while VHSIC is thought of as a military development program, and VLSI as a civilian technology, there is little difference between the two as far as Soviet production needs are concerned. The same materials, production, and test equipment will be used to produce both. In both of these technological areas, the USSR has developed effective means for illegally acquiring Western advanced products.

Prime Soviet collection efforts in computer technology through the 1980s are likely to include large-scale scientific computers such as the US-built CRAY-1 Computer. Computers of this class offer significant improvements over Soviet models in weapons-systems design and simulation and in the processing of numerical data for many military applications. Other hardware targets will include: very dense random-access memory chips; high-capacity disk drives and packs; the so-called "superminicomputer" class of machines; and the latest in general purpose computer technology. All of the above targets offer opportunities for significant performance improvements and represent technologies of substantial Soviet lag.

In computer software, the Soviets will continue to attempt to collect IBM programs and programs of other vendors written for these machines because of past Soviet decisions related to copying IBM computers. The large and growing number of IBM compatible computers in the USSR means that collection activity in this area can be expected to increase. The compelling attraction of computer networks also should spur great Soviet interest in acquiring network-control software and other programs related to networking.

Chairman ROTH. Senator Cohen.

Senator COHEN. Mr. Chairman, I have a prepared statement which I would ask your permission to insert in the record.[1]

Chairman ROTH. Without objection.

OPENING STATEMENT OF SENATOR COHEN

Senator COHEN. I agree with Senator Nunn that while he and Senator Jackson may have some dispute on strategic airlift, there is no dispute about the strategic vulnerabilities brought about by our lack of control over the export of technology to the Soviet Union and to other Warsaw Pact countries.

The subcommittee's interest in this issue has been a bipartisan effort. As Senator Nunn pointed out, Senator Jackson began the investigation in the early seventies and as a member of the subcommittee. I can recall, he also had a series of hearings in 1980. One of the issues that has been of great importance to me is one touched upon by Senator Nunn in his opening remarks: that is academic exchanges. It makes very little sense to me to undertake a program of controlling the flow of goods and materials to the Soviet Union and their Warsaw Pact countries, if, in fact, we allow them into our universities and colleges to obtain the information itself. It is for that reason that I asked Dr. Perry during those hearings in 1980 for a list of all the U.S. students studying in the Soviet Union and a corresponding list of those Soviet students who were studying in the United States.

It is contained in this record of our hearings, February 20, 1980. I will just take a moment to call attention to the disparity that currently exists. For American students studying in the Soviet Union, I will just list three or four topic areas: Ideas about the Russian east in the 19th century Russia and the role of geographical science in shaping them; debates of democratization of the military from 1866 to 1881; the musical genres in Russian music from the last half of the 16th century to the first half of the 18th century; administration of the Russian Empire under Catherine the Great, 1762 to 1796; and a study of the linguistic basis of Pushkin's Iambic Tetrameter.

It is interesting to note the comparison of what the Soviets are studying here. There are some 45 listed, so I will only list one or two: Research in the theory and applications of measuring computing systems for automation of scientific experiments and testing power engineering objects; research of the effect of various technological and constructive parameters on the properties of thin film covers; research of interaction of ions and plasmas to solid surfaces, especially with compound surfaces which are used as construction material for vacuum chambers of fusion devices; research in the field of automatic control as applied to space ships; and development of recurrent methods for navigation in space and optimal filtration of hindrances; and the list goes on and on. You can see there is in fact a double standard that is practiced as far as acquisition of information concerning our respective societies. I would submit this is an area where we ought to focus more seriously as we proceed with these hearings.

---

[1] See p. 313 for the prepared statement of Senator Cohen.

Thank you very much, Mr. Chairman.

Chairman ROTH. Senator Jackson.

Senator JACKSON. Mr. Chairman, I would like to ask consent to have my entire statement in the record together with two letters, a letter to President Reagan on March 8 and a letter to President-elect Reagan on November 14, 1980, together with a speech that I made on February 11 of this year, at an appropriate place in the record and that my statement be included as read.[1]

Mr. Chairman, I want to commend you as chairman for following through on the excellent work that Senator Nunn was able to accomplish as the previous chairman of this subcommittee, pursuing this all-important area of technology transfer.

Senator Nunn played a critical role in the evolution of the studies and investigations that are now underway.

I would point out that documents and other information made available to the Senate by the Select Committee on Intelligence, of which I am a member, as is the distinguished chairman of the subcommittee, Senator Roth, established that the Soviets are pursuing a purposeful and determined campaign in this field. Their activities, as the chairman knows and members of the subcommittee know, are diverse, numerous, and well funded, and they have in too many cases been successful.

We now know, and I believe these hearings will further demonstrate that in many ways the United States has in effect, been supporting the metastasizing power of the Soviet Union. As I stated in remarks to the Senate several weeks ago, there is no longer doubt that our technology has materially aided Soviet expansion. It has improved Soviet weapons, intelligence devices and economic leverage. The need for a clear and comprehensive technology transfer policy is urgent. Yet our Government still has a long way to go. And I want to reiterate what Senator Nunn said, and that is that this is a bipartisan problem. It is a problem that has been present in previous administrations as well as a problem for the present administration.

And may I just conclude on one point here that I think is vital. Our President is going to be sitting down with Mr. Brezhnev, or an appropriate designee, we hope very shortly, in negotiations of strategic consequence. One of the tragedies is that our President will not at this time be able to say to President Brezhnev, "We will be glad to help make for a more peaceful world. We will help make it possible for your country to enjoy some of the benefits of our technology if you will only cooperate in these other areas." In other words, our President will not have the bargaining power, the leverage which he should have in negotiations, because the Soviets have been able to obtain our technology by larceny, where they are not able to get it openly. This gives them an enormous edge both economically and militarily over what they could accomplish otherwise. This should not be the case, and I do want to emphasize the timeliness of this hearing and the importance of this investigation as we deal in the broad strategic area affecting negotiations between the two countries. We have lost a very valuable bargaining chip worth billions of dollars in commercial terms but of even bigger consequence in terms of diplomacy, in terms of

[1] See p. 315 for the prepared statement of Senator Jackson along with the two mentioned letters and copy of Senator Jackson's speech of Feb. 11, 1982.

national security and in terms of trying to reach an agreement that will make for a more peaceful world.

Chairman ROTH. Thank you, Senator Jackson.

Senator Rudman.

Senator RUDMAN. Thank you, Mr. Chairman.

I don't have an opening statement this morning.

Chairman ROTH. Senator Chiles.

Senator CHILES. Mr. Chairman, I would like to ask permission to put my opening statement in the record.

Chairman ROTH. Without objection.

[The statement follows:]

OPENING STATEMENT OF SENATOR CHILES

Senator CHILES. I do want to take this opportunity to thank Senator Jackson who started calling attention to this problem a number of years ago and to thank Senator Nunn and his staff. They did a tremendous amount of work to get prepared for this hearing.

I think this hearing is something we have needed to do for a long, long time. We have been allowing our technology to go to the Russians. It allows them to take a shortcut, and to be able to use their money and to put their money into developing technology for weapons and some of the other items and even using the technology they are getting from us, even in the weapons field, but to cut across and not to spend the research and development money, and that is something that has been going on for a long time.

We have known that technology was leaving this country. At the same time, so far we have done very little about it. One example of Soviet bloc efforts to obtain U.S. technology for military purposes took place in my home State. A Federal grand jury in south Florida indicted a Mr. Carl Heiser and another man and charged them with acting as agents for the Soviet Union and East Germany. He was convicted of conspiring to export, without licensing and authorization, an inertial navigation system and a large capacity advanced computer. Both of those products have directed military applications and although both men were found guilty in a jury trial, they were able to overturn their convictions on appeal. This particular case is only one example of Soviet efforts to obtain our most advanced technology.

I think while there are some laws on the books, enforcement has been very lax and the Commerce Department have not taken the kind of steps we have needed. I hope that these hearings are going to lead to a new policy and to a tightening of controls so that we are not exporting this technology. I am delighted to see these hearings are being held.

Chairman ROTH. Thank you, Senator Chiles. We will now call our first witness, Joseph Arkov. He is a former Soviet engineer now living in the United States.

Mr. Arkov, under our rules, we require each witness to take the oath. We will not require you to stand, but if you will raise your right hand.

Do you solemnly swear that the testimony you give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. ARKOV. I do.

TESTIMONY OF JOSEPH ARKOV (ASSUMED NAME FOR FORMER SOVIET ENGINEER)

Chairman ROTH. You may now proceed.

Senator NUNN. Mr. Chairman, may I make a brief statement on this?

Our first witness is Joseph Arkov, the assumed name of an emigre who, as an engineer in the Soviet Union, worked on various projects to copy or use American technology.

Mr. Arkov is testifying behind a screen because he is concerned about his relatives still living in the Soviet Union. I want to stress Mr. Arkov is here voluntarily. When subcommittee staff contacted him early this year, he was cooperative and forthright and said he would try to assist us in any way he could.

Mr. Arkov, I want to thank you on behalf of every member of the subcommittee for being here and testifying and I want to make it plain that he is using an assumed name for his family's protection.

Chairman ROTH. Please proceed.

Mr. ARKOV. My name is Joseph Arkov. I am a Russian emigre who currently resides in California. I have been in the United States for 2 years. I am employed as an engineer.

I make this statement gladly as a demonstration of my wish to cooperate with the Congress in gathering information about the Soviet Union's efforts to obtain, duplicate, and utilize high technology machinery and information from the United States. At my request, my true name, as well as specific references to my life in the Soviet Union have been deleted from this statement, in order to protect my true identity and to prevent possible harm to my family or me.

I was born and raised in the Soviet Union. My first 8 years of education were spent in ordinary public elementary schools. In my ninth year of education, when I was about 14 years old, I came to the attention of my teachers as being gifted in science and engineering. I was then enrolled in a special school sponsored by the department of physics at a well-known university in the Soviet Union. Following that 1 year program of study, I was allowed to attend an engineering school. I was a student in the engineering school for 6 years. During this period, I was also required to receive military training in a program similar to ROTC studies offered college students in the United States.

After graduation from the engineering school in 1970, I went to work in a research institute. A primary objective of the research institute was to develop highly sophisticated cameras for use in military applications. The institute's activities are examined closely by the Soviet defense ministry. I worked in the institute for about 6 years, from 1971 to 1977.

In 1977, I was assigned to work in another research institute. In this plant, as in many other engineering research and development facilities in the Soviet Union, the major emphasis is on military pursuits.

However, there often is a small section of the military-related installation set aside for the development of civilian and commercial products. Civilian and commercial product development sections are not high priority projects.

If, for example, a new American computer has been obtained by the Soviets, they will make a military application of it, rather than a civilian application. The institute used a sophisticated American computer in its military operations. Officials at the institute were very

proud of it and even provided tours for employees to see it. It was in such a civilian and commercial section where I was assigned to work.

The Soviet Government wants to develop its own ability to produce high technology equipment similar to that manufactured in the West and Japan. But once such products are made in the Soviet Union, the people of the Soviet Union still do not have confidence in them. They prefer goods from the West.

A special premium is placed on products produced in the United States. Goods made in Japan also are considered particularly desirable. Given the choice, the people of the Soviet Union do not prefer their own country's products. There is no patriotism in department stores.

The Soviet Government wants more high technology from the United States. Each technical institute is allocated a certain amount of money to be used for the purchase of Western, particularly, American technology.

The Soviet Union has two goals in mind when it seeks to obtain high technology machinery from the West. One objective is to study the equipment with the intention of imitating or duplicating it.

The second objective is to use the machinery, particularly to use it in the manufacture of other high technology components. The second goal—the use of the machinery—is, by far, the most important to the Soviets.

In my work in the second research institute, I had the assignment of copying Western and Japanese high technology. One of my tasks, for example, was to develop a system design for the production of color television cameras for video tape recorders. In this pursuit, my supervisors made no attempt to be deceptive about what they wanted me to do. I was not to conduct any original research and development. I was given television components produced in Japan and I was told to copy them.

The Soviet Government benefits to a certain extent from its programs aimed at duplicating Western technology. But the results have been, and will continue to be, limited. Soviet authorities have come to the realistic conclusion that their country's level of technology is too far behind the West for them to make great strides through copying. They do not have the human resources or the fine-tuned equipment required to produce the high technology machinery they try to copy.

Once they know what makes a given piece of machinery work, they find that they do not have the technical know-how and equipment to produce the product themselves. That is why they want Western high technology machines that will enable them to produce the products. And the Western products they desire the most are those produced in the United States. That is why they want American high technology machines with which they can produce the components for high technology products.

By using—not copying—the American high technology products, they move closer to their goal of technical self-sufficiency. Whether they will ever become self-sufficient in high technology is a debatable point. My own view is that this course of action gives them quick gains but, over the long run, it will result in their being permanently behind the United States, forever having to rely on American products to manufacture their own.

However, being behind us in technology is a relative condition. The Soviets can make progress in a technical sense and, at the same time, trail the United States but, by their standards, they will have achieved much. Their accomplishments will have been made with limited cost to them because the basic research and development will have been paid for by the Americans.

To repeat, then, the Soviet strategy in obtaining American high technology products includes efforts to copy and duplicate but the Soviets' primary objective is to obtain machinery which they can use in the manufacture of their own high technology equipment.

This distinction—the difference between copying of technology and the use of it—is an important one because it provides the United States with a key insight into which products the Soviets are the most anxious to obtain. It also can influence American policymakers in deciding which products the United States can afford to sell the Soviet Union, and which components should not be sold to them.

Soviet strategy in using American products can be seen in the following illustration. Let us say, for example, that the Soviets have 100 plants involved in producing components for use in space flight. Each of the plants could use a certain kind of American computer. But they cannot obtain 100 computers; that is, one for each plant. Instead, they are able to obtain three or four American computers of the desired type. They use the computers as best they can in those three or four plants where they can do the most good. They are not inclined to use them as nonproducing models to be studied in a laboratory for the purpose of copying.

Moreover, if the American product obtained in another transaction—if, for example, the product is a sophisticated oven used in the heating of microchips—then they are even less interested in copying or imitating. They will use the oven to produce microchips. There is no civilian use for equipment used to manufacture integrated circuits or semi-conductors.

The Soviet Union obtains American high technology in ways other than copying or utilizing machinery. The Soviets make the most of American technical journals and Government documents.

In the free society of the United States, there is not much that can be done to prevent the Soviets from getting hold of technical journals and other private publications. But it is my opinion that the U.S. Government is following an unwise policy in making public as much military data as it does.

[At this point, Senator Jackson withdrew from the hearing room.]

Mr. ARKOV. From my own personal experience in the research institutes, I know how the Soviets wasted no time in distributing information from the U.S. military. In a military refresher course following my graduation from college, I was part of a group that was shown films of U.S. military equipment such as tanks, artillery, and amphibious vehicles. One film showed the internal layout of one such vehicle. The blueprints revealed their publication date, a time only 2 months prior to the date of the refresher course. That indicated to me that the Soviets had obtained and made informational use of the design of the vehicle before it went into production. In addition, one of my duties in the research institute was to read American technical journals and U.S. Government publications. A special team of Eng-

lish-speaking Soviet linguists was employed to provide us with prompt translations into Russian of the journals and documents.

In most fields of technical research, development and production which I am familiar with in the Soviet Union, the overwhelming majority of resources are invested in military applications. If, in the area of high technology obtained from the United States, one much prized oscilloscope is obtained from the United States, it will be turned over for military application in virtually every instance. This strengthens the position of the U.S.S.R. armed services but it is done at the expense of the civilian sector.

The oscilloscope might have been used in the development of a consumer product but rarely are such high technology devices ever utilized to benefit the Soviet citizen as a consumer.

As a matter of fact, the Soviet industrial capacity is so completely overburdened with military production that the Soviets could not make a civilian or commercial application of certain high technology products even if they wanted to.

For example, there is almost no possible way the Soviets could make a civilian application of laser technology. Any laser component they obtain from the United States will go into the military sector. The Soviets have no other use for it. There is no commercial market for high technology equipment to the U.S.S.R. People cannot afford such luxuries yet the Government displays it for propaganda purposes. Most equipment is used by the Soviet military industry.

In my engineering jobs in the Soviet Union, I frequently was assigned to attend trade fairs where Western nations, including the United States, displayed their high technology equipment. I was seen as a potential buyer. But, in fact, I was not there as a would-be consumer. I had not been sent to the trade fair to buy anything. I was there to obtain information about Western technology concerning aircraft and missiles as well as other technical areas. I discovered many valuable technical ideas at trade fairs and reported on them to my supervisor back in the Soviet Union.

Aside from learning and inspecting the wares displayed in trade fairs, Soviet visitors have been known to steal products and their components. I know a man in Russia who had been assigned as a security guard at a trade fair in Moscow. This assignment was the turning point of his career. In league with the KGB, the man used his position as security guard to steal several pieces of high technology equipment. He was rewarded handsomely for his thievery. Not an especially intelligent man, he could never have earned on his own the Ph. D. degree he subsequently was awarded. He was then made director of a department in a research institute, a position for which his training, experience, and ability left him totally unqualified.

Senator NUNN. Might I interrupt while you are taking a break.

You are saying this individual stole equipment from a trade fair where he was a security guard and he was rewarded for that with a Ph. D. degree?

Mr. ARKOV. Yes.

Senator NUNN. Was it an honorary degree or do they have such a thing in the Soviet Union?

Mr. ARKOV. It is an honorary degree and it is awarded not only academically, but materially.

Senator NUNN. It is an honorary degree for thievery?

Mr. ARKOV. Yes.

Senator COHEN. It is called the "Peter Principle" in this country.

Mr. ARKOV. In my college days, neither I nor any of my fellow students were given the opportunity to study in the United States under a student exchange program. Normal students were never considered for such programs. Those who got to study in the United States usually were not even students in the usual sense of the word. They were much older than we were and often they were well established in their technical or scientific fields. Frequently they were professors who had already obtained their Ph. D. degrees.

One of my supervisors at a research institute visited the United States to work with the National Aeronautics and Space Administration in Houston on the Apollo space program. His duties at the institute related to its military operations and I am sure that he was instructed by Soviet officials to obtain and bring back any information he learned while working on the space program.

The Soviets considered college age students to be too young and unpredictable to be trusted to attend universities in the United States. Equally important, we had not yet advanced far enough in our studies and knowledge to obtain the high level of information Soviet authorities desired.

Soviet authorities selected participants in the student exchange programs from science and engineering. Conversely, American exchange students might be from the humanities; they might come to the Soviet Union to study Dostoyevski. But the Soviet students did not go to the United States to study Faulkner. Their purpose in the United States was to obtain American technology. In the engineering classes I took in college, I met students from Cuba, North Vietnam, and Hungary but no Americans.

As a youth, I was fascinated by Marxist ideology and believed in the society the Soviets were trying to build. But by the age of 19, I was becoming disillusioned. What contributed to my growing disenchantment with Soviet life was my realization of the extent to which the government put out false or distorted information.

In the Soviet Union, the government has a monopoly on truth. Officials lie about so many things that it is possible to slip into a frame of mind in which nothing the government says is believed.

Senator NUNN. Mr. Chairman, may I ask one other question at this point?

Do you think you were the exception in this regard in distrusting the government or was this pervasive in the young people of your age?

In other words, were you one person who was skeptical? Were there a lot of people skeptical about the Soviet propaganda?

Mr. ARKOV. Yes; that is true. There are a lot of people who are skeptical but not everyone.

Senator NUNN. Could you hazard a guess? What is the order of magnitude of people who really believe their own government is lying?

Mr. ARKOV. I would say most of the population feel that what government says is not true. But they don't have the source of other information and they cannot compare it.

Is it true or not? The Soviets have a feeling that it is not true, but they don't know what the truth is.

Senator NUNN. Are you saying a very large percentage?

Mr. ARKOV. Very large, most of the population.

Senator NUNN. More than half the people are really skeptical?

Mr. ARKOV. Yes; especially young people.

Senator NUNN. Young people particularly?

Thank you.

Mr. ARKOV. Besides my objection to the many official lies, I was also deeply troubled by the relatively low income I was receiving and could hope to receive in the future. While engineers enjoy a social status of some consequence in the U.S.S.R., they are paid very poorly. It is an odd contradiction on Soviet society that the government wants very badly to compete technologically with the West but rewards with meager pay the engineers whose job it is to make the country competitive. Moreover, the fact that I am Jewish was an additional barrier to any improvement in income.

All these factors—the official lies and distortions, the lack of professional opportunity, the anti-Semitism and, most important of all, the absence of freedom—combined to lead me to conclude that I had had enough of the oppressive Soviet regime. In the late 1970's, I concluded that I had no choice but to try to get my family and myself out of the country.

I applied for an emigration visa. I knew that authorities might quickly take punitive steps against me. I have a friend in Russia who applied for an emigration visa. A trained engineer, my friend was promptly fired from his technical job and was never given permission to leave the Soviet Union. Unable to find another professional position, he was forced to take any job that came along. The last I heard of him he had been reduced to working as gatekeeper.

I do not know why some applications for emigration visas are approved and why others, such as that of my friend, are consistently denied. But some applications do get through and, for reasons unknown to me, my family's and mine were approved. Although I was immediately fired from my job when I petitioned for the visa, after a wait of 4 months, we received permission to leave the country.

We have settled in Los Angeles County and I have found satisfying employment as an engineer in an optical firm. Things have worked out in a satisfactory manner for my family and me. We are thankful and proud to be living in this great nation.

Thank you.

Chairman ROTH. Thank you, Mr. Arkov.

I, too, want to join Senator Nunn in thanking you for your willingness to come before us and your fine cooperation throughout the hearing.

The subcommittee will limit the first round of questioning to 5 minutes. I would point out to my colleagues that we have, I think, five witnesses this morning so that it is important that we move as expeditiously as possible.

Mr. Arkov, what would you consider to be the most important steps for the United States to adopt to prevent the flow to the Soviet Union of modern technology and equipment? Would you list several measures that you think are important to protect our valued secrets?

Mr. ARKOV. It is a difficult question.

First, we have to study thoroughly what kind of fruits the Soviets obtain from the information and technology supplied to them. We have to analyze all of the information published.

Chairman ROTH. Why do you think that the U.S.S.R. prefers to obtain Western technology rather than concentrate more on research and development whether intended for commercial or military purposes?

Mr. ARKOV. Trying to obtain Western technology, they don't dismiss conducting their own research. They would rather try to be independent in their own way.

Chairman ROTH. Do the Soviets have the talent to advance in technology like the United States and other Western nations?

Mr. ARKOV. They do have an intellectual potential, but in most cases they are limited in the technological support in which to yield the high quality and quantity of products. There is also a lack of organization within the government system which prevents them from pursuing high quality achievements.

Chairman ROTH. Do you know of any instances where the U.S.S.R. obtained Western technology from U.S. allies or from Eastern Block nations?

Mr. ARKOV. Yes; the U.S.S.R. received a vacuum coating technology used in optic filters from Lichtenstein. The institute and the U.S.S.R. who received this sophisticated technology did extensive military research.

Chairman ROTH. Senator Nunn.

Senator NUNN. Thank you, Mr. Chairman.

What particular areas of technology and information were considered most important by the Soviets based on your experience?

Mr. ARKOV. Semiconductors, solid state devices, microelectronics, fiber optics, systems of communication, space technology, subsea technology, and surveillance and detection systems.

Senator NUNN. Where would you go in our society to obtain critical use technology?

Mr. ARKOV. First, I would try to establish contacts with people involved in the business of my interest. The best places to do this are at technical symposiums and meetings where people are less formal and more willing to talk.

Senator NUNN. Do you believe that the United States is putting too much emphasis on technology transfer to the Soviet Union? Do you think we are engaging in a degree of paranoia?

Mr. ARKOV. No, not at all. You should take first steps to prevent our technology from slipping to the Soviet Union.

Senator NUNN. How do you gage the United States and the U.S.S.R. in terms of technological advance? Are we far ahead of the Soviets? Are we somewhat ahead of the Soviets? Or are they gaining on us?

Mr. ARKOV. I feel that they are behind us but they can gain a lot using our technology if they can obtain it. And even then, they try to reinforce their labor force and manpower used for military purposes.

Senator NUNN. You understand we are an open society and that is one of our strengths. When you look at what the Soviets' obtained

from us in technology and look at our open society, how do you balance those two in terms of importance?

Mr. ARKOV. I wouldn't trade anything for freedom, but it is very difficult to analyze how to trade them. It is a very difficult question.

Senator NUNN. It is a difficult tradeoff. You understand that one of the strengths of our technological development is that we do have an open society, freedom of exchange, and so forth with our information.

Let me ask you another way: Do you think the Soviets closed society actually impedes their technology development?

Mr. ARKOV. No.

Senator NUNN. You do not?

Mr. ARKOV. I do not.

Senator NUNN. What is the major problem with the Soviet technology? Why aren't they further ahead than they are with the Soviet technology?

I am speaking in terms of the commercial and industrial sectors, not just the military.

Mr. ARKOV. First of all, it is a lack of organization.

Senator NUNN. A what?

Mr. ARKOV. A lack of organization. They cannot organize the society as well as the United States. But they do have intellectual potential. They have some smart people.

Senator NUNN. You say they do have intellectual potential?

Mr. ARKOV. Yes; but they do not have the organization which can help them to utilize the intellectual potential.

Senator NUNN. Mr. Chairman, I will come back after Senator Cohen.

Chairman ROTH. Senator Cohen.

Senator COHEN. I just have one or two questions. Your statement concerning the comparison between studying Dostoyevski and Faulkner, I think, is a good one. It reminded me of the double standard that we have even in our athletic competitions.

For example, our amateur, at least, true amateurs in this country, have to compete against what I believe to be true professionals in the Soviet Union for the Olympic games. Unfortunately, that is the way the rules are written. But it seems to me drawing from your statement about the disparity of students studying in this country and our students studying in your country or former country, that the Soviets are never going to allow our students to study anything much beyond the humanities.

Is that a fair statement?

Mr. ARKOV. Yes, very fair.

Senator COHEN. It is also clear that the Soviets are never going to allow young Soviet students to come to this country to study humanities or even physics or any other courses because they are considered to be too unprofessional, too unskilled for the purposes for which the Soviet Union would seek to use them.

Mr. ARKOV. Yes; this is true, especially the analogy of Faulkner is very good.

Senator COHEN. What is the option open for the United States? Is it to bar Soviet students from studying subjects which could be con-

verted to military purposes, or useful in developing military technology?

What is the option for a free society such as the United States?

Mr. ARKOV. I think that is a great idea to let our students study around colleges but they should let their own Soviet students to study the same things here, but not in high technology.

Senator COHEN. So we should have a so-call two-way street that since we allowed to study Soviet Russian culture, Soviet students should be allowed to study American humanities?

Mr. ARKOV. Yes; it should be done on an equal basis.

Senator COHEN. That is all I have, Mr. Chairman.

Chairman ROTH. Senator Rudman.

Senator RUDMAN. Thank you, Mr. Chairman.

Mr. Arkov, I notice in your statement that you spent 6 years working in what was called a research institute dealing with optics and cameras and used by the Soviet military, is that correct?

Mr. ARKOV. Well, it's correct.

Senator RUDMAN. Did that institute have any great independent research arm of its own or was it mainly aimed at obtaining technology from the Far East and from this country and essentially copying their technology to develop products that the Soviets would use in their military forces?

Mr. ARKOV. Well, the task of copying Western technology—it is part of the job they assign to them. The major application of their assignment was for military. Is that the question?

Senator RUDMAN. Yes; let me just follow that up. You spoke in your prepared statement about the use of sophisticated American computers in various Soviet military operations, and also about the use of semiconductor technology. There are those in this country who feel that had we not transferred that technology legally to the Soviet Union—we sold them certain semiconductor technology and certain sophisticated computer technology in the late sixties and early seventies—the Soviets would not have achieved the advantages in missilery which they have made in terms of the enormous throw weight and precision of their guidance systems. Do you agree with that assessment? Do you think that the sale of those semiconductors and those computers has given them a tremendous step forward in their technology in the defense area from your background and your knowledge?

Mr. ARKOV. Yes; I think so. I can't tell exactly. It's hard to estimate the degree of advantage they got. But they gained there using American computers and American semiconductors.

Senator RUDMAN. In your research institute, I assume you had computers. Were there computers in the research institute for your use?

Mr. ARKOV. Yes.

Senator RUDMAN. There were computers. Were they Soviets computers or were they American computers?

Mr. ARKOV. Most of them were Soviet computers, but they also did have American computers and they used both and we tried to establish computerized system resembling the American one.

Senator RUDMAN. Would you repeat the last part of that for me.

Mr. ARKOV. They tried to copy a computerized, a test system, using the American computer.

Senator RUDMAN. Did you find in your work in that institute, of those Soviet computers and American computers that the American computers were more advanced, easier to use, and could do more things?

Mr. ARKOV. Yes, it was, especially the minicomputer and the Soviets at that time didn't have minicomputers.

Senator RUDMAN. You are talking about microprocesses and minicomputers?

Mr. ARKOV. Yes.

Senator RUDMAN. Thank vou, Mr. Chairman.

Chairman ROTH. I have just one question. From your background and experience, do you think people in the Soviet Union believe that it is easier to secure technical information from the United States or from Japan and Western Europe? Which area has possessed the best security in protecting technological secrets?

Mr. ARKOV. I think, for instance Japan publishes less than the United States.

Senator NUNN. Publishes?

Mr. ARKOV. Publishes less technical information. First, they publish information in Japanese and maybe develop the same, but they really publish less.

Chairman ROTH. I gather from your testimony that much valuable information comes from military and Government journals themselves, U.S. military journals?

Mr. ARKOV. Well, not only military but other professional magazines.

Chairman ROTH. Other professional.

Senator Nunn.

Senator NUNN. You mentioned two or three times Soviets placed their top priority in actually utilizing American technology as opposed to copying it. Do they do both?

Mr. ARKOV. They do both.

Senator NUNN. But they actually utilize it. What happens when an American computer or other technology breaks down, if that computer has been obtained by illegal means? How do they repair it?

Mr. ARKOV. They probably don't. They study it thoroughly trying to copy it because they can't repair it. They don't have spare parts.

Senator NUNN. How good is the Soviet reverse engineering? How good are they at copying or reverse engineering, taking American pieces of equipment and then making their own?

Mr. ARKOV. There is a big gap between engineering knowledge and——

Senator NUNN. Big gap between engineering knowledge and what?

Mr. ARKOV. Big gap between engineering knowledge and their manufacturing ability. They do know how to make, but they cannot make it because there is a lack of technology.

Senator NUNN. So they have difficulty with reverse engineering, is that what you are saying?

Mr. ARKOV. That's right.

Senator NUNN. They do it, they work at it, they try to do it but it is very difficult?

Mr. ARKOV. Even if they do know how to make it, in many instances they cannot make it. So they still would be trying to obtain more and more technology.

Senator NUNN. Thank you, Mr. Chairman.

Chairman ROTH. I want to thank you, Mr. Arkov, for coming before us, for your loyalty to this country. I would say to our people attending this hearing that it will be necessary to clear the room to protect the security of this witness. So I would ask the security people now to clear the hearing room.

[Hearing room cleared at this time.]

Chairman ROTH. The subcommittee will please be in order. I thank the people attending the hearing for their cooperation.

At this time, we will call forward Mr. William Holden Bell. Mr. Bell, please come forward.

Mr. Bell, will you please stand, raise your right hand. Do you solemnly swear the testimony you give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. BELL. I do.

Chairman ROTH. Please be seated. Mr. Bell, you may proceed with your testimony.

Mr. Bell is represented by an attorney who is out for just a moment and will return.

Mr. BELL. Can I proceed?

Chairman ROTH. We will wait until your attorney comes in.

Senator NUNN. Mr. Chairman, while we are waiting, can I ask the witness a couple of background questions to lay a foundation?

Chairman ROTH. Sure, please proceed, Senator Nunn.

Senator NUNN. Mr. Bell, are you now serving a prison sentence?

Mr. BELL. Yes, I am.

Senator NUNN. Where are you serving?

Mr. BELL. Springfield Camp, Springfield, Mo.

Senator NUNN. What was the crime you were convicted of?

Mr. BELL. For passing defense data.

Senator NUNN. Mr. Chairman, Mr. Bell has an attorney here this morning. According to our rules, he is permitted to consult with his attorney at any point. I want to be sure that he and his attorney recognize that. He is entitled to consult with you if you would like.

Mr. KIRSTE. Thank you.

Chairman ROTH. Mr. Bell is under oath. Please proceed.

TESTIMONY OF WILLIAM HOLDEN BELL, PRISONER, ACCOMPANIED BY ROBERT LANDON KIRSTE, COUNSEL

Mr. BELL. Mr. Chairman, I am grateful for the opportunity to appear before this subcommittee and provide whatever information that I can. I have worked in the international field for more than 20 years and have first-hand experience in the transfer of technology to Western Europe and to the Soviet bloc nations.

In the way of background, I was born on May 14, 1920, in Seattle, Wash. After leaving school and working for my father as a teenager to support the family, I joined the Navy at the age of 18. The destroyer-minesweeper to which I was assigned swept the channel at Pearl Har-

bor during the attack on December 7 and was preshipped to sea. I also participated in civil operations throughout the world and was hospitalized following injury in an underwater explosion in Iwo Jima.

I married my first wife after receiving an honorable discharge. We have two sons and one daughter.

I completed my high school education by correspondence school while in the Navy. I attended the University of Southern California and the University of California Los Angeles where I received a bachelors degree in applied physics. In 1950, I was employed by Hughes Aircraft Co. as a test technician and the following year became accepted as an engineer and member of the technical staff.

During my 30 year career at Hughes Aircraft Co. I held a secret clearance classification and had many technical and managerial positions. I continued my education through research, experiments, seminars, symposiums, and constant reading of scientific literature. I was and am an expert in the military application of radar in tactical operations and weapons systems.

Since 1962, I have been directly concerned with the transfer of U.S. technology to Europe and the Middle East. From 1962 to 1965, I was manager of a European program for Hughes Aircraft Co. and from 1974 to 1976 I was manager of radar operations for Europe and the Mideast. In connection with these assignments and otherwise, I personally traveled extensively through Europe and the Middle East.

A number of personal events combined to set the stage for my recruitment by the Polish Marion Zacharski, my overseas assignments were financial nightmares, although they are touted as glamorous and lucrative. My wife and I were divorced in an extended proceeding. My assets were tied up and I was paying her $200 a week alimony.

I was pursued by four separate IRS offices for back taxes on disallowed deductions primarily arising out of my overseas assignments. I returned from Europe to find a younger group at Hughes and I shunted off to a quiet back room.

My youngest son, Kevin, to whom I was extremely close, died needlessly from burns sustained in a camping accident in Mexico. While I waited with an ambulance at Los Angeles International Airport, a Mexican Airlines pilot ejected him from the plane in Mexico preventing him from receiving prompt and adequate treatment.

I married a young Belgian citizen, Rita. We tried to build a new life with her young son in her Playa del Rey apartment complex. I was forced to file bankruptcy and name my employer on the schedules, however, I continued to pay or reaffirm most of my debts.

Zacharski and his wife moved into the apartment complex and he and I began to play tennis on a daily basis. He slowly became my best friend. He was about the age of my oldest son who had been close to his mother and quite distant from me since our divorce. When you are sent to Europe, you are told to expect attempts by foreign spies, but whoever would expect it to happen here at home?

Zacharski was the west coast manager of a Polish-owned American company, Polamco, which is a Polish-American receiving company. He had an extensive expense account and gave away various items out of their public relations funds. He was interested in what I did and enlisted my aid in making contacts in the industry for the possible

sale of Polamco machine products. He suddenly delivered $4,000 to me for my very minimal efforts in that regard.

He expressed an interest in having Polamco hire me as a consultant after I retired from Hughes Aircraft Co. In order to impress him I showed him a sample of some work I had done of which I was quite proud. Although I showed it to him on the tennis court, he took it to his apartment for reading. It was classified secret.

At this time, the apartments were being converted into condominiums at the cost of over $80,000. Zacharski asked me if I were going to buy one, as his company was buying his. He knew I didn't have the funds. In view of my prospective employment by Polamco, he thought he could help me. Subsequently, he appeared at my door handing me envelopes of cash. With this money I paid the IRS and made a down payment on the condominium. I signed a receipt for the money and concealed the source from my wife.

Zacharski furnished me with a movie camera. He instructed me to make a setup to photograph documents by using a single frame device. He told me that we would be making a trip to Europe but when it was time to go he did not accompany me. The primary purpose of the trip was to negotiate.

Even as I went to Innsbruck, Austria, I was rationalizing and kidding myself that the persons I would meet were representatives of Polamco, that this was just the kind of industrial espionage that goes on all the time.

This meeting started by my turning over film of documents that I had previously shown to Zacharski. I was paid $5,000 in expenses for the trip in cash. All of the cash that I was given was always in $50 or $100 bills. I talked with two men the FBI had since referred to as handlers. A man later identified as Paul and the younger guy whose name I cannot recall. Under the guise of discussing methods of payment to me, they took great care to describe where I lived and shopped in frightening detail. They also showed me pictures of my family, my wife and my young boy, and told me that there were only six persons involved.

They told me that if anyone caused a problem, they would be taken care of.

I was assigned the code name of Jackson and given a phone number in Poland. I signed a receipt for the money. There was no question of what I was getting into. I made one more trip to Innsbruck, another to Lintz, and a final one to Geneva, Switzerland. On the last two trips, I traveled with films of American secret technology in my luggage. They had provided me with black and white high-resolution film which had 8 to 12 feet of regular color home movie film attached to the ends in case it was inspected.

A young guy asked me to design a low-level-based radar which would detect planes coming into Poland from 200 meters above the sea. Both Zacharski and my handlers gave me extensive lists of documents to be obtained. They knew exactly what they wanted—right down to the company identification numbers. They even asked if I ould go to work for a different American company, DARPA, to get what they wanted. DARPA, incidentally, is the Defense Advanced Research Projects Agency, an organization funded directly by the Department of Defense.

They fund advance technical programs, technology programs, types of things the military would ordinarily handle but they would have a high payoff if they were successful.

Zacharski told me that he could go to any town in the United States and the local chamber of commerce would direct him exactly where to go and who to contact. He delivered additional cash in gold coins to me at my condominium. It was always the same. He would come to my door when I was alone, hand it to me with a smile and walk away, or place it in my tennis bag as we walked to the tennis courts.

He made constant trips to Chicago and in fact traveled extensively throughout the United States for the company—Polamco.

My financial burdens, of course, were resolved overnight. However, I was afraid when I could not, or would not, deliver more classified documents I would be liquidated or, much worse, my family would be endangered.

My third trip was to Lintz, Austria——

Senator NUNN. Did he ever tell you that or was that something you feared?

Mr. BELL. Yes, sir, I did. On one of my trips into Austria, on the first trip and the second trip, a man by the name of Paul threatened me on both trips. It was a very clear threat. He threatened me by showing me pictures of my 8-year-old son, my wife's son, whom I raised since he was 3½. He showed me pictures of my wife. It was very clear there were tenors of threat. Incidentally, it is a horrible feeling when you are operating on the wrong part of the law.

I am sure it is horrible to anyone who has their family threatened, but when you are on the wrong side of the law, it is horrible.

My financial burdens, of course, were resolved overnight. However, I was afraid when I could not or would not deliver more classified information, I would be liquidated.

My third trip was to Lintz, which is only 50 miles from the Czechoslovakian border. I was particularly frightened on this trip. I met the young guy and walked with him to a small restaurant. There was only one other patron, a roughly dressed man who appeared to be a laborer. The weather was stormy and the city dark and foreboding. The young guy seemed totally at ease. He took the film from me openly and disappeared into the kitchen. He returned and we drank coffee, making small talk, then left and walked about 100 meters to another restaurant where we drank more coffee.

Leaving the second cafe, we walked an inclined path lined with hedges up into a wooded area. After we had gone up some distance and stopped to talk, I suddenly saw the roughly dressed laborer which I had seen earlier pearing over a hedge or bush. He ducked down as I looked at him. I thought for a moment that I would be killed. The young guy simply smiled about it and told me that it was his man watching him because he carried a lot of money.

They constantly wanted me to go to Mexico City and I kept making excuses. I knew a man at DARPA who I respected and trusted. I thought if I could confide in him he might help me out of my dilemma. On a trip east, I tried to see him but he was out. I don't know if I would have actually had the nerve to tell him, but that was my intent. It is the closest I ever came to giving myself up.

Zacharski told me that he was being followed. From the way he described it, I couldn't believe it. He claimed that he was being openly harassed and I assumed it had something to do with some labor union rather than the FBI or likewise. Or some problem with Polamco. One day when we went to play tennis, he told me "There they are." He pointed out two cars in the parking lot. I went back to my apartment and got my camera. I photographed each of them, afterward laying my camera on the ledge. Then I went to each car and confronted the person in each car. I demanded to know who they were and what they were doing. They refused to tell me anything and departed. When I returned to the ledge, the camera was gone. To this day, I do not know what became of it.

The FBI tapped Zacharski's phone. I was told they also tapped mine. It didn't matter because Zacharski has told me never to talk on the phone. Although I was unaware of it, I was also being followed.

On my final trip to Geneva, I took film of the LPIR or quiet radar. I was followed all the way. When I arrived in Geneva, an innocent American in a turtle neck sweater engaged me in a conversation and a drink at the hotel. He happened to be from my birthplace in Seattle, Wash., and I understood that 6 months were invested in ascertaining that he had nothing to do with me. I went to the Arizona Museum a day early and noticed a man with a black hat, coat, and briefcase wearing dark glasses, looking at me.

I walked to a newsstand for a moment and left. He walked to the same newsstand. The FBI showed me photos of these men. The following day I gave away the film on the quiet radar to my handler in the elevator at the United Nations building. I was no longer being surveiled when I did this.

On this trip, I was instructed to go to Mexico City on the next trip and meet a new contact at another museum. I was to carry an airline bag and respond to the code phrase "Are you interested in the Aztec exhibit?"

By replying, "No, I'm interested in the Mayan calendar" I was shown a key chain with a black medallion bearing a silver P for Poland, which my contact would display. I never went. The FBI interviewed me first. I told them everything. There is little left of my life now but I feel I am freer in prison than I was with Zacharski.

I have set down the circumstances of my recruitment by Zacharski in detail so that similarities of what goes on in industry can be recognized. Within the avionics industry, it is a common practice for all companies to obtain the secrets of their competitors by the same technique Zacharski used with me.

Senator NUNN. You mean by that that it is such a common practice in the industry, that when industry people are approached, they are not going to be assured if it is a Soviet company or American company?

Mr. BELL. No, I——

Senator NUNN. You were not under any impression this was another American company?

Mr. BELL. Absolutely, yes, for the first 1½ or 2 years. I considered Polamco, it was a Chicago-based company operating in the United States under the full support of the U.S. Government, under their auspices. Yes, I considered them an American company but I certainly

did not when I started to get into this, I certainly did not. When I was offered a job as a consultant engineer for Polamco, I was interested in getting that job. It was a solution to all my problems.

They were successful, they were clever, very clever.

I sat down the circumstances of my recruitment by Zacharski in some detail so that the similarities of what commonly goes on in the industry can be recognized. Within the avionics industry, it is common practice for all companies to obtain the secrets of their competitors by the same technique Zacharski used with me.

An engineer from one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work—do you want me to repeat?

Senator NUNN. That is all right. Please talk directly into the mike.

Mr. BELL. An engineer for one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work and this is normally done without regard to their security classification. He may also be asked to provide specific documents directly. Sometimes the engineer is hired.

More often he is not. This is generally tolerated because, of course, both companies are American. And they are in competition with each other.

When American companies compete to make sales to friendly foreign governments, a considerable amount of technology is passed in order to make the sale. The companies themselves classify the technology in many cases which they develop under the authority of the Department of Defense. There is a clear conflict of interest between the security responsibility of classifying technology and information and the economic interest of the companies trying to market their products.

A well-known example of this problem occurred with the international competition for the replacements of the aging F-104 NATO tactical fighter aircraft. A memo of understanding was issued by our Department of Defense at this time. It was largely considered by the industry as a license to offer the highest American technology to the Europeans in order to win the contract.

While I was in Europe, I became aware of the impact of the various Communist Parties particularly in France and Italy. This dates clear back to 1958, 1957. I passed through many picket lines of red flags to reach my office at Dassault Aircraft Co. in St. Cloud, France. Many of the employees there were quite frank to tell me that they considered Americans as rabblerousers who had a mania about communism. I was prevented from attending a meeting at the Sylvania facilities in Naples, Italy, by a picket line of red flags. American technology passed to European industries is most certainly the target of Communist infiltration, as well as here.

[At this point, Senator Cohen left the hearing room.]

Mr. BELL. During the international fighter program, including Hughes Aircraft Co., delivered hundreds of drawings, specifications, photographs, and process specifications plus technical operation and performance documents. Thousands of man-hours of technical engi-

neering assistance was provided and teams of European specialists were brought to California for briefings.

All of this transfer was done for the purpose of submitting a planned purpose proposal in pursuit of the contract and to dazzle the Europeans with their technology.

Look down-shoot down radar systems both by Westinghouse and Hughes Aircraft Co. were proposed to the NATO countries, Sweden, Switzerland, Spain, Iran, Israel, Turkey, and Saudi Arabia. Briefings for the proposed sale and construction took place in 1974 through 1975 and following. This, incidentally, was more extensive than the information I passed to Poland 6 years later.

I would like to add the F-14 look down-shoot down radar was delivered to Iran and is still there undoubtedly compromised to the Soviet Union.

On other occasions, the Department of Defense is bypassed. Hughes Aircraft Co., for example, invented a system for very accurate bombing through a TV camera system which could be locked onto a target. This was sold to the U.S. Navy who rightly refused Hughes Aircraft Co.'s application to export it to interested European buyers.

Martin-Marietta, for example, transferred comparable technology to a French company for overseas productions and sales. I was told this was managed by ignoring the Department of Defense and operating directly through the Department of State, after the fact, which they were free to do since they did not have the Department of Defense contract.

Polamco operates openly in the United States as do other Eastern bloc corporations. Zacharski once told me he could ship a radar the size of a small desk to Poland in a machinery case. Incidentally, this is radar weighing 500 to 800 pounds. He had complete access to money and traveled anywhere he wished. Although his phone was tapped and he was constantly watched, the FBI agents never saw him do anything more than run a red light and change lanes illegally.

In light of all my financial and personal problems and my friendship with Zacharski, all of which the company was aware of, my security clearance surely should have been rejected or should have been reviewed. In California, you must renew your driver's license every 3 years. My clearance was 28 years old.

It also seems to me that a random imprint of a coded line running diagonally through a classified document could deter their reproduction. It would serve as a fingerprint to identify the person who is charged out to it and could be read automatically. This certainly would have deterred me. A security oriented classification review should be imposed on the transfer of technology during the sales process. The responsibility for security and profits should be effectively separated.

Every person employed in a security job should know what I did to myself, my loved ones and my country and realized how easy it is to get trapped.

Chairman ROTH. Mr. Bell, did Zacharski represent to you that Polamco was a client of McDonnell-Douglas? If so, why?

Mr. BELL. Yes. Mr. Zacharski showed me a letter that he had on McDonnell-Douglas stationery which was addressed to some subcontractors and I think to whom it concerned, which encouraged the

95-979 O - 82 - 4

subcontractors to do business with Polamco, to buy the machinery and was a glowing report on Polamco. I might add that I learned later that the reason for that letter was that McDonnell-Douglas was competing to sell the DC-10 for LOTT Airlines which was a Polish airline. This was part of the sales campaign.

Chairman ROTH. Were the Polish agents interested in the technology of any other Western nation?

Mr. BELL. Yes. I should add on the last one that Zacharski also had access to the atomic energy facilities in Nevada and various naval shipyards, all of which he had access to or installation of equipment, large machinery, for maintenance of the machinery and for training.

Some of this was done through subcontractors, but his people from Polamco had the access.

May I have the last question?

Chairman ROTH. Let me ask you a followup question.

So what you are saying is that despite the fact that it was common knowledge that Polamco was a Polish-owned company, it was free to compete in this kind of operation, even though it involved technical and classified information?

Mr. BELL. That is true. Polamco was operating in this country under the auspices of the U.S. Government and they are still operating. They have offices in Chicago, their main office, they have offices in Detroit, they have an office on the west coast in the Los Angeles area. They not only have the freedom to operate this way, it permits them to have people travel under the Polamco treasury to wash the money, if you will and it gives them access to various companies around the country operating under the guise of Polamco.

Chairman ROTH. So despite your experience with this organization as far as you know, there has been no limitation or change in the way Polamco operates?

Mr. BELL. As far as I know, that is correct.

Chairman ROTH. Were the Polish agents interested in the technology of any other Western countries?

Mr. BELL. Yes. They asked questions that were directed toward the technology in West Germany.

I believe the reason for this was they told me that they considered Germany as their historical enemy but also they were in economic competition with them and they wanted to maintain a par with their technology. They asked particularly about radar and weapons systems and my company developed and sold the large radar systems.

Chairman ROTH. Did Hughes Aircraft ever participate in joint projects with companies of other nations involving technology transfer? Was technology transfer an important consideration?

Mr. BELL. Yes. We had on many occasions. Probably the best example of it would be the international fighter program that took place in the 1974-75 time period in which they were looking for replacement of the NATO F-104 fighter bomber aircraft. There were several companies competing for that.

The U.S. companies were narrowed down to General Dynamics and Northrop, the European companies were Dassault Aircraft Co. in France, and one in Sweden.

There was a British company, also.

As part of that program, there was a consortium established by the Department of Defense which consisted of Norway, the Netherlands, Belgium, and Denmark, and the United States, five-country consortium. A memorandum of understanding was negotiated and issued which guaranteed an offset program of 60 percent of the equipment we manufactured in Europe and all of the technology. That is the main point, all the technology would be transferred. This was taken by the industry as a license to reveal all of our technology.

We were encouraged to dazzle the Europeans with our technology, with our advanced technology.

Chairman ROTH. You were encouraged by whom?

Mr. BELL. We were encouraged by the prime contractors under the full knowledge of the Department of Defense. I believe it was right for us to interpret this as a license to move out and discuss our technology. I don't believe anybody—I think we all used integrity. They didn't want to cause any harm. But when you get in the heat of competition, engineers are engineers, they are proud of what they do. They meet with their counterparts and they talk. They do talk. Much data was transferred. There is a climate. In this case, a requirement was to produce 60 percent of the system in Europe. Therefore, we had to price it. We could not price it unless they had the information to price. This required us to transmit a great deal of data and a great deal of information to conferences and so on; not only by the winner, but by the losers, as well, and all the subcontractors that were competing to get the award for the airplane.

This was one example. There are many others. This is one example.

Chairman ROTH. Senator Nunn.

Senator NUNN. Mr. Bell, is Polamco still operating in this country?

Mr. BELL. They were operating before I came in mid-December. I understand they are still operating here.

Senator NUNN. How many people do they have working for them?

Mr. BELL. They do somewhere between $30 and $50 million a year in business. In the Los Angeles area I have met and seen perhaps a dozen of their employees, anywhere from technicians up to senior personnel. However, it is important to note that senior executives from Polamco, people who traveled in the guise of senior executives, came to the United States, the Los Angeles area, a guest of Polamco, Polamco was their reason for being here. It was a gimmick to provide direct access in this country for technical people in Europe.

As an example, a good example, I believe, early during the days, perhaps a year and a half after I met Mr. Zacharski, he tried to arrange for a meeting between me and the professor from the University of Warsaw. This meeting was to take place in Santa Barbara. The meeting didn't take place. This didn't take place. I saw no reason why I should meet with the professor from the University. I didn't see how he would be associated with Polamco.

After I became involved, I was again requested on more than one occasion by the agents overseas, they tried to set up a meeting with the professor from the University of Warsaw. Incidentally, the data that I provided, I was assured was going to be held in one place at the University of Warsaw and would have, the access to it would be limited to about six people.

Chairman ROTH. Do you consider Polamco a legitimate company doing business in this country or do you consider it simply as a guise for Soviet spy activities through their proxy?

Mr. BELL. My feeling from what I have seen is that both are true. I think the most important one is this latter one. To me I was convinced when I realized that Polamco was not, perhaps it is—well, it is a Chicago-based company, but when I discovered absolutely for certain that it was under the control of the Polish Government and that they use it as a cover for their secret service operations, there is no question in my mind what they are here for, what they are doing.

[At this point Senator Roth withdrew from the hearing room.]

Senator NUNN. Do you know of any action they have taken against Zacharski since he was convicted of spying?

Mr. BELL. Polamco? Polamco, as a matter of fact, we just heard recently, I heard it—as a matter of fact, through my attorney—is that we have people that are in contact with Barbara, his wife, a lovely lady. She is still receiving the Polamco paycheck.

Senator NUNN. In other words, a Polish company is licensed to do business in the United States. One of their employees has been convicted of spying. He has gone to jail. Yet he is still on the payroll and in jail. Is that true?

Mr. BELL. That is true.

I wouldn't want to restrict it to just one executive. I believe it is deeper than that. As a matter of fact, one of the things which was going to happen the week after Zacharski was arrested, he was going to get me in contact with a follow-on contact. He was leaving for Chicago, moving to Chicago, as president of the company. He was going to get me in contact with somebody who would replace him in the Los Angeles area, which I assume—I, of course, cannot prove this, but my thinking was he would be from Polamco. But certainly Polamco was part of the whole thing.

Senator NUNN. I assumed Zacharski was not president. He was just an employee; is that right?

Mr. BELL. Competition for presidency of that company to replace the man that was president in the fall of last year took place in Poland.

Zacharski was one of the competitors. There was one other man competing. This took place in Poland. In talking to the agents in Europe, I know that this discussion took place within the government. So the government is putting the executives into Polamco.

Senator NUNN. Are you saying the spying efforts of Polamco include people all the way to the top?

Mr. BELL. I am sure of it. Yes.

Senator NUNN. Did Zacharski have any knowledge of the internal affairs of Hughes Aircraft separate from what you may have communicated to him?

Mr. BELL. Yes. I was surprised on several occasions he would know things I didn't understand how he would know about his aircraft company. Like for example, when my boss was changed, he knew that I had a new boss. I don't know how he ever found that out. But more important than that, that he would ask for data, drawings, and the data would be identified in many cases by the identification numbers,

through that identification number; not just Hughes, but one was from another company, such as Westinghouse.

He would have the identification numbers there also.

Senator NUNN. So you knew precisely what they were?

Mr. BELL. They knew precisely what they were. After I knew. They asked me for things which was impossible for me to deliver. As a matter of fact, most of the stuff I delivered was not asked for. I just delivered stuff, things that were available.

Senator NUNN. What kind of technology were they most interested in? What were the military applications?

Mr. BELL. The last thing, for the last few months they were very much interested in the cruise missile; a particular piece of the cruise missile.

I should say I don't know. I don't know anything about the cruise missile. I can only surmise as an engineer. They were asking for what they described as a video correlator. I don't know if I should surmise in this meeting, but except to say that I can see how it would be used on the cruise missile if it is on it. But they were very much interested in it, thinking it was at least a part of the cruise missile, and they thought that maybe Hughes was a manufacturer of that missile equipment.

I don't know if they were or not.

Senator NUNN. Did they ask you to seek employment in other firms so as to broaden their source of information?

Mr. BELL. Yes, they did on more than one occasion, but especially on one occasion. They asked me if I could leave my company and go to work for another company in the United States. They mentioned specifically not a company, but an organization within the Department of Defense. I have already told you what DARPA is. It would be a real key for them where they could have somebody in DARPA, where all the advanced technology work is being done.

They also, on the companies involved, it is my understanding, from previous conversations we had, conversations that led right into them asking me what they were interested in—in the way of companies was Boeing Aircraft Co. and perhaps Westinghouse.

Senator NUNN. Boeing and Westinghouse?

Mr. BELL. Yes. Boeing would be, I am sure, because of the cruise missile. I am not sure why Westinghouse.

Senator NUNN. Did they ever ask you about your level of security clearance?

Mr. BELL. Yes, they did. As a matter of fact, they asked me if I had a top security clearance. They have asked me more than once, but on one occasion they asked me if I had a top secret security clearance and I told them. I lied to them. I said I did.

Senator NUNN. At that time, you did not, though?

Mr. BELL. I did not.

Senator NUNN. Did you give them any information that was labeled top secret?

Mr. BELL. No. I did not. I gave them some secret information on the last two trips.

Senator NUNN. Did you ever turn over to them what is classified as top secret information?

Mr. BELL. No, I never did. It was not available to me. I suppose maybe there is some way of getting it. I don't know. I never tried.

Senator NUNN. Did you try to go beyond your own clearance?

Mr. BELL. No, I did not.

Senator NUNN. Are you suggesting that if every piece of classified information had some special designation that this would have a deterrent effect?

Mr. BELL. Yes, with modern coding techniques you could put random vertical lines through the paper when you print it, before the paper is delivered to the companies so they type on it.

Three or four lines, if they are randomly through there, then you can identify each document with the counter, like you see in a department store or a drug store, this scans over these lines and tells the ratio of distance between them. So they would have a fingerprint. They would know which document, the document signed out by me by the Document Control Center, would have my fingerprint on it. If I tried to pass it, I couldn't photograph it, there is no way of removing those lines without removing the print, it doesn't matter if it is blown up, made smaller, the ratio of distance between the lines still remain the same. If I knew that, if the person knew that, he would think twice before he would do something like this.

Senator NUNN. How would that work on the copies?

Mr. BELL. The same way. The copies, all that can happen is you could make it bigger or smaller, but the ratio of the distance between the lines remains the same.

Senator NUNN. Would you know where the copy came from in terms of the original?

Mr. BELL. You would know where that particular copy came from. I believe—I thought about it extensively—I believe it is something that could be done economically. And I think it should be done.

Senator NUNN. Did you offer to obtain an entire radar system for the Polish agents?

Mr. BELL. Yes, I did, in a sense. They were interested in obtaining a TWT which is a special high-powered radar transmitter, anywhere from 30 to 50 pounds in weight. They wanted one. They were going to ship it back to Poland by machine crates. It has something to do with the Polamco shipping plant, to move equipment back and forth. So I offered them, just testing, to see what they can ship, "Could you, would you be interested in a total system, which would weigh 500 to 800 pounds? It would be the size of a desk." They became very excited about it. Yes, they could handle it. So it shows you the flexibility they have and the power they have, having a company like that operating in the States.

Senator NUNN. Did you carry through on that offer?

Mr. BELL. No; I never delivered any equipment.

Senator NUNN. Did they mention to you how they would handle the equipment, how they would get it out of this country? Was there any discussion of the mechanism if you delivered it, what they would do with it?

Mr. BELL. We had some discussion around the subject where I know they were talking about using Polamco shipping crates or the Polamco shipping channels. Incidentally, this may not be directly associated

here, maybe it is, but they were bringing in vodka and they are bringing it in in the same way. They put it in the machinery. This gives you an idea.

Senator NUNN. Did they tell you how they repair equipment that they may have gotten illegally from the United States or other Western nations?

Mr. BELL. How they would repair it?

Senator NUNN. Yes.

Mr. BELL. No; they didn't.

But I could add a few lines on that if you don't mind.

Senator NUNN. Your opinion? Yes.

Mr. BELL. I know in transferring technology to Europe, any engineer in the industry will verify this, in order to transfer technology to an industry in Western Europe, I have to assume it would be more difficult than Russia, or any Soviet bloc country. It takes thousands of drawings, specifications, it takes a huge amount of data and that is to deliver enough data for them to reproduce it, put it in production. It takes a huge amount of data. Not only that, it takes thousands upon thousands of hours, man-hours of support once they have this data to get the stuff in production. We have had much experience doing this in Western Europe. How in the world the Soviet Union can put something into production when they receive only small amount of data on a sales brochure or even if they had all the drawings, I don't see how they would ever get it into production in the Soviet Union without having at least thousands of man-hours of support.

I believe that if you talk to anybody knowledgeable in this field——

Senator NUNN. You say reversing engineering is very difficult and time consuming even if they have the equipment itself, and all the plans and specifications?

Mr. BELL. To put it in production. That is true. You can get a lot of valuable information off of it. But to put that equipment into production, even if you had what I said, they do not have the components. That is the key to the whole thing.

The best system engineer in the world, that is what we do in system engineering, is only as good as the elements he has to work with. They do not have the components in the Soviet Union. I base that on two things, on what I have seen in Western Europe, I conducted a survey for Hughes Aircraft Co., throughout the industry in Western Europe, and Australia in 1970. I know what they have. They are a generation behind the United States, but they are coming up fast on Western Europe.

I have seen the Soviet Trade Show in Los Angeles. I saw what they had in the way of components and they were 2 years behind. This was maybe 5 years ago. But I have no reason to believe that the Soviet Union component technology is any further advanced than Western Europe.

Senator NUNN. What do you think is the most damaging information that you gave to them? How would you rate it?

Mr. BELL. The most damaging information I gave them was the OPIR, quiet radar data. I gave them a brochure. We were developing, not developing our radar, what we were doing, we had a radar which Hughes has developed on their own money, which DARPA

put money in to modify, to demonstrate the technology which is a quiet radar technology. That is the radar that can operate without being detected by another passive receiver. The document, the sales document that went forward to get that contract I handed over on the last trip to Europe. To me that was the most damaging one, the one I am most ashamed of.

Senator NUNN. What steps would you recommend, based on your own experience, for both Hughes Aircraft and for the Federal Government? I say "Hughes," I don't mean them exclusively, but any company dealing in high technology? What steps other than the ones you have now outlined about the fingerprints, and so forth, would you recommend?

Mr. BELL. I think that when they have people that are in access to classified material, at the level I was, that they should be reviewed more often. I don't think they should be fired. Perhaps we can help them with the problem, all the signals are there, everything. All the classical reasons, a guy is in trouble. I had them. They knew about them. I don't want to pick on Hughes Aircraft. It is a great company. This is true throughout the industry.

Senator NUNN. You are saying the industry should do a lot more themselves if they had more thorough periodic reviews of access?

Mr. BELL. Yes; I think yes; I definitely feel that is true. I believe on the Government's side it is clear, you know. We don't want to be, as Americans, suspicious of our neighbors. We certainly don't want to do that, but gentlemen, the way things are going, if you don't have more control of people coming in Zacharski was a good example. He was given a visa in Poland in 1977, I believe it was. Given a visa when I was told that they knew full well that he was a highly trained Polish intelligence officer.

Senator NUNN. Who knew that?

Mr. BELL. The FBI knew that. They told me that the CIA knew it and the visa was issued. Maybe they had good reason for it. Maybe they wanted to follow it. That sure puts us at a disadvantage. He was placed under surveillance the day he arrived in the United States and when he arrived in California, he was under continuous surveillance there.

As a matter of fact, he was under surveillance before I was guilty, before I had done anything, other than I was in the process of being entrapped.

It would have been so much easier to warn me.

Senator NUNN. But you are saying this passing of very valuable information took place right under the nose of our own law enforcement agencies who had in effect targeted both Zacharski and yourself before the information was passed. Is that right?

Mr. BELL. Yes.

Not only that, it took place over the period of time, on the last trip to Geneva, where I carried the most sensitive data, they followed me. They had a girl, FBI lady follow me into Paris, stay in Paris the few days I was there. They had an agent pick me up in either Paris or in Zurich, follow me to Geneva. But they lost me the day that the thing went down.

Senator NUNN. Did you know they were following you? Did you know they lost you?

Mr. BELL. I only knew after the fact, after they told me. I believe I mentioned two gentlemen they had pictures of, that took place the day before. I went up to the area where the contract was to be, just to look it over, as I was concerned. I was really concerned about as soon as my usefulness became negligible, that I would be eliminated. It is a natural, normal thing, and I was concerned about that. I wasn't particularly concerned in Geneva. I didn't think they would do it there. But I still went up 1 day ahead to look over the contract area. They followed me on that. They had pictures of the two gentlemen.

Senator NUNN. But you didn't know at that time?

Mr. BELL. I didn't know at that time.

Senator RUDMAN [presiding]. Mr. Bell, although you haven't said so in your testimony, you certainly, I think, have inferred that Polamco is something more than a commercial enterprise that recruited you.

Mr. BELL. I will say it. If I didn't say it directly, I will say it now. Yes. I am certain of that.

Senator NUNN. So it would be naive for this subcommittee or the public to feel that because you were the only one who was apprehended, you were the only one that they recruited?

Mr. BELL. When I was apprehended, they came to contact me about Zacharski and I knew, like I say, other times I considered it myself, I had to come to an end some way. I was concerned about doing it in the Los Angeles area because of the rest of my family, because they knew so much about where my family went to school, where we shop. So when they contacted me, it took me a couple of hours to finally do it, but then I told everything, I provided all the evidence, and so on. But with the idea that we would go after the entire operation and shut them all down. That was my understanding. I was assured that was the understanding by some of the agencies I was working with. But then at the last minute they decided because Zacharski was moving to Chicago, he had been appointed, promoted to president of the company.

Senator NUNN. President of which company?

Mr. BELL. He had been promoted to president of Polamco. He was moving to Chicago to take over that position. He was already in Chicago. He had been there for 2 weeks. He had come back on the weekends. His wife was packing up, everything was packed, she was planning on leaving in a week or two and Zacharski was going to come back the following weekend and that would be his last trip when he lived there.

He would be coming back.

Senator RUDMAN. That was at about the time he was apprehended?

Mr. BELL. That is when he was apprehended.

Senator RUDMAN. I would assume that the area you lived in, the apartment complex that you and he chose to live in, housed many employees of Aerospace Co.?

Mr. BELL. Yes.

Mr. Zacharski settled down in the Playla Del Rey apartment complex, which has about 525 apartments in there. There are many employees of the defense industry in those apartments. I don't know all of them. I know some of them. He was constantly trying to meet other ones. I don't know if he was successful or not. I don't know if he moved

in there, I have always thought about this. I would like to know some day, whether he moved in there to get to me or whether it was an accident. We happened to be living there.

Senator RUDMAN. I would assume it was no accident, Mr. Bell.

Mr. BELL. All the signals are there. In fact, when I discussed with the agents in Europe, they were aware that I filed bankruptcy. They had all the information.

Senator RUDMAN. That company is still operating as an agency of the quasi-official agency of the Polish Government?

Mr. BELL. That is correct.

Senator RUDMAN. It has employees in Chicago?

Mr. BELL. That is correct.

Senator RUDMAN. It has employees in Los Angeles?

Mr. BELL. That is correct.

Senator RUDMAN. It has employees, I assume, in other major American cities?

Mr. BELL. In Detroit, for sure.

Senator RUDMAN. Do you know how many employees this Polamco has?

Mr. BELL. No, I don't.

Senator RUDMAN. Would you assume they have a fairly large number or small number? Was it less than 100, do you know?

Mr. BELL. If I had to guess, I would say something over 100.

Senator RUDMAN. The president of this company was indicted, convicted?

Mr. BELL. That is correct.

Senator RUDMAN. He presently is serving time in this country?

Mr. BELL. That is correct.

Senator RUDMAN. Yet, he has been replaced and to your knowledge that company continues to operate?

Mr. BELL. That is correct.

Senator RUDMAN. It is your testimony here this morning, that in addition to legitimate purposes of building markets for Polish products, machinery products in particular, that you believe that his company is devoted to industrial espionage?

Mr. BELL. Yes, they do. As a matter of fact, I may put that first.

Senator RUDMAN. So you think their primary reason may be industrial espionage with the selling of legitimate Polish products and the buying of legitimate American products to export to Poland as being secondary?

Mr. BELL. That is what I believe.

Senator RUDMAN. That is your belief?

Mr. BELL. That is my belief.

Senator RUDMAN. You had more to do with them than anybody else we could talk to. So your belief is important.

Mr. BELL. I want to add that doesn't mean every employee there is involved in this. Certainly the company is the umbrella, is the supporting element that makes it possible for them to do this.

It is under the control of the Polish Government.

Chairman ROTH. Zacharski is still on the payroll of that government?

Mr. BELL. That is correct.

Senator RUDMAN. By virtue of the nature of certain products that they sell and under our country's policy of encouraging free competition, they have access to a number of American defense contractors and in fact a number of American defense installations?

Mr. BELL. Any company which manufactures using machinery is a potential customer to Polamco. They have a reason to go there and to talk to them; to have cocktail parties, to do the things you do when you are trying to talk them out of it.

Senator RUDMAN. It is bad enough that you might have a legitimate Polish company infiltrated by their intelligence people who might have access. We actually give access to a Polish-sponsored company and by virtue of what they sell. They have access at some level to a whole range of American companies?

Mr. BELL. I would certainly believe that to be true. Yes.

Senator RUDMAN. I would certainly say to Senator Nunn that that is something which requires some further looking into.

Mr. BELL. I would, you know we are talking here about Polamco, I would be surprised if it doesn't go further than Polamco.

Senator RUDMAN. I am sure every Soviet bloc country, in fact I know of a number of them which have trading companies.

As a matter of fact, they are moving from the area of which we are speaking. There are a number of other countries with trading companies that do indulge in industrial espionage that has nothing to do with national defense. It has to do with simply other trade secrets. That, of course, is a well-known fact.

Mr. BELL. I believe anything to do with technology involves the national defense, particularly component technology. I think that is where our advantage is over the rest of the world, not just militarily, but economically. We are the leading nation and the reason we are the leading nation is because we have the technology, that is the component technology; the tools of the trade.

Senator NUNN. I might add that tomorrow we will be getting into other companies of this nature, including one Soviet company, direct Soviet company. So it is not just the Zacharski case that we are dealing with. We are dealing with a good many of them.

Senator RUDMAN. I only have one other question unless Senator Nunn has other questions, and after that we will probably dismiss you as a witness today. You stated that companies tended to draw on the employees of other companies in terms of seeking employment, back and forth, and asked them to disclose documents that they had worked on, process, procedures and in fact people would bring classified documents to show the kind of work that they did. Is that correct?

Mr. BELL. That is correct. I think it is well known.

Senator RUDMAN. Common practice even though theoretically the whole security system is based on a need-to-know basis?

Mr. BELL. Right. This is not a—it is a violation of security, but not necessarily illegal.

Senator RUDMAN. Did you have any problems whatsoever of bringing documentation that was labeled secret out of your plant at Hughes to your home for photographing?

Mr. BELL. I'm sorry?

Senator RUDMAN. Did you have any difficulty in removing it from the premises?

Mr. BELL. I did not.

Senator RUDMAN. Was that illegal?

Mr. BELL. That is illegal.

Senator RUDMAN. You were not supposed to remove it?

Mr. BELL. Not supposed to remove it.

Senator RUDMAN. But you never were checked?

Mr. BELL. To be fair with the company, I was a trusted employee. I had been there 30 years. I know I was never checked.

Senator RUDMAN. Obviously, it is the trusted employees that people recruit because of the very nature of what you were doing.

Mr. BELL. Unfortunately.

Senator RUDMAN. Senator Nunn.

Senator NUNN. Thank you very much, Mr. Bell.

We appreciate your cooperation. I think you have made a major contribution to these hearings.

Senator RUDMAN. Thank you very much, Mr. Bell.

The subcommittee now calls Dr. Lara H. Baker, Jr.

Raise your right hand. It is the policy of this subcommittee to administer the oath.

Do you swear the testimony you are about to give in the course of this hearing shall be the truth, the whole truth, and nothing but the truth, so help you God?

Dr. BAKER. I do.

TESTIMONY OF DR. LARA H. BAKER, JR., ASSISTANT OFFICE LEADER, INTERNATIONAL TECHNOLOGY OFFICE, LOS ALAMOS NATIONAL LABORATORY, UNIVERSITY OF CALIFORNIA

Senator RUDMAN. Identify yourself and if you would like to proceed with a summary of your statement, all of which will be included in its entirety in the record.

Senator NUNN. Mr. Chairman, I have a brief introduction of Dr. Baker. Our next witness is Dr. Baker, who has just taken the oath.

He is employed by the Los Alamos National Laboratory. He is one of our Nation's foremost experts on the subject of Soviet computing and Soviet technology in general.

Dr. Baker gives advice to the U.S. military services and intelligence agencies in technical matters. He teaches computer science at the graduate level. He is certainly one of the most informed men in this country on these technology transfer issues.

We are delighted to have him here this morning. We have a much longer résumé which I would ask to be admitted to the record.[1]

Senator RUDMAN. Without objection.

Dr. BAKER. Thank you.

In my testimony today, I would like to followup on Senator Nunn's opening statement in which the Senator constructed, for purposes of discussion, a composite of a department within the Kremlin whose sole function is to obtain strategic and dual-use technology from the United States, Japan, and from other Western democracies.

---

[1] See p. 338 for the statement of Dr. Lara H. Baker, Jr. His résumé and related material follow the statement.

In an interview on March 8, 1982, the Director of Central Intelligence, Mr. William Casey said:

> We have determined that the Soviet strategic advances depend on Western technology to a far greater degree than anybody ever dreamed of. It just doesn't make any sense for us to spend additional billions of dollars to protect ourselves against the capabilities that the Soviets have developed largely by virtue of having pretty much of a free ride on our research and development.
>
> They use every method you can imagine—purchase, legal and illegal; theft; bribery; espionage; scientific exchange; study of trade press, and invoking the Freedom of Information Act—to get this information.
>
> We found that scientific exchange is a big hole. We send scholars or young people to the Soviet Union to study Pushkin poetry; they send a 45-year-old man out of their KGB or defense establishment to exactly the schools and the professors who are working on sensitive technologies.
>
> The KGB has developed a large, independent, specialized organization which does nothing but work on getting access to Western science and technology. They have been recruiting about 100 young scientists and engineers a year for the last 15 years. They roam the world looking for technology to pick up.
>
> Back in Moscow there are 400 or 500 assessing what they might need and where they might get it—doing their targeting and then assessing what they get. It's a very sophisticated and far-flung operation.

Thus, Senator Nunn's composite is basically accurate. There are offices and bureaus within the Kremlin, throughout the U.S.S.R. and throughout the Soviet bloc, whose principal purpose is to transfer high technology from the West to the Soviet sphere of influence.

I will describe several of the vehicles the Soviets use in their efforts to obtain our strategic technology, and then give some examples of how successful they are.

Classical espionage is one of those vehicles. The newspapers are full of accounts of how Soviet and Soviet bloc individuals, some of whom have diplomatic immunity, have been involved with traditional hand-in-the-safe spy rings.

We live in a free society and are proud of that fact. One of our greatest strengths is the information transfer that our Constitution allows and that we encourage among our own people.

Tapping into this information flow is an extremely fruitful technique for the Soviets to use. Also of high importance is the fact that they have been able to tie up a significant quantity of U.S. Government resources. These resources are dedicated to answering Freedom of Information Act requests, checking for downgrading and classification of documents, and evaluating national security implications of compilations of documents.

In our society, one of the most treasured freedoms is free speech. This reaches its epitome in the freedom of organizations to produce periodicals covering whatever they wish to talk about. Information suggests that the Soviets place a very high priority on Western technical journals. We heard that this morning in the first testimony.

Consider the areas of student exchanges.

As part of the spirit of détente, the United States and the Soviet Union entered into student exchange programs. This was a particular coup on the part of the Soviets, since the best technology transfer organization in the world is the U.S. university system. In the U.S. universities, a very large number of highly qualified, highly motivated, superbly trained people spend their working lives trying to come up with better ways to transfer technology to their students.

These people are called university professors. It's their job, and they do it very well.

Currently, approximately one-half of the graduate students in the United States are not U.S. citizens. The non-U.S. fraction for many science and engineering programs is higher. This is particularly worrisome when one considers the quality of graduate education available in the United States.

While there are U.S. Government restrictions on Soviet participation in graduate programs, these restrictions are not applied as stringently to Soviet bloc students, that is, Eastern European students. Thus, the best in U.S. graduate studies is available, albeit indirectly, to the Soviets. This helps alleviate the Soviet problems with training really first-rate engineers.

At several U.S. universities, including MIT and Stanford, one can start a particular program in electrical engineering with a blank notebook; at the end of 1 year, the successful student will leave this particular set of courses holding in his hand a microprocessor chip, a microprocessor being a computer on one integrated circuit.

During that year, the student will have used computer-aided design to design the microprocessor, he will have used computer-aided layout to lay out the processor on silicon, manufactured the chip either in the laboratory or in collaboration with a manufacturer, tested the circuit, packaged the circuit, mounted the microcomputer on a printed circuit board, and made the resulting computer work.

Thus, in 1 year, the student will have been exposed to an intense, carefully orchestrated program covering the U.S. integrated circuit industry.

I find in teaching, many people are not familiar with integrated circuits. I went out this morning to an electronic supply house in Maryland and bought some. I have these available if the subcommittee would like to take a look at them.

This particular kind of circuit is called an Erasable Programable Read Only Memory circuits. If you look inside the window on top of it, you see a three-sixteenths inch square piece of silicon. That square is the circuit.

The small lines leading from that circuit out to the rest of the package are gold wires. There are 24 of those wires bonded to that circuit and bonded to the other end of these prongs.

As you handle these, be careful. The prongs are sharp.

In the area of foreign-owned corporations, the tangled web of ownership of many U.S. corporations obscures the identity of their true owners. Eastern bloc or Soviet-owned corporations can be recipients of U.S. technology without the donors of that technology realizing that the information is going to a foreign government.

In the area of scientific exchange, again, as part of détente, the United States entered into several bilateral agreements with the Soviet Union on various scientific and technical subjects. As part of these agreements, the United States furnished technical information and equipment, such as a superconducting magnet for a Soviet magnetohydrodynamics—MHD system.

This magnet was produced with state of the art U.S. machining and quality control equipment, and was far beyond anything the Soviets

could build for themselves. It was loaned to the Soviets as part of an exchange agreement in return for participation in the MHD experiments.

The loan of the magnet to the Soviets was approved after review by the DOD, the DOE, and various agencies.

[At this point, Senator Rudman withdrew from the hearing room.]

[The letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive hearings without a quorum of two members for the administration of oaths and taking testimony in connection with hearings on the Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations, to be held May 4, 5, 6, 11, and 12, 1982.

WILLIAM V. ROTH, JR.,
Chairman.

SAM NUNN,
Ranking Minority Member.

Dr. BAKER. It was felt that the United States would acquire experience operating the magnet in a facility whose equivalent would not exist in the West before 1986 or 1987. Since all of the U.S. technical reviewers agreed that the Soviets could not reverse-engineer the magnet to acquire the critical manufacturing techniques, the loan was approved.

We did receive return from the exchange but also provided a source of technical equipment to the Soviets.

Business intermediaries: As an area for consideration, business intermediaries, that is, U.S. corporations that act as intermediaries for bloc firms without the manufacturers being aware of such arrangements, are a major source of Soviet covert technology acquisition. The use of these companies provides an open conduit, lubricated by greed, for transferring immense quantities of materiel and technology to the bloc.

The best known—and certainly one of the most successful for the Soviet Union, and perhaps one of the most damaging to the United States—was a business intermediary syndicate headed by a 34-year-old West German named Werner J. Bruchhausen.

I will refer to this as the Continental Technology Corp. or CTC Organization. The CTC scheme was based on his ownership of more than 10 electronics firms in southern California and West Germany and his close ties to other firms elsewhere in Western Europe. The individuals involved would meet with Soviet and Soviet bloc high-technology customers, they would discuss what the Soviets needed, and then would ship the goods, illegally, out of the United States into Western Europe. From there, they were transshipped into the Soviet sphere.

In 1981, part of the syndicate was immobilized and two of its principals brought to trial.

Of particular interest to me in the *Bruchhausen* case is the information it gives us about Soviet intentions. We delude ourselves if we

think the Soviets enter the black market in search of strategic components in a helter-skelter style, buying up dual-use commodities without rhyme or reason.

The truth of the matter is that the Soviets and their surrogates buy nothing they don't have specific, well defined need for. They know exactly what they want—right down to the model number—and what they want is part of a carefully crafted design.

Among the strategic components that Bruchhausen directed his accomplices at the Continental Technology Corp. in southern California to buy for the Soviets were the following:

The information on this laboratory memorandum, I believe, is available. It was made available to your staff yesterday. Included on this list is a summary of the information I sent to Customs.

The U.S. Customs Service and the U.S. attorney in Los Angeles prosecuting the CTC case needed a technical expert to assist them. They chose me. I sent them an expanded version, it turns out to be 60 pages, of this. The defendant's lawyer apparently felt he did not want me on the stand because he stipulated to this information at the trial.

Included in this description are microcomputer development systems, microcircuit test systems, microcircuits, as I have showed you, that sort of thing.

Senator NUNN [presiding]. We will make that part of the record without objection.[1]

It seems that the Soviets are highly organized in their overall espionage, covert-type activities in securing American technology. But we have heard testimony this morning that one of the big problems they have in producing their own technology is their lack of organization.

How do you explain the ability of the Soviets to be well programed, well-informed, know the details of everything they want, have a master plan about how they are going to get it and yet they are not capable enough in their own country of organizing, if that is true, to produce the technology themselves.

Dr. BAKER. I believe their problems in producing the technology includes organization, but I think their main problem is people. There is no incentive in the Soviet bloc to produce quality products. Someone who works in a factory works to generate products; their quality is of secondary importance.

For comparison purposes, the people in the United States who make integrated circuits like this—I have been through their factories where they work—those people are as close to fanatical about the care and precision they use to do their job as any group I have ever seen. I believe there may be basic cultural blocks in the Soviet Union that prevent the motivation of large numbers of factory workers to take this kind of care.

When I ask, how U.S. managers motivate these people, how much they have to pay them, the U.S. managers said it wasn't really money; they said they had to find people who wanted to do a good job and get out of the way.

---

[1] See p. 351 for the material referred to by Dr. Lara Baker, Jr.

Senator NUNN. They must have some incentive systems with the KGB because they are pretty diligent in their work.

Dr. BAKER. The KGB are the elite, as far as I can tell. They get the best people. They do motivate them. They do reward them and thereby get the collection done very well. That is how. They find very good people; they do reward them; that doesn't happen in the rest of the bloc.

Someone who gets in the KGB is well rewarded with high privileges, high status, everything.

Senator NUNN. If they had the incentive system for their engineers that they have for the KGB, they would not have to steal as much technology and could develop their own.

Dr. BAKER. I think that is very true, Senator.

This list of Soviet acquisitions has 60 or so examples but is by no means exhaustive. The equipment is a fraction of the exports; I examined about 400 air waybills. This is the result of 60 examinations.

The Soviets are having serious problems developing their integrated circuit/microcomputer industry, mainly in the areas of process control and quality assurance. The above-mentioned items significantly contribute to the Soviet availability of hardware for developmental and production systems.

There is no question in my mind that the major pieces of hardware purchased from Continental Technology Corp. over the last 4 years of the corporation's operation, taken together, include at least one complete integrated circuit processing plant. This conclusion is ineluctable when you examine the totality of information available on the case. The Soviets purchased everything they needed for such a plant, including: saws for cutting silicon crystals, equipment for making masks for integrated circuit production, plotters to draw the circuits, basic computer-aided-design systems for integrated circuit production, scribers for separating integrated circuits on wafers, testers for testing integrating circuits on wafers, bonding equipment for bonding connecting leads to integrated circuits, and packaging equipment for putting the circuits in final packages. As a result, they have purchased clandestinely all the hardware they need for equipping a good integrated circuit production plant. They showed no interest in purchasing production equipment that was not state of the art. They showed very good taste.

High-quality integrated circuits are the basis of modern military electronics. Integrated circuits form the basis for military systems which are more flexible, more capable, and more reliable than systems using discrete electronic components. The production tooling and equipment obtained by the Soviets will significantly improve the Soviets' capability to produce such circuits.

The Soviets purchased everything they needed for their plant. The sequence in which they purchased things and the quantities indicate the production plant would be of medium size and should be capable of delivering a high-quality product.

Because of the CTC, the United States gave up technology, much of which the Soviets could not have obtained elsewhere. It would have taken them considerably longer to equip the plant, if they could have equipped it at all, with indigenous capabilities.

95-929 O - 82 - 5

What is lost is lost; we cannot get it back. But there is a positive side to the case: It is in what we can learn from it. There is a wealth of intelligence to be learned from the *Bruchhausen* case. It tells us much about Soviet shortcomings and Soviet strengths and their long-term strategic objectives.

As background for this statement, I would like to talk about technology development.

In general, the development of technology can be broken into several areas: Theoretical research, applied research, development, and production.

I would like to look at those areas separately.

The Soviets have historically spent a large amount of their efforts supporting theoretical research. As a result, they have the theoretical basis for almost any technology they wish to exploit.

Experimental research has very slightly less support in the Soviet Union than theoretical research but still, by Western standards, extraordinarily good support. Like theoretical research, experimental research in the West is done by people who are advancing the cause of science and, for that and personal reasons, want to and do, publish extensively. The Western literature is available to the Soviets.

Although their literature is carefully censored, much of it is available to us. In the theoretical and experimental research areas, to varying degrees, the two countries support each other.

In the area of development, this lead is enhanced by the flexibility inherent in the Western political and economic system.

Western countries are encouraged, by tax advantages and simple self-interest, to do research into appropriate areas in order to increase their profits. In the Soviet system, on the other hand, the incentive for doing broad-ranging and possibly risky research is low. The penalty for failure is high. The penalty for failure in the United States is economic and professional, at worst. It isn't always even that, of course. The ready availability of components and technology in the West encourages wide-ranging developmental efforts. There is a true pyramiding effect—we build on each other's work.

The Soviet system in preproduction can manage to produce a few of almost any product they want, provided they are willing to devote the resources to it. The best example of this would be the Soviet "civilian" space program, in which they managed to put people in orbit before the United States did, but at a high cost.

In the area of serial production, that is, the day-to-day production of large quantities of a product, the differences between the two systems become most obvious. The United States is world renowned, and justifiably so, for the quality of its serial production facilities. Other parts of the world, notably Japan, are approaching the United States quality and quantity in this area. The Soviet bloc, however, is not.

Serial production is the Achilles' heel of the Soviet bloc. Especially in high technology areas, the big problem the Soviets have is quality assurance. As I said, they count products, not quality products. This is the area where the Soviets exhibit weakness and need the most help.

As a secondary part of this, they have serious problems manufacturing the tools to manufacture the equipment. This is what the CTC case

helped alleviate by providing a full complement of high quality working production equipment.

In the area of available manpower, one of the serious problems afflicting the Soviet economy is the lack of qualified, highly trained, technical people in the areas of computers and microelectronics. One cause of this is the lack of enough computing and electronic equipment to train the next generation of scientists and engineers. They simply don't have enough equipment to allow students sufficient "hands-on" practice at an early stage in their education. The Soviets are trying to alleviate this problem by producing large, for them, numbers of RYAD computers—copies of the U.S. IBM System 360's and 370's.

Many of the export license requests, both in the United States and elsewhere, are for computer systems going to universities or scientific research institutes in the Soviet bloc. It is difficult to turn such requests down on the basis of end-user since such organizations support the Soviet war machine only indirectly. Cases like the Bruchhausen organization are more obvious. Yet, when I brief various parts of the executive branch on Soviet bloc computing, I find a surprising lack of knowledge of the CTC case. Thus, one of the few public examples of effective compliance action is not widely understood.

Senator NUNN. What do you mean by "effective compliance?"

Dr. BAKER. This is a case where someone actually was exporting equipment, was caught, was convicted, and, most effectively, was put in jail.

Senator NUNN. They did succeed in getting virtually everything they wanted before that punishment took place, did they not?

Dr. BAKER. Yes and no. They got a complete plant, and I think they got everything they asked for up to the time. As far as I know, at the time the organization was shut down, the organization was still going full steam ahead. There was no evidence the Soviets tapered off in their attempts to acquire equipment through this firm. It just happened that the records we had information on—2 or 3 years—showed a complete circuit plant.

Senator RUDMAN. You believe they are capable of maintaining and repairing that equipment and keeping it operative?

Dr. BAKER. For a time. I think they can maintain it, depending on what goes on, for a while by putting very good engineers on it. They are going to have a problem with spare parts. You might consider the equipment as having a half life. That is, after a while, half the systems in the field are going to fail.

Usually four of everything were shipped to the bloc. I suspect two were used in production, two for spare parts. That will help in maintenance quite a bit because they have a working model to go from.

It is necessary that the U.S. intelligence community coordinate information derived abroad with data that surfaces here in the United States. We can discern Soviet objectives in the area of strategic commodities. We can then product with a satisfactory level of accuracy where the Soviets will be trying to tap into technology.

A recently formed interagency committee devoted to this problem will assist in this area.

One cannot prevent the dissemination of data forever; one can only slow down a transfer and thereby make it more expensive for the ad-

versary to acquire the data. Eventually, the adversaries get any information they want badly enough.

In the United States, the most advanced technology is often used in the civilian sector. Fielded U.S. military equipment is often many years behind its civilian counterpart because of the need for greater reliability, delays in the acquisition process, or for other reasons. On the other hand, the Soviet military gets the best, most modern equipment as soon as it is available. Thus, delays in the transfer of high technology to the Soviet bloc affects the military more seriously than it affects the civilian sector. I would like to emphasize that there is no real civilian sector in the Soviet economy—it is all a state enterprise. The military gets the cream of all the production.

The fact that, in the long run, the information will be transferred does not mean we should not control it. Any obstacle we can place in the path of technology transfer increases the amount of resources the Soviet bloc must devote to acquiring the information and decreases the otal quantity of information they receive. Such increases in demand on resources, albeit increases on the seemingly inexhaustible resources of the Soviet intelligence apparatus, are a drain on the Soviet system.

The Soviet system has difficulty in flexibly responding to new information. As a result, the longer information is delayed, the harder it is for the Soviets to integrate it into their production cycle.

Their planning goes on many years in advance, and the inclusion of new technology does not automatically cause a revision in the plan. It may cause an addition to the plan, but not necessarily a reduction in other, less productive, areas. The highly structured environment in the Soviet Union often has a self-defeating result: Factories or enterprises will produce obsolete equipment because they were ordered to although they have the ability to produce more modern equipment and know about the demand for that equipment but have no authority to produce it.

When we know better what the Soviets are attempting to acquire, we can more effectively prevent them from succeeding.

Senator RUDMAN. Again you are making an important distinction in the Soviet system. You said that when they stole this equipment, or detained it by covert means that they were going after state of the art; they knew what they were going after, they had a list of it, they had very good taste, in your words. But you are saying in their own production, in their own capabilities internally, they are not going after state of the art because the system just doesn't work that way; is that right?

Dr. BAKER. Yes, that is my judgment, that is what I see in the open literature and the other information. Serial production for the civilian economy is very low on the totem pole and the military economy suffers somewhat from the same inflexibility.

Many of our control efforts seem to be based on the assumption that we can control everything. We cannot. A more thoughtful enforcement approach is to decide which items are most important to the Soviets and focus our attention and resources on those items.

A key ingredient in the Soviet acquired integrated-circuit manufacturing plant is a high-pressure oxidation system One model of this

kind of system is called by the trademarked name "Hipox." It precisely controls the atmosphere and temperatures involved in the conversion of a wafer of crystalline silicon into a wafer containing several hundred integrated circuits.

Most high-technology components wear out over time. This is where I got my phrase in answer to your question a while ago, "half-life." In general, the higher the technology involved in the system, the shorter the half-life and therefore the greater the demand for spare parts.

The Hipox systems, so essential to the new Soviet integrated circuit factory, should be requiring parts by now. If this system and other critical systems in the plant cannot be serviced the factory will be slowed down or be otherwise negatively affected.

That tells us that the Soviets will soon be in the market for spare parts for the Hipox systems, among others. Only a very few companies in the world manufacture high-pressure oxidation systems. They are all in the West. Each of these companies could be put on notice to be on the alert for false documentation and other signs of CTC type business in their intermediary business.

Senator RUDMAN. Do you see any sign that our Government has organized to do this? You made two important points here, indeed many important points, but two that stand out. You are talking about instead of trying to control everything that involves high technology, they try to have a select group of items they are most in need of and really bear down on that.

Do you see any signs our Government is organized in that direction to make that kind of effort?

Dr. BAKER. There are two encouraging signs in that direction. The first is the Technology Transfer Intelligence Committee which was formed to find out what their real problems are. The second sign is the Militarily Critical Technologies List—MCTL—effort in the Department of Defense, Department of Energy, and other agencies which is an effort to put together a compilation of what technologies are, in fact, critical to us so that we can be alert on what technologies they are going to be after later. Also, later on the MCTL, we can find out the so-called civilian uses, in our case real civilian uses, of certain technologies, and be on the alert for purchases of that kind of civilian equipment which contains military technology. For example, very small turbine engines are used in auxiliary power units for jet aircraft, which is not in itself a critical area, but the technology is very similar to that used on military small turbines.

I do not mean to imply by earlier remarks that many, or even more than a few, of the U.S. industrial manufacturers are venal or unpatriotic enough to close their eyes to this kind of technology theft. However, they are very busy; given prima-facie evidence of respectability, they do not often investigate further. I have every reason to believe that, given a proper warning, the companies would report suspicious inquiries promptly and effectively. In addition, suppliers to these companies can be alerted to potential unusual requests.

This kind of precision targeting for export control requires the availability of accurate technical evaluations of the components and systems involved in an export or diversion. The expertise needed for these

evaluations is a scarce commodity. It is for this reason that the Department of Commerce continually calls upon technical experts from other agencies to review complex export cases.

The Assistant Secretary for Defense Programs, Department of Energy, provides technical expertise and policy guidance to other regulatory agencies with regard to export control matters; this service was also provided by the DOE's predecessor agencies. For example, I am the chairman of the technical task group that is responsible for rewriting the U.S. proposals to the coordinating committee for international control of exports of computers. Other national laboratory experts chair other committees. My group is devoted to computers and directly related items. Also, Department of Commerce licensing officers call laboratory experts, on a regular basis, to request technical advice on complex export cases.

In other forums, I have proposed the establishment of a center of expertise to provide a source of technical information for the various government agencies involved in technology transfer/export control activities. This will go far to help alleviate the scarcity of available technical expertise.

Senator NUNN. Where would that center be housed?

Dr. BAKER. I would like to see it housed in one of the national laboratories which executive department is not critical as long as the center is in a working, thriving laboratory so the people involved in making the export determination are in a state-of-the-art technical environment where they can maintain their skills and not become technically obsolete.

Senator NUNN. How many people and how much money are you talking about?

Dr. BAKER. The first estimate was on the order of 20 people, about $5 million.

Senator NUNN. Per year?

Dr. BAKER. Yes, sir.

Senator NUNN. This would be the center where all the other departments and agencies could go for their advice?

Dr. BAKER. The intent would be to set up a center that provided an honest technical answer. It is not the intent to suggest the center would answer policy questions. That is the province of the executive departments themselves, but it would be useful if there were a place where anybody who needed it, Customs, Commerce, Energy, Defense, could pick up the phone and get an honest technical answer promptly.

With 20 people, there is no way you can cover the field of all disciplines necessary for that kind of a center but you can cover the field well enough to find out who should be asked, so the Government can call one spot and know that the question will be forwarded to the proper person. For things like computers, lasers, the common questions, obviously people should be in the center itself.

In any decision to allow or prohibit the export of a piece of equipment, or a technology, three factors come into play.

First, are the procedural considerations: Are the forms filled out correctly? Are proper concurrences received? Are the overall characteristics of the equipment within appropriate limits, et cetera?

Second, is the technical evaluation of the item to be exported. Is the system truly appropriate for the stated end-use? Are the statements about the end-use/end-user true?

As I have previously stated, the technical evaluation of an export case is a very complex task requiring a particular expertise. The technical evaluation is best made by an individual who is technically competent in the field and who understands the state of the art in the West and in the Soviet bloc. Such individuals are rare.

The third factor in implementing export controls is policy. The policy sets the rules: What we are allowed to export, what we are not allowed to export.

The key consideration among the three factors—procedure, technical, and policy—is the technical evaluation. In fact, policy is usually the result of technical evaluation. For example, a policy that includes a prohibition against the export of certain oscilloscopes is based on the technical evaluation of what national security uses the adversary could make of oscilloscopes. The United States is frequently criticized for having a poorly articulated policy on export controls or, at best, an uncertain policy.

The point may not be as clear as I would like to make it. Let me try to say it another way. I cannot overstress the importance of having an effective system of technical evaluation. To achieve the goal of such an effective evaluation we must optimize three functions.

First, we must be able to look closely at a commodity and be able to assess its capabilities in both the commercial and the military sectors. Obviously, the knowledge of its military uses is critical. That question can be answered only by competent technical evaluation—implying an evaluation done by a technically competent analyst.

Second, we must decide whether or not the stated end-user is who the purchase documents and export documents purport him to be.

For example, is the end-user really a tractor factory or is it a tank factory? That question can be answered only with competent intelligence data. The analysis of such intelligence data requires intelligence expertise as well as technical expertise.

Third, we must assess the adversary's capability to use the commodity in a manner that could harm us. That question can be answered only with detailed technical knowledge and competent intelligence data about the adversary's system.

I would like to conclude my prepared testimony with the recommendation that, in evaluating export controls, the subcommittee take into account the very important distinction between strategic and dual-use equipment versus strategic and dual-use know-how.

Even if our investigative and enforcement capabilities were near perfect, they would still be directed primarily against equipment. In both the law and in the Federal regulations, controls should be strengthened with reference to the know-how that accompanies a product.

If the Soviets clandestinely acquire a piece of equipment, and the equipment works, they have acquired a capability that presumably they did not have before. Along with that equipment, especially if it is high-technology equipment, they need the technical data that goes with it. They need the technical manuals that support the product; they need the technical art that enhances the equipment.

In many ways it may be difficult to control the shipment of technical manuals that accompany manufactured equipment. However, I believe that we can control the art and the support that goes with legally acquired equipment. Showing the Soviets how to make the rope with

which to hang us does not strike me as a reasonable approach for the United States to take.

I thank you very much for the opportunity to testify and I hope that my testimony has been useful to you. I would be happy to try to answer any questions at this time.

Senator NUNN. Thank you, very much. Your testimony has been very useful and we thank you very much for your help.

John Marshall, who will testify after you, talks about the Soviets first equipping the semiconductor plant with manufacturing equipment in 1975.

Mr. Marshall says that by 1977, they will probably be ready to start equipping or testing equipment. Does that square with what you know?

Dr. BAKER. Precisely, sir. In the CTC invoices I saw for the 1978–79 timeframe, they were requiring production equipment and in the 1979–80 time period, they were principally working on test equipment such as complete integrated circuit test systems, handling complete systems and equipment for the plant. Mr. Marshall's data is quite consistent with my information.

Senator NUNN. Why did Assistant U.S. Attorney Wu and the U.S. Customs Service seek you as a technical adviser in the Maluta-title prosecution?

Dr. BAKER. I believe they sought me because of my technical expertise and the fact that they needed help in a very short time. I was called through unconventional channels on very short notice and asked to help support the Customs people.

Senator NUNN. Does the Commerce Department have people available for this kind of technical advice?

Dr. BAKER. I believe so.

Senator NUNN. Was it your understanding that the prosecution's inability to get the needed technical assistance what caused a serious delay in the Government's efforts? Was that one of the reasons you were called?

Dr. BAKER. I would recommend you ask that question of Mr. Wu when he testifies. I was told at the time that they had a serious statute of limitation deadline and were about to be unable to prosecute the cases.

Senator NUNN. What kind of technical assistance was needed for that prosecution?

Dr. BAKER. They needed really two kinds. First, they needed someone to go through the list of equipment that had been shipped overseas and determine which of them were, in fact, illegal shipments; that is, which required licenses and which didn't. That is in essence a licensing officer's kind of decision.

Second, they needed a decision as to the military importance of the equipment being shipped. They needed to have someone who was willing to say, and willing to testify in court to the fact, that a particular shipment or set of shipments was of military importance to the Soviets and made a difference in their military capability.

Senator NUNN. What is the difference between the talents you brought to that prosecution in terms of technical expertise and what the Commerce Department could have brought today?

Dr. BAKER. I can only answer that in terms of the Commerce Department licensing people and experts I worked with and have worked with for about the last 9 years. Those people are very good at making decisions about whether or not something requires a valid export license.

They could have done the first half of the evaluation quite well and told the customs people which equipment was improperly exported and which wasn't, which did or did not require a license.

For the second part of the evaluation, involved with the military significance, I do not believe the expertise exists in the parts of Commerce I have seen.

To my knowledge, the people from the licensing branch could not have answered that question.

Senator NUNN. Is it your opinion that there is no question as to where the ultimate destination of that equipment was supposed to be in the CTC case?

Dr. BAKER. There is absolutely no question in my mind; it went to the Soviet Union. My source for that kind of information was the invoices I saw marked to the principal electronics import-export firm for the Soviet Union in Moscow.

Senator NUNN. In the CTC invoice evaluations, you note the fact that a piece of machinery is either ahead of the state of the art of the Soviets or at least equal to what the Soviets have. What is the significance of that?

Dr. BAKER. To me the significance is that they are buying equipment that they cannot make themselves. They are buying equipment obviously to try to produce in this case integrated circuits, that their current equipment will not make. They were trying to improve their long-term capabilities, they were spending a large amount of very rare hard currency to get the equipment.

It indicates to me that they were trying to improve the military potential by acquiring the production line.

Senator NUNN. Dr. Baker, based on your experience working with the Commerce Department, do you believe that they have access to enough intelligence to properly perform their job?

Dr. BAKER. I would recommend that question be asked to the Commerce people, but the people I work with in Commerce do not have access to all—source intelligence and do not, as a general rule, have access to intelligence at all. I work with licensing people and people who handle cases.

Senator NUNN. Are you familiar with the Commerce Department's own intelligence group?

Dr. BAKER. This last weekend I was given an opportunity to read the staff study before these hearings. Up until I read that staff study, I had no idea Commerce had an intelligence group.

Senator NUNN. You follow this whole area very closely, do you not?

Dr. BAKER. Yes, sir.

Senator NUNN. Does that indicate that since you didn't know that the Commerce Department had an intelligence unit in the compliance division that most other people in this field probably aren't aware of it either?

Dr. BAKER. Certainly the people I work with in the export control of electronics and computers do not or have shown no evidence of being aware; I have never heard it discussed, mentioned, inferred, anything.

I was going to say I am also, as an employee of a DOE laboratory, part of the intelligence community. As a result, I work with intelligence agencies and have never heard it mentioned there either.

Senator NUNN. Does that indicate that the intelligence unit itself is so small or so unknown that it probably is not getting the kind of information it needs from others to have that capability or would you conclude that?

Dr. BAKER. It would appear that the intelligence unit needed to gather information in this field should be larger than the one I saw mentioned at Commerce. Again both CIA and DIA are putting together the units to study this problem.

Senator NUNN. You testified about the intelligence value of the CTC Maluta case; that is, what the United States can learn from the conduct of Maluta and the others.

You are an expert on the technical considerations of the CTC case.

Have you ever been approached by an intelligence person who asked for an evaluation of the CTC case?

Dr. BAKER. No, sir.

Senator NUNN. Do you know anyone else who has? Do you know whether they have really studied that case?

Dr. BAKER. No, sir.

Senator NUNN. If they have, you don't know about it?

Dr. BAKER. If they have, I don't know about it. As I say, I was the technical expert for the U.S. Customs Service and U.S. attorney in this case.

Senator NUNN. You are saying that that case has a wealth of information for our own intelligence experts?

Dr. BAKER. I believe so.

Senator NUNN. So you are certainly recommending that they study that in detail?

Dr. BAKER. Yes, sir.

Senator NUNN. Do you know whether the Commerce Department has had anyone studying that in detail?

Dr. BAKER. I don't know.

Senator NUNN. If they have, you don't know about it?

Dr. BAKER. Correct, sir.

Senator NUNN. Under the best of circumstances if our Government were organized to make good use of technology transfer intelligence, what should have happened as a result of that case?

Dr. BAKER. In the best of circumstances it would have been useful if there were a place for a person like me to go, a single place to explain what I thought had happened and to provide a way to get this information down to the street level, enforcement agencies, quickly in order to get things stopped and/or to draft my decision, follow up a different way. But there was no place to go to that I know of.

Senator NUNN. You referred to the half life of the Hipox oven as being a clue as to when the Soviets expect to be back in the Hipox

marketplace. When should they arrive and what should we do to anticipate it?

Dr. BAKER. I think they ought to be here now. I expect they are trying to get parts for it right now. I would think the best procedure would be to notify the manufacturer and suppliers of that kind of equipment to expect shipments to people they don't know. The integrated circuit business is a surprisingly close knit group.

Most people in that group, because they attend the same parties, go to the same beaches, that sort of thing, know who the suppliers are and would know when the potential diversion could be occurring.

Senator NUNN. Do we have anyone in Government now who is responsible for performing this task; that is, of anticipating what the Soviets may be after next in dual-use technology? Do we have anybody who is primarily responsible for that in Government who should be informed about the CTC-Maluta case? Do you know of an agency or group of people designated for that purpose?

Dr. BAKER. I am not aware of any.

Senator NUNN. That is what you are suggesting, are you not?

Dr. BAKER. Yes, sir.

Senator NUNN. You are suggesting some reverse engineering in the espionage area by the United States in the sense of determining in advance what would be most useful for the Soviets, what they need, what they are most likely to go after and disseminating that knowledge to those who need to know?

Dr. BAKER. Yes, sir. That is a good way to put it.

Senator NUNN. Is nuclear nonproliferation also one of your responsibilities at Los Alamos?

Dr. BAKER. Yes, sir.

Senator NUNN. Has this half life concept worked in our efforts to curtail potential nuclear proliferation problems?

Dr. BAKER. Yes, sir. In one particular instance we had reason to believe that a country would be acquiring some commodities that would be of use in their efforts. The Department of Energy went to the suppliers, mentioned to them "if you get any strange requests for this kind of commodity, please let us know." The suppliers cooperated beautifully. The equipment was not shipped.

Senator NUNN. Dr. Baker, you probably know as much about this subject as anyone we will have before us, perhaps more than anyone. In summary, what are we doing correctly as far as preventing or delaying the amount of technology going out of this country to the Soviet Union? Where would you give the Federal Government high marks?

Dr. BAKER. I understand. A couple or three areas I would give the highest marks to DOE's long-standing efforts in technology transfer control, and the efforts by the CIA and DIA to get into the technology transfer arena much more strongly than they have in the past. Again they are reflecting a requirement of the administration; they work for it, the law requires it; they are going into this area very well. I think they have very good people.

The above refer to analysis and forecasting. In the area of enforcement, the efforts of the U.S. Customs Service, in cooperation with the Justice Department, should be encouraged.

Senator NUNN. CIA and DIA?

Dr. BAKER. CIA, DIA, DOE, and other parts of the intelligence community, are going into it and I think have good people working on it. The militarily critical technologies list will be helpful to us in trying to figure out what areas we need to pay most attention to on our part. If the Soviets are going after something that we don't care about, simply charge them a lot of money, and let them have it. If they are going after something we do care about, we should protect it.

I think these hearings will be useful in publicizing the problem. Most manufacturers I think will be quite interested and quite effective in helping control this problem but many, many people don't believe there is a problem.

Senator NUNN. Where would you give us low marks? You have already talked about your primary suggestion, but how else would you summarize what the Government needs to do?

Dr. BAKER. I would suggest and again this is not my field, I am a technologist, not a Government organization specialist. But working in the field, the lacks I see are the lack of centralized technical support, a lack of, a place to go to get prosecutions done in this kind of a case easily, some place perhaps to gather the information for prosecutions in cases like this and the lack of a mechanism whereby the information that may become available through intelligence or other sources could be quickly gotten to people who need it, to get something done effectively.

Senator NUNN. So it is lack of a concentrated pool of people who have technical capability serving as a central source and as a primary source and also as a clearinghouse source to point to where the knowledge exists if they don't have it. Is that right?

Dr. BAKER. That is correct, sir, either in technology, or in prosecution, or in intelligence. As I say, the intelligence organizations are trying to solve the problems on the intelligence side.

Senator NUNN. You are saying that one area that ought to be looked at is perhaps a national laboratory like Los Alamos?

Dr. BAKER. Los Alamos has done a lot of work in the area; but there are other laboratories who do work in the area. The main thing in providing a technical center, is to get it out of Washington, into areas where there is a high technology environment so you attract the people, keep them busy.

Senator NUNN. Would there be approximately 20 new people and approximately $5 million of new money per year?

Dr. BAKER. That is what I was anticipating. I would expect in the long run that there would be no actual saving of money by the Government in doing this because the people involved in evaluating cases, technically now, would begin evaluating them in their own specialties. For example, the military who have to evaluate cases technically could now not worry about that, but could worry about the military implications.

Senator NUNN. Would there be a lot of people who could be able to feed into this process who would continue in their existing jobs?

Dr. BAKER. That is correct, sir.

Senator NUNN. So you would be having access to a lot more people?

Dr. BAKER. There would be access, more than that number of people; yes, sir. Another reason for putting this center in something

like a national lab, if you need an expert in a particular field, you can go down the hall and get him. Again, this is simply having it away from Washington.

Senator NUNN. Dr. Baker, thank you very much for being with us. Thank you for your testimony and your splendid cooperation and we hope we can continue to call on you as a resource as we frame our recommendation.

Dr. BAKER. Thank you, sir.

Senator NUNN. Our next and final witness of the day is Mr. John D. Marshall. We had planned to have staff statements today but the Senate is going into closed session on the military authorization bill at 2:15, so we will defer our staff statements until tomorrow's hearing.

Mr. Marshall, if you will hold up your hand, I will give you the oath. Do you swear the testimony you will give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. MARSHALL. I do.

Senator NUNN. Thank you. I know you have a statement. We would like to get your statement. Could you give us a little bit of background?

TESTIMONY OF JOHN D. MARSHALL, BUSINESSMAN, SANTA CLARA, CALIF.

Mr. MARSHALL. I have been in the electronics business since 1961. I am a chemist by education, I have been involved in the formation of a number of businesses, both manufacturing of integrated circuits and companies to build the equipment for the integrated circuit industry.

Senator NUNN. Thank you.

Could we have the subcommittee room in order, please?

Mr. Marshall, if you would wait. In just a minute, we will have quiet in the room and you can go ahead.

Senator NUNN. Mr. Marshall.

Mr. MARSHALL. I am a chemist and have been in business in Santa Clara County in a variety of scientific and engineering pursuits since the early 1960's.

One of the businessmen in Santa Clara County whom I had dealings with was Carl Storey, president of II Industries. I had known Carl since 1964. At the time, I had recently sold a business I owned, and planned to start a new enterprise in the near future. But, when I met Mueller, I was more or less between assignments and was supporting myself by working for several firms as a consultant.

Storey told me that Mueller was setting up some kind of semiconductor plant in Hamburg, West Germany. A short time later I learned that Mueller was less interested in actually building a factory but that his main goal was to sell equipment to European semiconductor companies.

Mueller told me that he was doing business with the Soviet Union in regard to equipment for electronic watch production.

In the winter of 1975, I made two trips to Moscow with Mueller. On both trips, the Soviets treated Mueller with special deference. Clearly,

he was someone they had had dealings with before and someone they wished to cultivate.

On the first trip, Mueller and I met briefly with a Soviet named Pavlov. It was hardly more than an introduction, however, and I did not learn much about him. The trip was not very productive.

On the second trip, we met several Soviets who purported to be technical people. They were not very well trained and were not familiar with sophisticated technological thinking. But it was apparent to me by the questions they asked and the subjects they discussed that the Soviets had built a semiconductor manufacturing and assembly plant and they were anxious to equip it. They wanted American semiconductor manufacturing equipment and they had detailed literature on the precise kind of equipment they wanted. They also wanted me to obtain for them certain semiconductor components. It was clear to me that Mueller had deceived me as to the Soviets' intentions, that it was not merely electronic watches that the Soviets wanted to manufacture. It seemed to me they had in mind the manufacture of any number of high technology products, including computers.

I realized that for me to provide such equipment for them would have constituted questionable or illegal conduct on my part. I wanted to play no role in such activity and refused to participate further and left.

Senator NUNN. Did they offer you money or were they just going to use your services and pay you? What was the offer?

Mr. MARSHALL. They really didn't offer me money. Supposedly I was Mueller's employee as a consultant. Mueller offered to pay me my standard consulting fee.

Senator NUNN. You were actually working for him?

Mr. MARSHALL. I was working for Mueller.

Senator NUNN. Did he pay your expenses on the trips?

Mr. MARSHALL. He was supposed to. He didn't pay me.

Senator NUNN. He was supposed to?

Mr. MARSHALL. That's right, he was supposed to pay me and pay my consulting fee. What I really learned through the whole thing, Mueller was trying to prove to the people there that he had some technical expertise and when they started going into areas that were definitely sensitive and I got the drift of really what was going on, I told him I wanted no part of it. And got out.

In addition to the questions the Soviets asked me, I began to better understand certain conversations I had overheard between Mueller and persons he was meeting with during our trips to Moscow. It became apparent to me that Mueller and these persons were involved actively in a relatively substantial effort to buy American semiconductor manufacturing equipment for illegal shipment to the Soviet Union.

Among the persons I met during this association with Mueller was another West German named Volker Nast, who was introduced to me as being one of Mueller's partners. I met Nast in Germany as we were enroute to Moscow. In Hamburg, I met an English or Canadian subject whose name I cannot recall whose mission was to supply the Soviets with semiconductor technology; that is to say, he was to show them how to make integrated circuits and how to use properly the

equipment they would be obtaining. In Moscow, I met a woman who spoke English with a German accent who was planning to ship certain American-made photolithographic materials to the Soviet Union via East Berlin. I do not remember her name.

In 1975, the United States was preeminent in the field of semiconductor technology. It is my view that the Soviets had built their manufacturing plant, or plants, to specifications for American-made equipment—for the manufacture, assembly and testing of integrated circuits. Now that the facilities were constructed, they were, in the winter of 1975, confronted with the next step, which was to equip the facilities.

In 1975, their primary interest in equipment would have related to the manufacture and assembly phases of semiconductor production. By 1977, they would probably have been ready to begin equipping the facilities with the test equipment; and with software development equipment.

Senator NUNN. Thank you very much, Mr. Marshall. We appreciate your being here and your cooperation. We also appreciate your being alerted to what was about to go on and getting involved in that. That is a good example for a lot of other business people who may be exposed to the same thing. Do you know whether Mr. Mueller was ever charged with any crime in this country?

Mr. MARSHALL. I believe he was charged with a crime. In fact, as I mentioned, the gentleman that introduced me to Mr. Mueller was subsequently brought to trial for shipping equipment illegally to the Soviet Union.

Senator NUNN. Is that Mr. Nast?

Mr. MARSHALL. That was Mr. Storey.

Senator NUNN. Mr. Storey, so Mr. Storey was actually indicted and tried?

Mr. MARSHALL. And tried.

Senator NUNN. Was he convicted?

Mr. MARSHALL. I testified at his trial, he was convicted. Apparently there was an incompetent reporter at the trial and so, I guess they negotiated a plea after that. They went to retry. He was convicted at the trial.

Senator NUNN. How about Mr. Mueller, he never has been——

Mr. MARSHALL. Mr. Mueller, I think is a German citizen. I believe he has been indicted but I don't think he is going to come back into the country and I guess you can't extradite from Germany.

Senator NUNN. How about Mr. Nast?

Mr. MARSHALL. Same situation.

Senator NUNN. Indicted?

Mr. MARSHALL. I believe so.

Senator NUNN. In other words, we can't extradite them on those charges as far as you know?

Mr. MARSHALL. In fact that is the information I got from your investigators because I asked these questions of them. They are very aware of the situation.

Senator NUNN. Mr. Asselin, are you familiar with this or Glenn Fry? How about taking the stand and let's complete this part right now.

TESTIMONY OF GLENN W. FRY, STAFF INVESTIGATOR, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

Hold up your right hand, do you swear the testimony you give in this case will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. FRY. Yes.

Senator NUNN. State your name and present position.

Mr. FRY. My name is Glenn Fry, staff investigator for the minority.

Senator NUNN. How long have you been investigating this case?

Mr. FRY. Approximately 1 year.

Senator NUNN. Would you tell us what the status legally is of Mr. Mueller we heard testimony about and Mr. Nast?

Mr. FRY. Richard Mueller is a West German and he initially started to procure American equipment as early as 1974.

Senator NUNN. I don't believe that mike is on. I can't hear you.

Mr. FRY. Is this all right?

Senator NUNN. That is better.

Mr. FRY. Richard Mueller is a West German who as early as 1974 was attempting to procure semi-conductor manufacturing equipment from the United States, specifically two companies on the west coast, II Industries and Kasper Electronics. He tried at first through an individual in Germany named Luther Heidecke who worked for Honeywell A.G. in West Germany. His attempts in this area failed. The next time he was heard of was when he was dealing directly with II Industries and Kasper Electronics.

Senator NUNN. Did he get indicted in this country?

Mr. FRY. Yes; he did.

Senator NUNN. Has he ever been tried?

Mr. FRY. No; he hasn't.

Senator NUNN. Why not?

Mr. FRY. He and Volker Nast both flew to Germany.

Senator NUNN. Both been indicted?

Mr. FRY. Both have been indicted.

Senator NUNN. Has our Government tried to extradite him?

Mr. FRY. There is no way to extradite him for these charges.

Senator NUNN. Why is that?

Mr. FRY. The West German Government is just not sympathetic.

Senator NUNN. Let's say he was a murderer in the United States, what would happen if he fled to West Germany then?

Mr. FRY. I am not that familiar with the extradition laws, but I assume something of that severity——

Senator NUNN. I ask you to have the staff look into this as soon as possible and get us the status of the law as to why this is not an extraditable offense. Your understanding is that it is not an extraditable offense?

Mr. FRY. This is the information we received from Justice and Customs.

Senator NUNN. And the offense he was charged with was violation of the U.S. Export Administration Act?

Mr. FRY. Yes, sir.

Senator NUNN. What about espionage, would that have been an extraditable offense? If you don't know, you can furnish it in a memo?

Mr. FRY. I don't know.

Senator NUNN. I would like to have that in the record. You are going to be testifying tomorrow. Perhaps you can get it by then.

Mr. FRY. All right.

Senator NUNN. We are engaged in a military alliance with West Germany as one of our prime partners. We are spending billions and billions of dollars. The efforts that were being made in this case that you related, Mr. Marshall, were aimed at improving the Soviet military capability. We charge people involved with the crime and they flee to one of our prime allies that we are helping to defend against the Soviets and we can't get them back. Does that strike you as being somewhat of a paradox?

Mr. MARSHALL. It certainly does. I was dumbfounded with the fact we couldn't do anything because I went to the Custom's people and cooperated with the Custom's people in prosecution of this case and found out at that time, too, there was nothing they could do to Mueller. Another thing I found out during the same time was apparently the Russians are also getting a lot of semi-conductor integrated circuit technology from Japan and apparently there is no problem in them obtaining this very sensitive technology from the Japanese and now the Japanese have made very, very substantial strides over the last 10 years and now are just on about a par with our existing technology and seems to me if the Russians want something they can go to the Japanese and get it, no questions asked.

Senator NUNN. Another one of our allies.

Mr. FRY. Japan?

Senator NUNN. Yes.

Mr. FRY. It is.

Senator NUNN. In the defense budget on the floor today, we are spending so much money on our own allies, yet we didn't exercise much effort in terms of agreeing to extraditable offenses with them. If we have I don't know about it. I would like a staff analysis of that.

[At the request of the subcommittee. Dr. Edith Palmer, a senior legal specialist in the European Law Division of the Library of Congress, prepared a report on "Problems of Enforcement of National Security Export Controls Involving Illegal Conduct Abroad." The report follows:]

PROBLEMS OF ENFORCEMENT OF NATIONAL SECURITY EXPORT CONTROLS INVOLVING ILLEGAL CONDUCT ABROAD

Diversions of controlled technology are at times carried out through complicated schemes involving interim exports to West European countries, particularly the Federal Republic of Germany, in conjunction with various forms of transit through neutral countries such as Austria and Switzerland before the goods reach their final destination in the Soviet Bloc.

These schemes hamper enforcement of our national security export controls in two major ways. First, they often involve the participation of foreign nationals operating from abroad who cannot be brought to justice because they are neither extradited to this country nor punished in their home countries. Second, they make discovery of illegal conduct very difficult in that the cooperation of several European countries is required in investigating the facts. This cooperation works well with regard to the Federal Republic of Germany, but the Swiss authorities have in such cases refused assistance. It is also questionable whether cooperation could be obtained from Austria.

An example of the impunity with which foreign nationals violate our export controls is the case of Volker Nast, a national resident of the Federal Republic of Germany. In April of 1976, Volker Nast was indicted by a Federal grand jury

in San Francisco for violation of 18 U.S.C. § 371, conspiracy to violate the Export Administration Act.[1] Even though his conspirators in the United States were prosecuted and convicted, Volker Nast could not be brought to trial because his extradition was not obtained.

In 1980, Volker Nast again participated in a scheme of illegal exports of U.S. technology in violation of the Arms Export Control Act.[2] Through the diligent efforts of the U.S. Customs Service, the illegal export of the controlled item, a Microwave Surveillance Receiver System, was forestalled. Two co-conspirators in this scheme, one a U.S. citizen and the other a German citizen, were apprehended in New York City and were tried and convicted. On May 26, 1981, Volker Nast was charged with a two-count indictment in Baltimore, Maryland, for conspiracy in violation of 18 U.S.C. § 371, and with aiding and abetting an attempt to violate the Arms Export Control Act, in violation of 18 U.S.C. § 2 and 22 U.S.C. § 2778. But because of his German residence he could not be tried.[3] Given Volker Nast's conduct to date, it is foreseeable that he may continue his profitable activities unless ways and means can be found to deter him in the future.

The most effective deterrent for offenders like Volker Nast would be to obtain their extradition to the United States. However, this often will not be possible for various reasons, the most compelling being that the offender is a national of the country that is requested to extradite. In fact, in the Federal Republic of Germany, the extradition of a German national is barred by a constitutional prohibition.[4] This constitutes a preclusion of law justifying the refusal of extradition as provided in Article 7 of the Extradition Treaty between the United States and the Federal Republic of Germany.[5]

Aside from the issue of German nationality, it is not clear to what extent the Federal Republic of Germany under the Extradition Treaty now in force would grant extradition of a U.S. citizen or a citizen of a third country to the United States for violations of U.S. export controls. If the offender were a U.S. citizen, the issue would turn on a finding of double criminality for the conduct.

The intent of the parties is to interpret the Extradition Treaty broadly in order to avoid any possible gaps in the prosecution of crimes.[6] The Treaty obligates the Federal Republic of Germany to grant extradition for any Federal offense under U.S. law that is punishable in the United States and in the Federal Republic by imprisonment for more than one year.[7] It would seem that a good faith interpretation of the Treaty would warrant a German finding of double criminality because German export control laws make the unauthorized export of certain controlled materials punishable by imprisonment up to three years.[8] However, it is by no means assured whether or not a German court invoked to examine the allowability of extradition would come to this conclusion, since German export control laws are not nearly as comprehensive as those of the

---

[1] 50 U.S.C., app. 2401–2420.

[2] 18 U.S.C. § 2; 22 U.S.C. § 2778.

[3] Affidavit of April 5, 1982, of Michael Dolphin, Special Agent, U.S. Customs Service, stating these facts to Glenn Fry and Jack Key of the Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs.

[4] Art. 16, para. 2, of the Basic Law of the Federal Republic of Germany (Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, Bundesgesetzblatt [official law gazette of the Federal Republic of Germany, BGBl.], p. 1.

[5] Treaty Between the Federal Republic of Germany and the United States of America Concerning Extradition [US-FRG Treaty], signed at Bonn, June 20, 1978, entered into force August 29, 1980, T.I.A.S. 9785.

[6] H. Grützner and P. Pötz, Internationaler Rechtshilfeverkehr in Strafsachen II V 10, p. 26, note 2 (Hamburg, 1955–).

[7] Articles 1 and 2, US–FRG Treaty. Article 2 also incorporates as extraditable an enumeration of offenses contained in the Appendix. In the German interpretation of the Treaty, this enumeration prevails only for requests from the United States that are based on offenses under state law, whereas for offenses under the Federal laws of the United States, extraditability is determined by double criminality plus the punishment threshhold. The numerated offenses, however, are indicative of the intent of the Treaty as to the types of crimes covered. Number 27 of the Appendix specifically includes :

(a) Offenses against the laws relating to importation, exportation, or transit of goods, articles, or merchandise.

(b) Offenses relating to willful evasion of taxes and duties.

(c) Offenses against the laws relating to international transfer of funds.

The only category of offenses that is excepted from extradition is that of political offenses. According to Article 4 of the Treaty, the requested State determines whether or not an offense is political. While a German finding of political intent with regard to U.S. export control violations would seem unlikely, given the obvious commercial motives underlying such transactions, violations of U.S. espionage laws would almost certainly fall under the political offense exception.

[8] Secs. 34 and 7, Aussenwirtschaftsgesetz vom 28. April 1961, BGBl. I, p. 481, as amended, in conjunction with secs. 5, 38, 40, 45, and 70, Aussenwirtschaftsverordnung vom 22. August 1961, BGBl. I, p. 1381, as amended.

United States. Criminal sanctions in the German export control system are viewed as exceptional, in view of the free-trade orientation of German foreign economic relations legislation, and most infractions of it are punishable merely by administration fines.[9]

If the United States were to request the extradition of an offender who is a national of a third country for U.S. export control violations, the Federal Republic might refuse extradition if the illegal conduct occurred entirely outside the territory of the United States, since the Treaty, with regard to non-nationals of the requesting country, requires that the requested country must in its own laws have jurisdiction over the type of offense when committed extraterritorially.[10] German criminal law, however, does not list export control violations among the offenses for which it prosecutes foreigners for acts committed abroad.[11]

With regard to persons who are not German nationals, the United States might at times succeed in obtaining extradition when the violators of the U.S. export control laws commit other offenses as well that are extraditable under the Extradition Treaty with Germany. Fiscal offenses and perjury might fall into this category. However, the rule of specialty would limit U.S. prosecution to the offenses for which extradition was granted.[12]

The refusal to extradite nationals is a concept that the Federal Republic shares with many European countries,[13] and this principle is frequently defended by its proponents with the argument that these countries will exercise jurisdiction over their nationals for offenses committed either in their territory or abroad and that they will punish them according to their domestic laws.[14] However, this argument fails to be convincing when, as in the case of export violations, the conduct of the person whose extradition is sought is not punishable in the requested country.

It is a well-recognized principle in international law that a state refusing to extradite a criminal should punish him according to its municipal laws. This principle has been expressed in numerous international conventions dealing with the suppression of crimes, and these agreements frequently contain clauses obligating the member countries to make the reprehensive conduct punishable according to their own laws and to establish jurisdiction in their laws over offenders whose extradition is refused.[15] Whereas these conventions deal with universal crimes for which there is a broad consensus that they need to be suppressed, this may not be the case with regard to U.S. export controls. However, the protection of these controls might well constitute an obligation among the members of the North Atlantic Treaty[16] to protect their mutual security by adopting laws to enforce these controls.

The difficulties of investigating violations of U.S. export controls abroad became especially apparent in 1980, when Theodore Wai Wu, Assistant United States Attorney, traveled to West Germany and subsequently to Switzerland to investigate massive schemes of diverting U.S. controlled technology to the Soviet Bloc involving exports to the Federal Republic of Germany and various forms

---

[9] Aussenwirtschaftsrecht 1975, at 33 (Frankfurt, 1975).

[10] Art. 1, US–FRG Treaty.

[11] Secs. 5 and 6 of the German Criminal Code, i.e., Strafgesetzbuch in der Fassung vom 2. Januar 1975, BGBl., p. 1, as amended.

[12] Art. 22, US–FRG Treaty.

[13] Austria bars the extradition of nationals by a constitutional provision: sec. 12, Auslieferungs- und Rechtshilfegesetz vom 4. Dezember 1979, Bundesgesetzblatt [official law gazette of Austria], No. 529/1979. Switzerland bars the extradition of nationals by legislation: Art. 7, Rechtshilfegesetz vom 20. März 1981, Bundesblatt [official law gazette of Switzerland] I, p. 791.

[14] E. Wise, "Some Problems of Extradition," 15 Wayne Law Review 715 (1969).

[15] Obligations to provide jurisdiction and criminal provisions to punish offenses for which extradition is not granted are contained in: Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague, December 16, 1970, entered into force for the United States October 14, 1971, T.I.A.S. 7192, the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, done at Montreal, September 23, 1971, entered into force for the United States January 26, 1973, T.I.A.S. 7570; Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons Including Diplomatic Agents, done at New York, December 14, 1973, entered into force for the United States February 20, 1977, T.I.A.S. 8532; Single Convention on Narcotic Drugs, done at New York, March 30, 1961, entered into force for the United States, June 24, 1967, T.I.A.S. 6298. Most European countries are also bound by such an obligation according to the European Convention on the Suppression of Terrorism, done January 27, 1977, BGBl. 1978, II, p. 321

[16] Arts. 3 and 4, North Atlantic Treaty, signed at Washington, April 4, 1949, entered into force for the United States August 24, 1949, T.I.A.S. 1964.

of transit through Switzerland and Austria.[17] The West German authorities were very cooperative and their assistance, granted under a bilateral customs agreement,[18] was instrumental in discovering the complex schemes of diversion. But the Swiss authorities denied assistance on the grounds that the country's political neutrality barred assistance for U.S. export control enforcements that are viewed by the Swiss as involving political considerations. They also denied it on the grounds that the Swiss business secrecy laws prohibited certain inquiries. Mutual assistance in criminal matters is granted to the United States by Switzerland under the Mutual Assistance Treaty of 1973.[19] Whereas this U.S.-Swiss Treaty contains broad obligations of assistance, refusals of the type described above are possible because of discretionary clauses contained in its Articles 3 and 10.[20]

Mutual assistance between Austria and the United States is granted on the basis of reciprocity in the absence of a treaty. It is possible that the Austrian authorities would also refuse assistance to the United States for the investigation of export control violations, since the Austrian Law on Extradition and Mutual Assistance contains a general reservation precluding assistance when it would violate essential Austrian interests.[21] Austrian neutrality and business secrets are prime examples of such protected interests in the intent of the Austrian legislature.[22]

National security export controls of the United States cannot be enforced effectively as long as these difficulties in prosecuting foreign offenders and investigating operations abroad continue to exist. These factual problems and the legal situations on which they are based should be taken into consideration by the U.S. Secretary of State in consultation with the Secretary of Defense, the Secretary of Commerce, and the heads of other appropriate departments and agencies when negotiating with other countries regarding cooperation in restricting the export of goods and technology under the Export Administration Act, as provided in 50 U.S.C., app. § 240 (k).

Senator NUNN. Mr. Marshall, during your exposure to Richard Mueller, can you recall the circumstances that led you to believe he was illegally diverting United States technologies to the Soviet Union?

Mr. MARSHALL. While I was with him I began to overhear a lot of conversations he was having with other people and conversations he was having on the telephone which definitely indicated that he was doing this. In fact, as I mentioned, I was a witness for the prosecution of the people in the *II Industries* case because I had some direct knowledge and I guess it was my testimony that was key in getting a conviction.

Senator NUNN. Did Mueller appear to know exactly what United States technology he was to obtain for the Soviets?

Mr. MARSHALL. I believe so.

Senator NUNN. How do you gather that?

Mr. MARSHALL. He was after certain things. In fact, during this time he wanted me to get involved, he was trying to get me to supply, or wanted me to supply some very sophisticated maskmaking equipment. I told him he was nuts, but it was some very sophisticated equipment. He was saying he was going to buy it from West Germany and then move it from West Germany into the Soviet Union.

---

[17] Statement of Theodore Wai Wu, Assistant United States Attorney, Criminal Division, Central District of California, before the Permanent Subcommittee on Investigations, United States Senate, May 5, 1982.

[18] Agreement Regarding Mutual Assistance Between the Customs Services of the United States and the Federal Republic of Germany, signed at Washington, August 23, 1973, entered into force June 12, 1975, T.I.A.S. 8098.

[19] Treaty Between the United States of America and the Swiss Confederation on Mutual Assistance in Criminal Matters, signed at Bern, May 25, 1973, entered into force January 23, 1977, T.I.A.S. 8302.

[20] Article 3 of the Treaty gives the requested state discretion to refuse assistance that is likely to prejudice its sovereignty, security, or similar interests. Article 10 makes the disclosure of business secrets by Switzerland subject to the approval of the Swiss Central Authority.

[21] Sec. 2, AHRG, supra note 13.

[22] R. Linke and H. Epp, Internationales Strafrecht 19 (Wien, 1981).

Senator NUNN. He was making no bones about that?

Mr. MARSHALL. That's right.

Senator NUNN. Did he tell you it was illegal?

Mr. MARSHALL. It was obviously illegal.

Senator NUNN. He knew it was illegal and no question about it?

Mr. MARSHALL. Sure.

Senator NUNN. Did he mention whether money was available for this purpose?

Mr. MARSHALL. Not really. He mentioned they wanted the equipment and I guess he was being rewarded very handsomely by the Russians. He was spending a lot of money, bought two new Mercedes, was in the process of building a very large home in the countryside around Hamburg. So he obviously was doing very well financially.

Senator NUNN. Did he do other things or was he primarily engaged in trying to obtain equipment for the Soviets?

Mr. MARSHALL. I think that was his major job. What he was doing was trying to work under the guise of being a manufacturer's representative for some sophisticated equipment in Europe, and using that as really a guise to obtain the equipment to ship to the Soviet bloc.

Senator NUNN. You gave testimony in a trial involving II Industries and Kasper Electronics, two Silicon Valley firms which pled guilty to violations of the Export Administration Act. Were you familiar with the nature of the equipment that was being shipped for the Soviets?

Mr. MARSHALL. Yes, I was.

Senator NUNN. What was it to have been used for in your opinion?

Mr. MARSHALL. It would have been used for the production of the integrated circuits. It was part of the photolithography process used to make integrated circuits.

Senator NUNN. What about the military applications?

Mr. MARSHALL. The circuits certainly have military application; the equipment has no military application.

Senator NUNN. This is primarily industrial?

Mr. MARSHALL. For production circuits used to print the patterns, the microscopic patterns on the silicon——

Senator NUNN. Does that mean once they produce these they would have been using it for commercial purposes?

Mr. MARSHALL. Commercial or military.

Senator NUNN. Or military?

Mr. MARSHALL. Yes.

Senator NUNN. Members of the minority staff showed you a list of equipment that has been illegally exported to the Soviets over the period 1976 to 1980; is that correct?

Mr. MARSHALL. Yes.

Senator NUNN. These illegal exports were valued at about $10 million. Have you looked at that list?

Mr. MARSHALL. I have seen the list; yes.

Senator NUNN. What type of equipment was this and how would it have been used, in your opinion?

Mr. MARSHALL. Most of the equipment there really broke down into two categories. One category was mainly test equipment, for testing integrated circuits. Another area was software development for de-

veloping software for a particular microprocessor chip, 8080 microprocessor chip. There was, I guess, one piece of equipment there that would be used for the processing of the integrated circuits which was really more advanced than anything that existed during 1975 when Mueller was talking to me. This is a relatively new piece of equipment, the Hipox machine.

So it sounds like maybe they have something going and they are continuing to facilitize it and update it with modern equipment just like a U.S. manufacturer would.

Senator NUNN. Mr. Marshall, based on your experience, do you have any suggestions for the Federal Government as to how to curb technology transfers to the Soviet Union and the Eastern bloc?

Mr. MARSHALL. I listened to Dr. Baker's testimony and his idea about limiting, taking key segments away from them and spare parts for those segments just would be, I think, a very effective way to control it because I think with the proliferation of semiconductor technology as exists in the world today it would be hard to control everything, but I think there are a few key areas that if controlled it would seriously limit their ability to continue to modernize the technology.

Senator NUNN. So you agree with Dr. Baker's suggestions in that respect?

Mr. MARSHALL. Yes, sir.

Senator NUNN. Is there anything else you would like to offer to the subcommittee this morning?

Mr. MARSHALL. No.

Senator NUNN. We appreciate very much your cooperation, Mr. Marshall. Thank you.

The hearings of the Senate Permanent Subcommittee on Investigations on Technology Transfer will continue on Wednesday, May 5, which is tomorrow, at 9 a.m. We will start at 9 o'clock in the morning and catch up with some of the additional information from the staff. We will hear from Jack Vorona, Director, Scientific and Technical Information, DIA; Theodore Wu, assistant U.S. attorney, Central District of California; John Maguire, president of Software A.G., Reston, Va.; Theodore Greenberg, assistant U.S. attorney, Eastern District of Virginia; and Douglas Southard, assistant district attorney, county of Santa Clara, Calif.

We will start with our own staff which has an important analysis of their investigation.

The subcommittee will adjourn.

[Whereupon, at 1:30 p.m. the hearing was recessed, to reconvene at 9:05 a.m., Wednesday, May 5, 1982.]

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

WEDNESDAY, MAY 5, 1982

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met at 9:05 a.m. in room 3302, Dirksen Senate Office Building, under authority of Senate Resolution 361, dated March 5, 1980, Hon. Sam Nunn presiding.

Members of the subcommittee present: Senator Sam Nunn, Democrat, Georgia; and Senator William S. Cohen, Republican, Maine.

Members of the professional staff present: S. Cass Weiland, chief counsel; Michael C. Eberhardt, deputy chief counsel; Katherine Bidden, chief clerk; Eleanore J. Hill, chief counsel to the minority; Gregory Baldwin, assistant counsel to the minority; Jack Key, Glenn Fry, and Fred Asselin, staff investigators to the minority; and Kathleen Dias, executive secretary to the minority chief counsel.

[Senator present at time of convening: Senator Nunn.]

[The letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive hearings without a quorum of two members for the administration of oaths and taking testimony in connection with hearings on the Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations, to be held May 4, 5, 6, 11 and 12, 1982.

WILLIAM V. ROTH, JR.,
Chairman.

SAM NUNN,
Ranking Minority Member.

Senator NUNN. The subcommittee will come to order.

Our first witnesses this morning will be Mr. Fred Asselin, staff investigator, and Mr. Glenn Fry, staff investigator.

If you all would take the stand.

Mr. Fry has been sworn but let's both take the oath again.

Do you swear the testimony you give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. ASSELIN. I do.

Mr. FRY. I do.

TESTIMONY OF FRED ASSELIN AND GLENN W. FRY, STAFF INVESTIGATORS, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

Senator NUNN. I believe both of you have statements this morning and we will ask you to proceed with those.

Mr. ASSELIN. Mr. Chairman, I am Fred Asselin. I am an investigator on the minority staff of the Senate Permanent Subcommittee on Investigations.

I have shortened considerably my prepared statement. I request that my entire 32-page statement be printed in the hearing record.[1]

Senator NUNN. Without objection, your statement will appear as if read.

Mr. ASSELIN. I also have a summary of the CTC-Maluta case that I would request be inserted in the hearing record.

Under the Export Administration Act, the U.S. Department of Commerce, through its Office of Export Administration, has jurisdiction over most nonclassified exports from the United States.

Enforcement of the Export Administration Act is carried out by the Compliance Division of the Office of Export Administration.

The Compliance Division has three Branches—Investigations, Intelligence, and Facilitation—Inspections.

The minority staff of the subcommittee has made an evaluation of the effectiveness of the Compliance Division. An assessment of Compliance Division resources and procedures was made. The minority staff interviewed current and former executives of the Division, and current and former special agents of the Division. Also interviewed were law enforcement personnel from other agencies, Government intelligence officials and officials of agencies whose mission brings them in contact with the Compliance Division.

Uppermost in our minds as we made this evaluation were the national security implications of the responsibility vested in the Compliance Division. The Export Administration Act itself spells out that national security responsibility.

The minority staff also evaluated the Compliance Division in terms of its being a law enforcement entity.

The information that the minority staff has gathered about the Compliance Division was compared to official pronouncements which the Department of Commerce has made about the Division in testimony before Congress and in annual reports to Congress.

The investigation, which lasted more than 1 year, resulted in a series of preliminary findings, which are now submitted to subcommittee members for their consideration. It is our recommendation that subsequent witnesses to these hearings from the law enforcement and national security fields be asked to comment on the minority staff's preliminary findings wherever appropriate.

In reports to Congress, the Commerce Department has portrayed the Compliance Division as if the Division were competently organized

[1] See p. 366 for the prepared statement of Fred Asselin.

and adequately staffed to enforce the Export Administration Act export controls provisions. By contrast, our investigation found that the Compliance Division is not effective. It is an understaffed and poorly equipped and, in certain instances, undertrained and unqualified investigative and intelligence unit.

According to Commerce Department congressional testimony, Department officials "regard the enforcement program as an integral part of the export control system," and say their policy is to "marshal our limited resources to exact maximum compliance with the law."

It is useful to note the reference to limited resources because the staff also will underscore the limited nature of the Commerce Department's commitment to enforcing export controls. Moreover, the staff inquiry concluded that the Department's commitment to export controls enforcement is so limited, in fact, that it is impossible to expect "maximum compliance with the law." It is optimistic to expect very much compliance at all.

Our staff investigation revealed the number of inspectors for the entire Nation is five or six—and five of them are located at the John F. Kennedy International Airport in New York. On a rotating basis, one of the five inspectors is on travel much of the time, trying to conduct inspections for the rest of the Nation. Some airports and seaports never are visited by Commerce Department inspectors in the course of a year. Other exit ports are visited 1 week a year. A sixth inspector is in the Washington, D.C. area.

The Commerce Department's testimony provided this description of the Intelligence Branch of the Compliance Division:

> The Intelligence Branch is staffed with criminal investigator intelligence reporting officers and other support personnel who develop and maintain intelligence information regarding possible export control violations. Branch personnel review all incoming allegations, voluntary disclosures and referrals from the Facilitation Branch to determine whether referral to the Investigations Branch is warranted.

The testimony suggests a much larger operation than actually exists. The Intelligence Branch has a Chief, a Deputy Branch Chief, two full-time professionals and one detailee from the Drug Enforcement Administration.

The Intelligence Branch Chief, who is unique among the three Branch chiefs because of his considerable background in law enforcement, told the staff in a prehearing interview that his office is so overwhelmed with its workload and so understaffed that it is impossible for him to provide the kind of intelligence analysis needed for the Division's national security and law enforcement mission.

The Intelligence Branch is supposed to be able to process and assess sensitive information. Yet, the Branch has no secured telephone. None of its professionals has access to sensitive compartmented information; that is, sensitive intelligence data.

Intelligence Branch personnel often are bogged down in relatively insignificant assignments and do not have the time to collate and synthesize information in an effort to anticipate violations.

In its testimony before the House Committee, the Department went on to describe the Investigations Branch of the Compliance Division by saying it "is also staffed with criminal investigators and conducts full-scale investigations into alleged violations."

The use of the adjective full scale to describe investigations suggests a substantive effort. However, the subcommittee staff was informed by the Chief of the Investigations Branch and by a former Director of the Compliance Division that a full-scale investigation can be a phone call or a letter.

Both, the fiscal year 1980 and 1981 reports to Congress, speak of "full field investigations."

In 1980, Compliance Division special agents conducted 61 full field investigations; and in 1981, an undisclosed number of full field inquiries were made, according to the two reports to Congress. The Branch has about eight investigators. With such limited resources at its disposal, the Compliance Division would be very hard pressed to conduct 61 full field investigations in a 12-month period.

The Chief of the Investigations Branch told the subcommittee staff that 61 full field investigations might not have been the meaning that the report to Congress intended to convey and that there might have been a misunderstanding due to poorly constructed writing in the report.

The testimony also noted that "A principal focus of the Investigations Branch is preventive enforcement. We try to thwart illegal transactions before they occur to avoid possible irreversible harm to national security."

Our investigation revealed that preventive enforcement is far removed from the realistic objectives of the Investigations Branch. The Branch has about eight special agents, some formerly trained in traditional law enforcement, some untrained. Most of their work they do on the telephone or by mail. There is some travel but the bulk of the work is done in the Washington headquarters of the Commerce Department. Investigative support is provided by a three-man field office in New York.

In law enforcement, the term "preventive enforcement" suggests something quite different than an eight-member Investigations Branch that does most of its work from the office. Preventive enforcement means sending agents into the field, staying in close and frequent contact with the many segments of the affected community.

Senator NUNN. Let me ask you a question right there. You talked about several different branches. You mentioned the Inspection Branch. Is that one separate branch?

Mr. ASSELIN. Yes, it is known formally as the Facilitation Branch.

Senator NUNN. Intelligence Branch is another branch?

Mr. ASSELIN. Yes, sir.

Senator NUNN. That is two separate ones there?

Mr. ASSELIN. And Investigations is a third.

Senator NUNN. There is an Investigations Branch?

Mr. ASSELIN. Yes.

Senator NUNN. How about a Compliance Branch?

Mr. ASSELIN. That's it.

Senator NUNN. It's all under one?

Mr. ASSELIN. The Compliance Division has the three branches—investigations, intelligence, inspections.

Senator NUNN. How many people are in the Intelligence Branch?

Mr. ASSELIN. They have a chief, a deputy chief, two full-time analysts and one detailee, so that's five.

Senator NUNN. How many people are in the Intelligence Branch?

Mr. ASSELIN. That's five.

Senator NUNN. Inspection Branch?

Mr. ASSELIN. They have a chief and a deputy chief here in Washington. They have five or six inspectors, five at JFK in New York.

Senator NUNN. How many is that all together, eight or nine?

Mr. ASSELIN. Eight or nine professionals.

Senator NUNN. How about the Investigations Branch?

Mr. ASSELIN. Approximately eight. There is also a three-man investigations office in New York.

Senator NUNN. Which one of those branches is responsible for goods that are going out of the country at the point of departure, like the terminals, the airlines?

Mr. ASSELIN. Inspections presumably, but they are only located at one airport.

Senator NUNN. Are they working with Customs, is Customs supposed to feed information to them?

Mr. ASSELIN. From time to time, they have had a working agreement with Customs. One year they had two Customs people assigned to them. I think that contract has terminated. I think now they are back on their own again. They are supposed——

Senator NUNN. That is patently absured to believe eight or nine people can——

Mr. ASSELIN. It is. It is also absurd to locate them all at one airport.

Senator NUNN. What possible good can you do to visit an airport once a year?

Mr. ASSELIN. That is a very good question. I don't know what they expect to achieve with these random visits.

Senator NUNN. Is it a public relations visit, what is it?

Mr. ASSELIN. We weren't able to establish that, sir, what it is they do when they go to these places.

Senator NUNN. They do not tell you what they do? When you ask the question, what is it you do when you go to the Atlanta Airport or the Miami Airport once a year, what is it you do there?

Mr. ASSELIN. They are supposed to go through shippers' export declarations. They are supposed to carry out——

Senator NUNN. Those that have already gone or those that are going?

Mr. ASSELIN. Those that are going at that moment.

Senator NUNN. That day?

Mr. ASSELIN. Right.

Senator NUNN. It's a random sample, then?

Mr. ASSELIN. Yes, they claim they saw, and it's apparently a viable statistic, 230,000 in fiscal year 1981, which sounds like a lot, but it isn't when you consider there are 9 million SED's filed a year, which means they are missing 8.7 million they do not see.

They see 230,000 and they do not see 8.7 million.

Senator NUNN. That is the written paper, the shipper's export declaration, right?

Mr. ASSELIN. Yes, it's one sheet. It is possible for 5 to 7 men to go through 230,000 of those a year, I guess. They say it's possible and other people have said it's possible.

Senator NUNN. Do they have a computer operation that that is run through, that triggers——

Mr. ASSELIN. They thumb through them. They go to the site and they thumb through them.

Where we wondered about the validity of that figure is in this regard: They also claimed that in fiscal 1981, they found 10,000 discrepancies in those 230,000 SED's. Of the 10,000 or so discrepancies, they actually opened cargo on about 10,000 discrepancies. To do that, they have to first of all call back to Washington to establish whether or not a validated export license is needed—in other words, they have to do some inquiry to check on why there is a discrepancy. Then you begin to wonder how they did 230,000 because it comes down to about—you start dividing 5, or 7 persons into 230,000, you get an awful lot of individual shipper's export declarations they went through and at the same time opening up 10,000 pieces of cargo. So they are a very busy group of people.

It is also interesting to note two or three of them are working 32-hour weeks. They are not full-time employees. I don't doubt their statistics. It just seems to me they work terribly hard, those inspectors. They are grades 5, 7, and 9. Another statistic that may be useful is that 50 percent of the cargo in this category goes out of JFK, which means 50 percent of the Nation's exports in this area are not being seen to the extent that 50 percent at JFK are being seen.

Senator NUNN. Go ahead.

Mr. ASSELIN. In law enforcement, the term "preventive enforcement" suggests something quite different than an eight-member investigations branch that does most of its work from the office. Preventive enforcement means sending agents into the field, staying in close and frequent contact with the many segments of the affected community. Preventive enforcement is aggressive policework.

Equally important, preventive enforcement means having an imaginative and resourceful intelligence capability as well. The Compliance Division has none of these.

The official pronouncements of the Commerce Department reports to Congress and congressional testimony are sharply different from the views expressed by experienced law enforcement personnel who are familiar with the operations of the Compliance Division.

One special agent currently employed in the Compliance Division had served for more than 20 years as an Army criminal investigator and has well established credentials as an agent. He said the Compliance Division is totally ineffective in preventing dual-use technology from being shipped to the Soviet Union. He said the Kremlin's spy organization, the KGB, could not have organized the Compliance Division in a way more beneficial to Soviet interests. This agent's view was not contradicted by persons in the law enforcement and national security field. Unfortunately, it was virtually impossible to persuade these persons to speak for attribution.

Senator NUNN. Why is it you have a department that seemingly does not have the personnel, has been given a vary large mandate, an administration that is very concerned about this problem and yet they do not seem to be willing to admit they have a problem?

Mr. ASSELIN. They won't admit it and it's the worst kept secret in the executive branch.

Everybody knows the inadequacies of the Compliance Division, yet no one will come forward and tell the Congress and speak for attribution in this regard.

As I note later on, we asked the preeminent law enforcement organization in the United States, the FBI, to please help us evaluate this organization. The FBI refused. As recently as last night we asked the Justice Department to please assist us in evaluating this organization. The Justice Department refused. They even insisted on not even being asked the question in open session. I don't know why, to answer your question.

The result of this reluctance to criticize constructively the Compliance Division in public session leads to the current situation in which the only evaluation the Congress hears is from the Commerce Department, which houses the Division and which is less likely to make a candid and forthright evaluation of the shortcomings of one of its own components. For that reason, it seemed important to the minority staff that Congress be informed of the widespread dissatisfaction that exists in the executive branch concerning the Compliance Division and the principal reasons for that dissatisfaction.

The Department of Commerce has as its major focus the promotion of domestic and international trade. It is the finding of the minority staff, based on interviews with officials of the Department and other agencies, that Commerce is not comfortable with the task of limiting the sale of anything, whether it is dual-use technology or some other commodity.

The Commerce Department has devoted insufficient resources to the Compliance Division. In 1967, for example, the intelligence branch of the Division had six or seven professional analysts. Today—15 years later—the intelligence branch has two analysts and one detailee from another agency.

The Department of Commerce, therefore, has reduced its commitment of resources in the intelligence field at the very time when the problem of technology diversions has become more pressing for the country.

Senator NUNN. The Reagan administration and high levels of government are complaining about this problem and saying they are going to really begin to restrict it. Doesn't it seem to be a paradox that the agencies responsible for carrying it out are not able to tell the top people in the Government, including the congressional committees that they have a major problem when the President, their executive branch leader, is apparently very concerned about this problem, very interested in trying to do something about it?

Mr. ASSELIN. Yes, I agree with that and, as I will note later on in the testimony, this has real consequences when a President thinks he has the capability, as we will see on the grain embargo section of this presentation.

The highest leaders of our Nation are led to believe we have an export control capability when, in fact, we don't and they make policy based on a mistaken premise we have the capability, yet we don't have the capability. I will get to that in a moment.

The minority staff is not the only entity that has questioned the depth of the Commerce Department's commitment to regulating technology transfers. In introducing legislation to create an Office of

Strategic Trade, Senator Garn said the Commerce Department can be criticized for its work as "lead" agency in combating diversions. Senator Garn said the Commerce Department has shown itself to be preoccupied with the goal of more and more trade with the Soviets to such an extent that the Department has become blind to national security considerations stemming from the sale of certain kinds of high technology data and machinery.

The result of the Commerce Department's inadequacies in controlling diversions has been a historic erosion in American technological preeminence, Senator Garn said.

The Commerce Department has limited tradition and limited expertise in traditional law enforcement. Yet the Compliance Division is perceived and described by the Department as being a law enforcement organization. Its personnel include special agents, whose titles alone suggest law enforcement assignments. The special agents are classified as series 1811 Federal criminal investigators.

The Compliance Division asserts its "lead" role in enforcing export controls for the entire Government. The Division undertakes exercises requiring specialized law enforcement skills and capabilities such as the conduct of surveillances of suspected export controls violators.

But, because of its lack of tradition and expertise in law enforcement, the Commerce Department does not require that its special agents meet established standards of formal training. "On-the-job" training is common at the Commerce Department; yet there is no requirement that newcomers to the investigative ranks undergo formal training in the enforcement of export controls or in the most fundametal aspects of police work.

The Agent's Manual is a basic instructional document in most law enforcement organizations. Each agent is given a copy of the Agent's Manual and is expected to study it and be fully and currently informed about it.

The Agent's Manual describes proper procedures for the agent in every aspect of his professional life—on points ranging from proper dress to the opening and closing of cases to the writing of reports of investigation.

We asked for a copy of the Compliance Division's Agent's Manual. Its status is not clear. We asked the Acting Director of the Division if we could see it. He gave us a bulky, loose-leaf binder and explained that it was the only such document in the building. We did not think that it was suitable for distribution to and retention by his Special Agents for frequent referral and updating; he concurred.

Another executive of the Division, asked if there was an Agent's Manual, described it as "a semblance of an Agent's Manual."

The absence of a comprehensive, compact and readily available Agent's Manual is reflective of a procedurally uncertain law enforcement environment in the Compliance Division.

Executives in the Compliance Division have had insufficient law enforcement background and training to be supervising investigators on how to proceed in their inquiries.

The Director of the Compliance Division from 1963 to 1979 was a former Customs Appraiser in Chicago with limited experience and limited formal training in law enforcement before he got the job.

He told the minority staff that he did not believe experience or formal training were required for law enforcement work.

He was replaced in the Office of Director of the Compliance Division by a person who also had limited traditional law enforcement experience.

At this time, the position of Director of the Division is formally vacant. It is being filled on a part-time basis by William Skidmore, whose permanent position is Director of Anti-Boycott Compliance. Mr. Skidmore has limited traditional law enforcement experience.

The former Director of the Compliance Division told the minority staff that on several occasions from 1979 through the first quarter of 1982, she recommended to senior officers of the Commerce Department that steps be taken to increase the effectiveness and numerical strength of the Division. The Department rejected many of her recommendations, she said.

Compliance Division inspectors have limited resources at airports and seaports to detect the export of controlled high technology commodities. The chief of the facilitation branch told the subcommittee staff that the number of inspectors—five or six—was insufficient.

Compliance Division inspectors are not authorized to search and seize suspected cargo. They must rely on U.S. Customs service personnel. Similarly, unlike Customs agents and inspectors who have kindred and formalized working relationships with Customs employees throughout many parts of the world, Commerce inspectors have no counterparts on any foreign soil.

Compliance Division Special Agents working in the investigations branch are not required to have any formal training in investigative techniques, law enforcement or the Export Administration Act.

The approximately eight professional members—the Special Agents—of the investigations branch have varying degrees of law enforcement background. Some have extensive law enforcement background. That would number about three of them. Others have limited background in law enforcement. One Special Agent's previous job experience was secretarial.

Most of the investigative work of the investigations branch is done in the office. Agents are expected to conduct inquiry on the telephone and by mail. The most frequent response to allegations of violations of the Export Administration Act is to send the alleged violator a letter of warning.

The subcommittee staff tried to find out the size of the branch's backlog. That was not possible. The chief of the investigations branch said he was not sure how large it was. The previous Director of the Division said the backlog was possibly as large as 300 or 400. The new acting director said he thought it was about 200 cases.

The staff inquiry concluded that a backlog of 200, 300 or 400 cases with an investigative staff of 8 agents seemed to be inordinately large. So many cases hanging over a relatively small investigative staff could create pressure on Special Agents to close cases without sufficient inquiry.

The intelligence branch also has a significant backlog of unfinished business. The chief of the intelligence branch said he had a backlog of about 600 cases. He said that by the end of the calendar year, he could have a backlog of 1,000 cases.

It is the view of the subcommittee minority staff that the backlog—whether it is 600 matters or 600 cases—is too large and its size has an important bearing on the efficiency of the entire Division.

That is because many cases begin in the intelligence branch. A serious backlog there can cause delays throughout the system. Large backlogs prevent the entire Compliance Division from moving in a timely fashion against suspected violators.

Compliance Division investigators have no authority to search and seize shipments suspected of being in violation of the export controls statute. They may detain cargo; however, as the chief of the investigations branch admitted to the minority staff, if the persons in possession of the suspected cargo resist having their shipment detained, Compliance Division personnel have no measure of established force to enforce their decision to detain.

For, coupled with their inability to search and seize is Compliance Division special agents' lack of authority to make arrests. In addition, Compliance Division agents have no authority to carry firearms and have no mobile communication equipment. Yet they carry out surveillance operations of suspected violators.

Several surveillances have been staffed and directed by Compliance Division personnel not extensively trained in the techniques of surveillance work.

In addition, sending unarmed agents on surveillance is a procedure which some law enforcement officials question. Moreover, to conduct its surveillances, Compliance Division personnel have had to borrow mobile communication equipment from the U.S. Marshals Service and other agencies.

Untrained, unarmed, poorly equipped personnel conducting surveillances under the direction of inexperienced executives is a practice inherently risky. It also demeans and trivializes the efforts of formally trained, properly equipped law enforcement agents whose surveillance work is performed according to established procedures. It is the finding of the minority staff that if a surveillance is worth doing, it is worth doing in a professional, procedurally sound manner.

The Division was given the responsibility to investigate violations of the grain embargo. President Carter announced that he had directed the Secretary of Commerce to restrict exports and re-exports from the United States to the Soviet Union.

A former Compliance Division investigator told the subcommittee minority staff that he was given the assignment of investigating embargo violations. He said no other agents in the Compliance Division were assigned to assist him.

At several interagency meetings of high level officials, working on implementation of the grain embargo, the agent, himself a GS–12, was the sole representative of the Commerce Department. His security clearance was at the secret level and this meant that on some occasions he was not allowed to enter the meetings until issues requiring higher clearance were discussed.

The other agencies—USDA, CIA, State Department, Navy—felt the matter was important enough to send senior officers while Commerce was represented by a GS–12, he said.

As for the agent's principal assignment—the investigation of alleged violations of the grain embargo—the agent said he did the best he could with the limited resources he had.

The agent said that for the most part, the majority of his investigative work was from the office, as he relied on long distance telephone calls, cables to American Embassies overseas and assistance from the USDA and Customs.

Senator NUNN. You mean to testify that based on your investigation, the grain embargo that resulted after the Soviets invaded Afghanistan had one person in the Commerce Department checking on violations?

Mr. ASSELIN. Yes, sir.

Senator NUNN. Was any other agency responsible for checking on violations?

Mr. ASSELIN. I spoke with the Agriculture Department official who was chairman of the high level interagency group which monitored the agricultural exports during the grain embargo. He said the group was formed early in 1980 when it became apparent that the Commerce Department was committing insufficient resources to assembling information about compliance and investigating allegations of violations.

He said it was his understanding that "one or two" persons were representing the Commerce Department in this task and that he saw that as a "terribly limited" dedication of personnel. He said information assembled by the high level interagency group reflected a much broader base than the Commerce Department could supply. He said, however, that "the hard core business of proving violations"—that is, the actual investigation—was the responsibility of the Commerce Department.

He said members of the interagency group he chaired talked openly of the unsatisfactory commitment of resources by the Commerce Department. He said he recalled that the Commerce Department sent representatives to the interagency group meetings whose security clearances were not high enough to enable them to be there. He said in certain instances the Commerce Department representative had to wait outside the room until more sensitive issues were discussed.

Senator NUNN. So you have a major decision by the President of the United States on a major foreign policy issue involving the United States and the Soviet Union, involving all our allies, involving the credibility of our foreign policy and economic policy around the world and you have the Commerce Department assigning one individual for enforcement purposes.

Mr. ASSELIN. That's right.

Senator NUNN. And that individual didn't have security clearance high enough to even get in the room when they were talking about high level classified information.

Mr. ASSELIN. He had a secret clearance.

Senator NUNN. He was not cleared for top secret information?

Mr. ASSELIN. No. In fact, the first person Compliance sent over was a Deputy Director of the Division. They refused to even let him in the room until he got a higher clearance.

Senator NUNN. Who is they, the other people?

Mr. ASSELIN. The people at this high level group. The minority staff inquiry found that the inadequate response of the Compliance Division in enforcing the grain embargo demonstrates the serious government operations problem in which the most senior officers of the executive branch, from the President on down shape policy and promulgate directives on the mistaken premise that the affected agencies

95-929 O - 82 - 7

have the necessary means to turn the policy and directives into reality.

Senator NUNN. That really means that the grain embargo in effect was a voluntary program and it was enforced virtually on the honor system, was it not?

Mr. ASSELIN. To the extent it was enforced. I don't mean to suggest there were not USDA and others monitoring, but they found no violations, no one was prosecuted, you had 100 percent compliance in a sense with the grain embargo.

Senator NUNN. If they found a violation, if anybody found it, it would have been up to the Commerce Department to investigate it and they had one person to investigate the whole Nation.

Mr. ASSELIN. Yes; that is the point. And the Commerce Department's commitment was so inadequate right from the very start that that led USDA and others to take a more aggressive role because they were unsatisfied with what Commerce was doing.

President Carter's grain embargo speech might have been received in a different light had he also announced the Commerce Department would assign one man—a GS-12 in the Compliance Division—to investigate alleged violations.

Senator NUNN. Did you find any evidence that the Agriculture Department or the Commerce Department or anyone had informed President Carter that this was the degree of priority Commerce Department was giving the grain embargo?

Mr. ASSELIN. I don't think Presidents are ever told things like that.

Senator NUNN. It's like President Reagan now, when he starts talking about the export of technical equipment that aids the Soviet Union, nobody tells him that they have eight inspectors covering all the airports and ports of the country in enforcing the Export Administration Act; do they?

Mr. ASSELIN. This is precisely the point. The very existence of a Compliance Division sounds as if somebody is there to do the work.

Senator NUNN. Would you say the Commerce Department is fair to both Republican and Democratic Presidents, they treat them pretty much alike?

Mr. ASSELIN. Yes; of course, this goes back about 30 years, that the Compliance Division has been in operation. We have had Presidents of both parties in that period.

Senator NUNN. Of course, you had a great emphasis on it in the last 4 or 5 years. You had two Presidents who expected their major foreign policy decisions would be eminent; have you not?

Mr. ASSELIN. Yes; in fact, the grain embargo was a debated issue in the last Presidential campaign. GAO found that the Soviet Union was largely inconvenienced by the grain embargo. That would be about the extent of it.

Senator NUNN. So really now today we do not have anyone in the Government, any agents in the Government, who can tell us whether the grain embargo was complied with by exporters or not.

Mr. ASSELIN. I think we had 100 percent compliance according to the statistics.

Senator NUNN. But no one was exporting any grain they weren't supposed to.

Mr. ASSELIN. According to the statistics, yes. The agent had 17 cases he looked into. I think there may have been one or two letters of warning.

Perhaps the Commerce Department can fill us in on the extent of the violations, but we found no criminal violations of the embargo.

A lack of close cooperation existed between the Compliance Division and the U.S. Customs Service. The result was that effective enforcement was reduced.

In Customs and in other offices of the executive branch—both in law enforcement and in national security affairs—there is an unwillingness to say anything critical in public about the effectiveness of the Compliance Division. The reluctance to criticize the Compliance Division exists amid a widespread sense throughout affected areas of Government that the investigative capabilities of the Compliance Division are inadequate.

The failure not to criticize the Commerce Department ignores the fact that because of the inadequacies of the Compliance Division significant amounts of dual-use technology that contribute to Soviet military strength are being shipped to the Soviet bloc.

The minority staff should not be the only entity to make an evaluation of the effectiveness of the Compliance Division. It was our hope that other law enforcement organizations would come forward and critique the Division in a constructive and professional manner. In this pursuit, we were met with resistance. Working agents and senior officials alike would be candid, while insisting on their anonymity.

As I said, we asked the FBI to help us, they are the preeminent law enforcement organization in the United States, their views would be most helpful. The Bureau refused, they even insisted on the question not being asked in open session. They said for the Justice Department to answer it. So we asked the Justice Department, "Will you evaluate these people for us?" "No; it's not for us." That is as recently as last night, Senator. So there you are, we are stuck with it. We welcome the opportunity. But the professionals in the field should be asked to make a contribution, too.

Senator NUNN. So the attitude generally is what the President of the United States doesn't know about the inability of his Commerce Department to carry out his own policy doesn't hurt him, right?

What the Congress doesn't know doesn't hurt them.

Mr. ASSELIN. That is a fair surmise, yes, sir,

The subcommittee staff did obtain a copy of a memorandum written by a senior Customs Service officials who was critical of the Compliance Division's procedures. The memorandum, written by William Green, Deputy Assistant Commissioner in the Office of Border Operations, was critical of the Commerce Department on several points, including alleged lack of trained personnel and an alleged counterproductive determination to involve itself in customs work overseas.

The many shortcomings of the Compliance Division as a law enforcement organization are apparent in the investigation of a syndicate of businesses, known as the CTC group, owned, controlled, or utilized by a West German named Werner J. Bruchhausen. Mr. Chairman, I have prepared a summary of the CTC case which was drawn from information provided the minority staff by Commerce Department agents, Customs Service agents, the Department of Justice, and other sources.

It is rather lengthy. I request that it be printed in the hearing record as if read and that I be allowed to give a brief description of what occurred in the CTC case.

Senator NUNN. Without objection, it will be printed as if read.[1]

Mr. ASSELIN. From 1977 to 1980, the CTC network of companies in the United States and Western Europe bought dual-use technology under false pretenses in the United States and then exported it to the Soviet Union and Warsaw Pact. As has been shown in yesterday's testimony by Dr. Lara Baker, the CTC syndicate of companies was not buying up high technology equipment at random. They had been given a precise shopping list by the Soviets. As Dr. Baker pointed out, the equipment the CTC syndicate bought was for the specific purpose of building and equipping a semiconductor plant in the Soviet Union.

Testimony will show that as early as 1975 such a semiconductor plant had been built in the U.S.S.R. and the Soviets were in the process of equipping it with American-made machinery.

The existence of the CTC network of companies was first brought to the attention of the authorities in 1977 and 1978 when two anonymous letters were received at the American Consulate in Dusseldorf. The State Department translated the letters into English and referred them to the Compliance Division in Commerce. The letters were received by the Compliance Division in 1978 and insufficient effort was made to investigate the allegations.

After receipt of the letters, two U.S. producers of dual-use technology reported to the Commerce Department that they were suspicious of the CTC companies. Insufficient inquiry was conducted in response to the first letter.

A Commerce Department special agent did interview CTC's principal executive in Los Angeles, a naturalized Russian-born American citizen named Anatoli Maluta, also known as Tony Maluta and Tony Metz. Maluta told the special agent from Compliance that he did not know anything about export controls, or the need to have validated export licenses to ship certain controlled commodities. But, Maluta said, because of the agent's interest, he was canceling the suspicious order.

No further investigation of the CTC network was conducted until a second letter arrived at the Compliance Division, this time from another high-technology producer who also voiced suspicions about the CTC companies.

Early in 1980, a second Compliance Division agent, Robert Rice, was assigned to the case and conducted the kind of comprehensive preliminary inquiry that was called for. Rice, the most senior agent in the Division, came upon considerable information indicating widespread violations of export controls.

He presented the evidence to the Office of the U.S. attorney in Los Angeles in March 1980. A major inquiry was begun by the U.S. attorney's office, under the direction of Assistant U.S. Attorney Theodore W. Wu and the U.S. Customs Service. Customs ultimately assigned about 15 agents to the case in California, Texas, New York, and Western Europe.

Compliance Division Special Agent Rice was the only Commerce Department representative assigned to the case on a regular basis.

Indictments were brought against Bruchhausen and Dietmar Ulrichshofer, both of whom remain in Europe and are fugitives

[1] See p. 390 for the summary prepared by Fred Asselin on the CTC case.

from American justice, and two Los Angeles accomplices—Maluta and Sabina Dorn Tittel. Maluta and Tittel both were convicted.

The CTC case demonstrated technology diversions of about $10 million and is considered by law enforcement and national security specialists to be one of the most important export control cases ever brought to trial.

The inquiry showed that:

First, the Compliance Division did not move quickly to establish the value of the anonymous letters.

Second, the Compliance Division did not connect the anonymous letters to the allegations that were reported by two U.S. manufacturers.

Third, when Compliance Division Agent Rice turned over the results of his inquiry to Assistant U.S. Attorney Wu in Los Angeles, it was apparent to Wu that considerable expenditures of resources would be needed. Trained investigators would be required to conduct interviews, evaluate shipping documents, surveil suspected violators, and carry out other aspects of a traditional law enforcement full-scale, full field investigation.

Commerce's contribution to that effort was Agent Rice, a competent investigator in whom Wu had confidence. But he needed more than one agent. He enlisted the assistance of the Customs Service. Later assistance was provided by trained criminal investigators from the IRS.

Senator NUNN. So the individual Commerce had working on this was, according to all the opinions, a competent, good investigator?

Mr. ASSELIN. Yes; according to all reports he is one of their best, if not the best.

Senator NUNN. What is his name?

Mr. ASSELIN. Robert Rice.

Fourth, at an early point in the inquiry it was necessary to seize shipments. Commerce had neither the authority nor the manpower to seize shipments. Customs did it.

Fifth, at another point in the inquiry it was necessary to search the premises of CTC companies and the quarters of certain of its employees in the United States and Europe. The Compliance Division had insufficient resources to implement simultaneous search warrants. The Compliance Division had no law enforcement capabilities in Western Europe to work with German customs in coordinating the searches abroad. Customs executed the warrants in the United States and, through its agreements with West German customs, arranged for the execution of the warrants in Germany.

Sixth, to substitute sand for one of CTC's shipments to Moscow, a sizable expenditure of funds was needed. The Compliance Division balked at the shipment substitution strategy and refused to pay the cost of recrating the sand and airfreight. Customs officials approved of the substitution and agreed to pay the cost.

Seventh, extensive overseas coordination, in addition to the search warrants, was called for with West German Customs and other foreign officers. Commerce Department's Compliance Division had no overseas law enforcement contacts. U.S. Customs' contacts were used.

Eighth, extensive surveillance was necessary. Armed Customs agents and armed Internal Revenue Service criminal investigators

and an unarmed Compliance Division Special Agent Rice provided it. Two suspects under surveillance had firearms in the back seat of their car. The firearms were not used. But it was an important law enforcement advantage for the agents on surveillance to be armed as well.

Ninth, experienced supervisors with law enforcement background and training were needed to direct the inquiry in the field. The Office of the U.S. Attorney for the Central District of California, working with supervisorial personnel in the Customs Service, provided the needed direction. Contact with supervisorial personnel in the Compliance Division, who remained in Washington, was made on the telephone and the persons who worked on the case in California did not consider such communication to be satisfactory.

Tenth, When the appropriate time came to apprehend Anatoli Maluta and Sabina Dorn Tittle, IRS agents made the arrests. Customs agents, like the trained IRS criminal investigators, are authorized to make arrests. Even had the Compliance Division dispatched sufficient numbers of agents to assist in the inquiry, they could not have arrested the suspects.

The CTC case does not qualify as a Commerce Department investigation. Customs Service agents did most of the work; and executive supervision was provided by Assistant U.S. Attorney Theodore Wu and Kenneth Ingleby, the Chief of the Customs Service Investigations Office in San Pedro.

In participating in the inquiry on a full-time basis and in conducting himself in a competent, professional manner, Compliance Division Special Agent Robert Rice was handicapped in not being able to do the things Customs agents can do routinely—search and seize suspicious freight, make arrests, and carry a weapon.

Capable and resourceful as he was, Rice cannot be considered to have been essential to the CTC inquiry. It could have succeeded without him. It could never have succeeded without the Customs Service. Customs contributed necessary manpower and fundamental law enforcement tools. Commerce's contribution was Robert Rice.

After the CTC case was brought to Wu, the Compliance Division played no essential role in the inquiry. That recognition leads to the minority staff's final finding, which is that the Commerce Department should not have the enforcement function under the Export Administration Act.

It is the finding of the minority staff that the national security implications of enforcement of the Export Administration Act are too important to be entrusted any longer to the Commerce Department as presently organized.

For three decades the enforcement function has resided in the Commerce Department—through administrations controlled by Democrats and Republicans.

Three decades is sufficient time to allow reasonably capable officials to perfect the most challenging task. But serious procedural and operational problems still exist in the Compliance Division. We find the conclusion inescapable, therefore, that effective enforcement of the Export Administration Act is beyond the institutional capabilities of the Commerce Department. Moreover, from a Government operations and executive organizational standpoint, the mere existence of the

Compliance Division is an impediment to efficient and effective enforcement of the act.

[At this point Senator Cohen entered the hearing room.]

Mr. ASSELIN. Understaffed, flagrantly short of resources, the Division cannot do the job effectively; but, by its presence, prevents other components of Government from taking on the task.

It is our view that two solutions—one short term, one long range—are available.

Immediate relief could be found if the Compliance Division were abolished and all its functions placed in Customs. This action would insure that competent, professional agents, trained in formal, traditional law enforcement procedures, would be assigned to investigate alleged violations of the EAA; that they would work under the supervision of executives who also would have formal, traditional law enforcement backgrounds; and, perhaps most important of all, the entire function would exist in a Cabinet-level Department with long-time experience in and commitment to traditional law enforcement. It is the staff's recommendation that subcommittee members consider that concept as an immediate solution as these hearings proceed.

In addition, in terms of longer range considerations, it is our recommendation that subcommittee members consider the proposal put forward by Senator Garn to create an independent Office of Strategic Trade that, in summary, would absorb the Commerce Department's Office of Export Administration and its components.

Mr. Chairman, that concludes my portion of the staff presentation. I have a series of 27 documents I request be received as exhibits. They start with exhibit 2. I request exhibit 10 be printed in the record.

Senator NUNN. Without objection.

[The documents referred to were marked "Exhibits 2 through 28," for reference, and may be found in the files of the subcommittee. Exhibit 10, as requested, follows:]

EXHIBIT 10

DEPARTMENT OF THE TREASURY,
U.S. CUSTOMS SERVICE,
October 30, 1980.

MEMORANDUM

To: Robert L. Keuch, Associate Deputy Attorney General, Chairman, Inter-Agency Working Group on Export Control.

From: Deputy Assistant Commissioner, Office of Border Operations.

Subject: Response to Request for Assessment of the Inter-Agency Working Group on Export Control (WGCE) Subcommittees' Reports.

In your memorandum dated October 10, 1980, you requested the various WGCE members to comment on the four subcommittee reports which were attached. Given below are my comments, together with some general remarks on particular export control matters which you may wish to consider.

Concerning the subcommittee reports, I have no comments concerning the Intelligence Coordination and Prosecutive subcommittee's reports; except to say that I believe they fairly portray the present situation. I am in agreement with the conclusion and recommendations. The Administrative and Regulatory Procedures subcommittee report also, I believe, fairly portrays the current situation and I support their recommendations. I would, however, like to add two further recommendations. I recommend that a review of the present Arms Export Control Act of 1976 be made with the view in mind of recommending an increase in the penalty provisions and secondly, an addition to the Act empowering Customs officers to make warrantless arrests for export violations.

The present statute provides for a maximum penalty of $100,000 and/or 2 years' imprisonment. Since most of the more sophisticated investigations involve violators who are major corporations, agents of unfriendly foreign powers, international munitions brokers, or members of revolutionary/terrorist groups, the maximum penalty is far too lenient to match the possible severity of the crime. For example, a member of a terrorist group who exports explosives to his compatriots is only subject to 2 years' imprisonment, even though the explosive could cause loss of life and bring about dire political consequences.

Addressing the question of warrantless arrests for export violations, at the present time Customs officers do not have Federal warrantless arrest authority for export violations but must depend on the various state citizens arrest statutes. Fortunately, there is judicial precedence for these warrantless arrests (citizen arrests) for export violations. However, if the authority existed by statute, it would eliminate suppression hearings and result in a savings of time in connection with prosecutions involving warrantless arrests by Customs agents.

It should be noted that both of the above points were discussed in the Ad Hoc (O'Mally) Committee final report and it was recommended that appropriate lobbying for legislative action should take place.

Concerning the final report prepared by the Law Enforcement Coordination Subcommittee, I again find that generally the report fairly portrays the existing situation. There are, however, several observations I would like to make concerning the current enforcement program of the Export Administration Act of 1979.

Throughout the report reference is made to the lack of present-day coordination and the need to improve same. What is particularly significant is Commerce's (OEA/CD) continued action to impede cooperation in investigations even while it states that it wishes to fully participate in all cooperative ventures. Commerce continues to take unilateral and uncoordinated action concerning either joint or Customs initiated investigations by requesting foreign inquiries through various U.S. embassies and consulates without consulting with either Customs Attaches or Headquarters. Such action is causing serious problems. These problems are not limited to hampering instant investigations, but also the compromising of U.S. Customs and foreign government sources, damaging the previously close and long relationships between U.S. Customs and their foreign counterparts, and directly impacting on national security.

These unilateral actions taken by Commerce are not limited to investigations initiated solely by Commerce and being worked only by them; but more importantly, include investigations initiated by Customs and now being either jointly worked by both agencies, or by Customs alone. What is particularly significant is that these unilateral actions have taken place while the Law Enforcement Coordination Subcommittee deliberated and even after the final report was prepared. Attached as an appendix are representative examples of Commerce's action.

While Customs acknowledges that, under the Export Administration Act of 1979, OEA/CD is the agency primarily responsible for administration and enforcement of the Act, OEA/CD is not at this time adequately staffed to enforce the Act. OEA/CD has stated that it is planning to establish foreign offices, together with adequate staffs, and assume those duties related to export control enforcement which the EDO's and Customs Attaches now perform. Once again, OEA/CD is not adequately staffed to assume these duties and does not have experience concerning the conduct of investigations abroad. OEA/CD is also at a distinct disadvantage in that they have no foreign counterparts with whom they can relate and/or work. They will not have access to Customs mutual assistance agreements on which they can rely to gain access to investigative data and/or other desirable information, nor is it anticipated they will be able to establish such agreements. The U.S. Customs Service is in a much better position to conduct export control investigations and inquiries abroad because we do have foreign counterparts with whom we work and relate; we do have formal and informal agreements with our foreign counterparts; we have established foreign offices with a staff of experienced investigators and have conducted export control investigations and inquiries abroad since at least before 1900.

Finally, Customs has maintained a neutral position over the past 2 years on the question of who should assume primacy in the export control enforcement field. It was Customs position that should they state they could do the job better than another agency, the deliberations between the various agencies may degenerate. However, neither Customs nor Treasury ever stated they would be

unwilling to assume additional duties in the export control enforcement area. In fact, Deputy Secretary of Treasury Carswell, in a memorandum to Mr. Brzezinski on February 8, 1980, in response to the Ad Hoc NSC Technology Transfer Group, states ". . . Ideally, a single agency should have all the responsibility and resources for administering the Export Administration Act, including strong enforcement of its criminal provisions. Under current law, this would be the Commerce Department. If, however, the United States desires to intensify and improve criminal enforcement of this statute, then it must look to an agency with worldwide posts and substantial criminal investigative resources already established. Customs has these capabilities. It has offices with investigators in eight major foreign cities; it has experience in performing this function for the State Department under the Arms Export Control Act; and it has a widely dispersed group of agents in the United States For these reasons, transferring the criminal enforcement functions under the Act to Customs is the most realistic alternative if we want to enhance performance in this area, at least as it relates to high technology exports. . . ."

Before any final recommendation is submitted to policy bodies, such as the NSC, concerning who should do what in the field of export control enforcement, I would like to offer several points for thought:

1. Is Commerce (OEA/CD) really equipped today or will they be in the future if they receive their requested additional slots, to conduct sophisticated investigations involving critical technology transfer? Are their investigators trained and as experienced as Customs special agents? Perhaps more important, how long will it take to train them to bring them up to the level that now exists at Customs?

2. Does Commerce contemplate asking for legislative authority to give them powers to arrest, to execute search warrants, to make seizures, and to conduct Customs searches? As you are aware, they do not have such powers now and must rely on Customs.

3. Does Commerce anticipate opening offices in most major cities, which Customs has presently established, so they can quickly respond to matters concerning export control?

4. Would it not be wiser and would it not be more efficient for government operation, to transfer the enforcement functions of the Export Control Act of 1979 solely to Customs, with the licensing and administrative provision remaining with Commerce?

This is not a new concept to Customs as it already does the enforcement duties for the Arms Export Control Act of 1976. State Department (Office of Munitions Control) administers the Act.

The only answer is a single-agency concept for all export control enforcement. While not faulting Commerce in its attempt to increase its enforcement posture, it should be noted that Customs already has the necessary authority, has a foreign presence that has been in place for at least 80 years, has over 60 domestic offices, has over 500 experienced criminal investigators, and has had experience in export control matters since early in the history of our country. Concerning additional resources, it has been stated that if Customs should assume the entire export control enforcement program it would need approximately 25 additional slots. While this figure may change due to exigencies such as workload, source development, and foreign liaison, it should be noted that any new personnel gained because of the resource increase would not be initially assigned sophisticated critical technology cases, but would be assigned to experienced investigators. The new agents would take up the slack caused in lesser areas of the Customs enforcement program.

WILLIAM GREEN.

Senator NUNN. Does Senator Garn's bill, the Office of Strategic Trade, set up a separate department for that or is it under an existing department?

Mr. ASSELIN. As I understand it, sir, it would be comparable to Office of Special Trade Representative. It would be independent. It would not operate within an agency.

Senator NUNN. So what you are saying is, the Commerce Department as the agency to carry out the enforcement of the Export Admin-

istration Act has proved itself inadequate for the task over a long period of time?

Mr. ASSELIN. Yes, sir. As will become apparent when we hear from Commerce and others, they are now opening an office in Los Angeles and an office in San Francisco, each of them to have six slots with supervisors. So they are adding 12 or 13 personnel. That will help. The same people who gave us the Compliance Division as presently organized are the same people who are giving us the two offices in Los Angeles and San Francisco. I think that is a cosmetic attempt to look as if they are enlarging and expanding their capability when it is still inadequate.

Senator NUNN. If Customs took this on, would they have to have a whole new group of people or could the same people in Customs that are working now with some organization also have this responsibility?

Mr. ASSELIN. According to the Green memorandum of 1980, that we read into the record this morning, Customs would have to add 25 persons. They will have to add more than that. However, the capability is there. That is the point, the law enforcement capability. However, they have overseas people, they have trained investigators. The cost will never be the same, will never equal the amount Commerce——

Senator NUNN. In other words, if Commerce were to do this job right, they would have to add hundreds of people, they would have to add administrative staff that knew about law enforcement, they would have to have top people in the Commerce Department who were trained for law enforcement which is not the case now. You are simply saying the Customs agents and Customs Service can do it much more effectively and sufficiently and utilize what they already have out there now?

Mr. ASSELIN. Yes, sir, everywhere you have to put this enlarged Commerce operation, Customs is already there. You would have to put Commerce people overseas.

Senator NUNN. So Commerce would have to duplicate Customs to——

Mr. ASSELIN. Almost in every instance. Where there is a Customs man now, you would have to have Commerce. Why do you have two agencies in the field even if they were doing a good job, when one agency would suffice?

Senator NUNN. You are saying there are some good people in the Commerce and Compliance Division that could be shifted over?

Mr. ASSELIN. Yes; that is certainly true and Rice is certainly one of them. He would be a good contribution to customs.

Senator NUNN. Senator Cohen, we just had a complete staff statement which is very explicit on the problems in the Commerce Department in enforcing this act with a recommendation from the minority staff the Compliance Division be abolished and put in the Customs Service. Do you have any questions or observations?

Senator COHEN. What are the total number of inspectors we have available now?

Mr. ASSELIN. In Commerce?

Senator COHEN. In Commerce.

Mr. ASSELIN. Five.

Senator COHEN. Five inspectors.

Senator NUNN. I think you ought to make a distinction now because there are three separate parts of the Compliance Division.

Mr. ASSELIN. The Compliance Division has three entities in it. It has an Inspections Branch which has five or six. It has an Investigations Branch which has 8 to 11 persons and it has an Intelligence Branch which seems to have 3 to 5. That is the extent of the professional enforcement capability of the Commerce Department.

Senator NUNN. Five or six of all their inspectors are in New York.

Mr. ASSELIN. At the JFK airport.

Senator NUNN. The others they don't visit other ports——

Senator COHEN. How many exit points do we have in the United States?

Mr. ASSELIN. I don't know, Senator. It is more than they could ever handle with five.

Senator COHEN. I understand. I am trying to draw it in its dramatic——

Mr. ASSELIN. I don't know the answer to that.

Mr. FRY. The customs started a program called Exodus to enforce violations of the Export Administration Act. It is my understanding they have a minimum of 7 to 10 special agents at the 10 major ports throughout the United States assigned to this type of operation. I am not certain as to the number of inspectors but the inspectors are permanently located at these 10 major ports.

Senator COHEN. How many international airports, for example, do we have?

Mr. ASSELIN. I don't know. I do know these figures: They say 50 percent of the traffic goes out of JFK, so it is not surprising they put their principal focus at JFK. But they cover no other airport.

Senator NUNN. You have more international airports now than you did. They are expanding. A lot of international flights go out of Atlanta, out of Boston, they are out of Dulles, they are out of San Francisco, Los Angeles, and Chicago.

Senator COHEN. Bangor.

Senator NUNN. Bangor is next on the list.

Mr. ASSELIN. There is a paragraph I deleted in shortening my statement, if I may read it. The Acting Director of the Compliance Division acknowledged to us there were problems in the operation of the Division. He said the problems could be corrected but that such a process takes time. Elaborating on this point, he said the Government has slowly changed. He said the Compliance Division was organized more than 30 years ago at the time when the challenge of export controls is not as great as it is today. But he said as export controls became more of an urgent problem to the United States in recent years, the Compliance Division tended to remain about the same.

We asked the Acting Director if the Nation could afford to wait while the Commerce Department and its Compliance Division adjusted to the new challenges in export controls. He had no answer to that inquiry but he did say it was a valid question. So it is true, the problem has risen and gotten much bigger but Commerce has not risen with the problem.

Senator NUNN. Senator Cohen, one other interesting thing I found astounding when I first heard about it several months ago and I kept asking the staff to check on it and check on it because I couldn't believe it. Staff testified today that the Commerce Department, which was responsible for investigation of violations of President Carter's grain

embargo, had one person working on that and it turns out there was 100 percent compliance with the grain embargo according to statistics.

If we could get that one guy over there in the Internal Revenue Service, we could balance the budget.

Senator COHEN. Well, he may have had the same inflated reporting system we have as far as projecting what the inflation is, I believe. Let me just ask one other question since I don't know whether the staff covered this in your presentation, are there any restrictions on what can be labeled as protected under diplomatic pouch?

Mr. ASSELIN. Senator, we didn't get into that. I don't know the answer to that.

Senator COHEN. It seems to me I have been seeing some reports about how easy items can be shipped under the protection of diplomatic pouch. I just wonder if you had any information on that?

Mr. ASSELIN. I don't know the answer, sir.

Senator COHEN. That is all.

Senator NUNN. Mr. Fry?

Mr. FRY. Mr. Chairman, my name is Glenn Fry, staff investigator for the minority. I would like to summarize my statement if I could but I would request the entire statement be entered into the hearing record as if read.[1]

Senator NUNN. Without objection.

Mr. FRY. The Commerce Department's ineffective response to the challenge of technology transfer is an illustrative example of the failure of the Government, in general, to organize itself effectively to remedy this national security problem.

We have learned of the shortcomings in the Commerce Department's efforts to investigate violations of the Export Administration Act thereby causing a serious deficiency in its ability to enforce the statute and its regulations. The law enforcement effort, although critical, is only a part of the overall effort to prevent the harmful flow of U.S. technology. Even if the law enforcement operation were professionally administered with sufficient resources, its effectiveness would continue to suffer due in part to deficiencies within other executive branch agencies.

The Commerce Department is mandated to administer and enforce the Export Administration Act; however, matters concerning this act which involve national security interests, require the consultation of the Department of Defense, and the intelligence community as well as Commerce. Ineffective control of the transfer of U.S. technology and the enforcement of export laws will prevail if the Department of Defense and the intelligence community continue to provide less than their best efforts to support this national security mission. Despite several previous congressional investigations and hearings conducted on these matters, dating back to 1974, the responsible executive branch agencies continue to have difficulty in organizing an effective operation.

Technology transfer can occur through the illegal export of controlled or embargoed commodities; however, it can also occur with

[1] See p. 426 for the prepared statement of Glenn W. Fry.

equal damage, because of inadequate control and protection of critical information and through ineffective handling of legitimate export licensing cases. The minority staff has made preliminary findings that the technology transfer programs of the Department of Defense and the Intelligence Community contain basic deficiencies which impair the Government's overall effort to control the flow of critical American technology.

The following are areas within the Defense Department's program that demand attention and ultimate resolution if the Government intends to control the flow of U.S. technology:

First, the Freedom of Information Act is a legal tactic available to U.S. citizens, foreigners, and even Soviet surrogates to obtain critical dual-use technology. Dual-use technology, which can be used commercially and militarily, is not excluded from Freedom of Information Act requests. There is no protection or means to control the harmful transfer of technology that does not fall within the exclusions prescribed by the Freedom of Information Act.

Second, there have been instances where classified information has been prematurely declassified in accordance with an automatic declassification schedule. In other instances, critical technologies which have military significance are never classified. In either case, the end result is that such information, although not readily distributed, becomes available to anyone.

The Department of Defense's Office of Research and Engineering and International Security Policy are responsible for the review of export licensing requests for national security interests. Presently, Defense reviews predominantly those export cases involving the Soviet Union or Warsaw Pact nations. There is very little review of free world license requests except for cases involving very advanced computer technology. The program presently administered within the Department of Defense suffers from several fundamental deficiencies.

First, on August 26, 1977, the Secretary of Defense issued an interim policy statement for the export control of U.S. technology. Today in 1982, there has yet to be any followup to this interim policy. This is representative of the weak overall priority afforded the technology transfer issue throughout Government. Sources within Defense has indicated that there is ambiguity regarding which DOD office has overall accountability for technology transfer decisions.

Second, the Office of Defense Research and Engineering does not have an adequate number of permanent staff specialists to effectively conduct its technology transfer mission. Temporary personnel have been assigned to this office; however, there is an annual turnover. Consequently, much valuable time and resources are continually used to train and familiarize new personnel rather than attend to its primary responsibilities.

Third, military and Department of Defense research laboratories who are tasked by Defense Research and Engineering to review licensing cases lack a charter delineating export control or technology transfer responsibilities. There is also no specific funding for this type of operation. Consequently, technology transfer issues are not a priority and do not receive appropriate attention.

Fourth, there is no adequate data base of information available to all participants in the technology transfer program within our Government. This deficiency is analogous to prosecutors working without the benefit of a legal library There has to be a centralized repository of information that maintain available data relevant to the decisions to grant exports.

Fifth, the Department of Defense does not review a sufficient number of free world export license cases. Exports to free world nations many times are improperly or illegally reexported or diverted to East bloc nations. This has been demonstrated by recent export violations involving nations such as Switzerland and West Germany that were used as conduits for the illegal reexport of high technology commodities to the Soviet Union. The United States trades with many nations such as India and Pakistan who have open trade policies with the Soviet Union. To blindly export critical technologies to nations such as those without the benefit of the DOD's review could run the risk of having U.S. technologies end up in the Soviet Union.

Sixth, Defense Research and Engineering has not devoted sufficient resources to the program which reviews foreign technical visitor programs. Defense Research and Engineering is responsible for determining militarily critical technology that requires export control. This effort is being done in concert with U.S. industry. In this light, Defense Research and Engineering has devoted tremendous resources to the development and understanding of new dual-use technologies; however, there is not an adequate organization within D.R. & E. to assess what areas visitors are concerned with and what technology is obtained by these visitors. Therefore, due to this inadequate oversight, Defense Research and Engineering has little control over the potential loss of U.S. technology. Consequently, there is no way to assess what critical technologies have been obtained by our adversaries thereby making it virtually impossible for the intelligence community to determine how the loss impacts on our national security.

The effective control of critical dual-use technology is largely dependent on the proper gathering, dissemination, analysis, and use of intelligence. It is the view of the minority staff that the Soviets, in many cases, are precise about what technology and equipment they want from the United States. It follows then, that if the United States can determine what the Soviets desire, where they are deficient, what they need and what direction their technological efforts are aimed, we are in an improved position to prevent them from obtaining our technology which may meet their needs.

At the very least the United States could create delays in the Soviets' efforts which will impede their progress and maintain our lead time in critical areas of technology. Testimony will be given which describes the Soviets as having an enormous, systematic and organized effort to obtain United States and other Western technology. The United States, however, does not have a mechanism equal to the Soviets' task. There has been no overall coordinated, systematic and organized program in the United States to effectively prevent loss of our technology to the Soviets.

Intelligence is the key to anticipating the technology on the Soviets' "shopping list." U.S. law enforcement authorities can mount effective enforcement strategy directed toward illegal exports when they are

apprised of what the Soviets are looking for. Department of Defense and Commerce representatives who review export licensing cases would be in a better position to render proper decisions based on national security interests if they had the most available intelligence. But, after reviewing information obtained from law enforcement and technology specialists in the executive branch, the minority staff has reached the preliminary finding that the U.S. intelligence effort regarding export controls is insufficient. Coordination among affected agencies is inadequate. Commitment of needed resources is lacking. The intelligence community is not organized to use information to block prohibited diversions.

Specifically, the minority staff found the following deficiencies within the intelligence operations of the technology transfer control effort:

First, the Export Administration Act mandated Commerce to determine the foreign availability of critical dual-use technologies. The foreign availability of technologies is an important ingredient in the decisionmaking process for granting or denying export licenses. However, authorities within the executive branch assert that current foreign availability determinations are not adequate.

Second, the intelligence community has not been utilized sufficiently by either Commerce or the Department of Defense. Sources within the intelligence community state that they have virtually no communication with Commerce's Compliance Division regarding ongoing investigations of export violations. One representative of the intelligence community indicated that there is little feedback from Commerce regarding the intelligence information it provides. The information is submitted to Commerce's Office of Intelligence Operations and it is not known whether it is disseminated to the Compliance Division or other divisions as well. Conversely, the Compliance Division rarely seeks the expertise of the intelligence community regarding investigations.

Moreover, once the intelligence apparatus is strengthened, then methods should be devised that enable sensitive information to be sanitized and passed on to law enforcement personnel in a form that will assist them. Several experienced law enforcement investigators pointed out that frequently intelligence on technology transfers has such a high classification that many agents working export controls cases cannot set it.

Third, Defense Research and Engineering tasks the Defense Intelligence Agency to conduct end user investigations. Essentially, Defense Intelligence Agency is to determine whether the end user of an export is not a national security risk. Defense Intelligence Agency performs this task as a support function to Defense Research and Engineering—its license review procedures. Historically, DIA has been utilized infrequently in this capacity. Within the last 18 months DIA has been tasked more frequently; however, it does not have sufficient resources to conduct end user determinations that are necessary.

Fourth, there is no mechanism or organized program which conducts followup investigations of foreign exports or reexports of U.S. technology. In fact, there is no adequate system to accurately determine what has been exported, reexported, where it is used, and how it is used. There is no way to accurately determine the adverse impact to the United States of that dual use technology that has been obtained by our adversaries.

Officials working in the technology field are troubled by the fact that our Government has difficulty determining a current assessment of the state-of-the-art of American technology. Given such a fact, the difficulty in assessing what technology has been lost and its impact on U.S. national security seems almost insolvable given the current resources and policy.

In summary, the U.S. Government, at present, has no high level interagency task force or entity comprised of senior Cabinet-level officials addressing the problem of export control and technology transfer. All past and current efforts along this line have been done by lower echelon Government officials who can merely make recommendations rather than needed changes.

Senator NUNN. Thank you very much, Mr. Fry.

I want to thank you and Mr. Asselin for not only your testimony this morning but your investigative efforts over a long period of time. You have both done an excellent job. We appreciate it very much.

Senator Cohen, do you have any questions?

Senator COHEN. Just one question.

Has anything at all been done since we held the hearings on Senator Garn's bill on September 24 and 25, 1980? It seems to me, Mr. Chairman, we are going over the same issues time and time again for the past 3 or 4 years. We keep talking about it, but nobody does anything about it.

Mr. FRY. Senator, that was our finding, that very little has been done. They have made some efforts. The interim policy, to the credit of the Departmentof Defense, is the only policy in this area of export control technology transfer put out by any executive agency.

However, it is still an interim policy.

Senator COHEN. Do you come to the conclusion that we ought to create a separate office of strategic trade, an independent power such as the Federal Reserve Board?

Mr. FRY. I think it is a viable alternative.

Senator COHEN. Because the essence of that is, as far as Senator Garn is concerned, that there is a tremendous bias within Commerce to promote exports and sales. The State Department has its own diplomatic or political biases or preferences that it might seek to achieve and then you have the responsibility of the Defense Department.

So, we have three major departments each having perhaps a different objective. If you left it up to DOD, they may say don't export anything.

If you left it up to the State Department to have the final decision, they would say it depends on what we are trying to achieve in a period of détente or no détente.

If you leave it up to the Commerce Department, then you would promote the sales in order to invigorate our own domestic industry. It seems to me that our whole process is caught in a crossfire between these three separate departments with Congress sort of on the sidelines having some interest, but only peripheral at best, in terms of being able to do anything about it. So, I would think, based on what I have heard, Senator Nunn, that something ought to be done in terms of consolidating the responsibility of the jurisdiction in one office that can weigh the conflicting pressures that are inherent in our system.

Frankly, this whole issue of dual use goes back to the Kama River Plant, in terms of whether or not that sale should have been authorized. I am sure you can certify that practically any item that is subject to classification under this act you can be excepted based upon foreign availability. Given these problems, I would suggest that some initiative ought to be taken to consolidate responsibilities into one office and perhaps really enhance and increase the enforcement capability of that office.

Senator NUNN. We need to look at the licensing function in a different vein from the enforcement. I think there is real merit in creating a strategic trade office and Mr. Asselin had the recommendation that the Garn bill be considered. Is that what you recommended?

Mr. ASSELIN. We recommended that members of the subcommittee certainly consider that. As a long-term solution, it is the best thing we can think of.

Senator NUNN. But you also are saying, from the way I read your conclusions, that we may very well want one group to do the licensing and another group to do the enforcement. If Customs already is out there in every port of exit in the United States, the question must be asked of whether it makes sense to have anybody else out there enforcing the law. Enforcement and licensing are two different functions. Under the Arms Export Control Act, the State Department does the licensing, Customs does the enforcing. It seems to me there is a real case to be made for the approach like Senator Garn has, in the case of the licensing and have the Customs agency do the enforcement.

Does that make sense?

Mr. ASSELIN. Yes, sir. It was our recommendation that for the short term, the problem is serious and requires immediate relief. It will take some time if the Congress in its wisdom wants to create the Office of Strategic Trade.

In the short term, the problem is serious enough. That is why we recommended for immediate relief that the Compliance Division be abolished and the Customs have the enforcement function very similar to what they have in the Arms Export Control Act.

Senator NUNN. But until something like a Garn bill passed, you would recommend that the Commerce Department still do the licensing? Somebody has got to do the licensing?

Mr. ASSELIN. Yes; that is the point. That will leave the licensing in the Commerce for the time being.

Senator NUNN. Temporarily unless something like the Garn bill passes?

Mr. ASSELIN. Yes; I don't think Customs wants the licensing function.

Senator NUNN. You are also implying congressional wisdom takes time; right?

Mr. ASSELIN. Yes, sir.

Senator NUNN. What is the day of the Garn hearings?

Senator COHEN. The days of the Garn hearings were September 24 and 25, 1980.

Mr. ASSELIN. I spoke with a member of Senator Garn's staff who said the Senator was planning to reintroduce the bill sometime either

95-929 O - 82 - 8

just before our hearings or sometime after them. I don't know if he has done it yet.

Senator NUNN. The problem is always whether you need to create a new agency and the proliferation of agencies, you run into that argument over and over again. The question is whether there is any other logical thing to do.

Senator COHEN. The other issue you raised during those hearings, as I recall, is that if we don't have a fundamental restructuring of the classification system, a definition of exactly what we are about, it doesn't make any difference if we create a new office. With all of the same conflicting standards and rules and exceptions, you really have not accomplished anything other than consolidating the mess all in one place.

It seems to me we have got not only to have a new structure institutionally but we have got to define classification.

Senator Nunn, you mentioned this yesterday how we classify items, how we determine which ones will in fact be put on a list. Should we have the Cocom list, for which historically the United States has requested more than 50 percent, closer to 60 percent of all the exceptions for Cocom.

So we can hardly expect our European allies to be following a hard line and not exporting items of national security importance to the Soviet Union and Warsaw Pact countries.

The other issue is, should we include all Warsaw Pact countries if we are going to prohibit the sale and distribution to the Soviet Union; does that not include by necessity putting a restriction on all countries under the Soviet bloc?

Senator NUNN. I guess the other question that I would like to get your opinion on here, Mr. Asselin, and Mr. Fry, what about putting the export licensing function under the State Department? State already has arms export licensing. In other words, put both licensing functions in the same agency.

Mr. FRY. I don't want to address that.

Senator NUNN. Do you have any idea about that? If you don't just say so.

Mr. ASSELIN. No; I would be against that. I think Commerce is the proper place for the licensing function if the Department were properly organized. But we interviewed the present Acting Director of the Compliance Division. He was formerly the Chief of the Office of Export Administration for 1 year. His name is William Skidmore. He admitted that there were problems in the Compliance Division.

He acknowledged, yes; there are problems there but when he was head of OEA, he spent all his time trying to straighten out the licensing section. Our staff didn't look into the licensing section. All we looked into was the Compliance Division. We found that to be inadequate, to say the least. If he felt his real problems were in licensing and he thought it was more important to straighten out licensing than it was Compliance, then that gives you an idea what an inadequate operation licensing possibly may be.

Senator NUNN. Even under the best of circumstances as Senator Cohen pointed out, licensing is always difficult because you have different views. I think the point that was made yesterday about having

an assessment of what the Soviets are really after is the beginning point.

It seems to me that your policy needs to be driven somewhat by that. We are right now trying to review everything, instead of going down the list to those items they really need in their technology. As the witness testified yesterday from Los Alamos, the technical capability to really analyze what it is the Soviets need would be a good starting point for any licensing procedure.

Mr. ASSELIN. Yes. Dr. Baker made quite a point of the fact that the Commerce Department is very good in licensing to this extent. They are very good at saying whether a particular piece of equipment needs a validated export license. Where they are not very good, where they are not very adequately trained is in the determination of what uses that piece of equipment can be put to overseas in the hands of an adversary. That is where the technical expertise falls short in Commerce. That was his basis for his recommendation for that center of technical expertise.

Senator COHEN. Along those lines, given the jurisdiction to the State Department over arms sales, what would be done about ceramic tiles, for example? Ceramic titles might seem fairly innocuous and have a nice household use. The first witness yesterday, however, indicated that very little if any technology that is transferred to the Soviet Union ends up in the household. Ceramic tile is also important in terms of the space shuttle.

To what extent could you put a prohibition—I see a gentleman in the audience shaking his head. But the fact of the matter is we have some rather extensive improvements in the field of ceramic tiles which Rockwell does in fact use for the space shuttle.

It is very difficult to classify that as being an item of strategic value in the abstract. So I think it lends more support to what can in fact be converted because almost any item that we export could be converted to another use.

Senator NUNN. I certainly agree.

Whatever the situation is with licensing, you have concluded without any doubt that compliance is beyond the Commerce Department institutional capability?

Mr. ASSELIN. Yes; very definitely.

Senator NUNN. Do you agree with that?

Mr. FRY. Absolutely.

Senator NUNN. Thank you both.

Our next witness is Dr. Jack Vorona, Director, Scientific and Technical Information, Defense Intelligence Agency, Department of Defense.

Dr. Vorona, we appreciate your being here. We swear all of our witnesses in.

Do you have anyone accompanying you?

Dr. VORONA. Alone.

Senator NUNN. Will you hold up your right hand?

Do you swear the testimony you will give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Dr. VORONA. Yes, sir.

TESTIMONY OF DR. JACK VORONA, DIRECTOR, SCIENTIFIC AND TECHNICAL INFORMATION, DEFENSE INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE

Senator NUNN. Dr. Vorona, why don't you go ahead?

Dr. VORONA. Thank you, Mr. Chairman.

I welcome this opportunity to talk to the issue of technology transfer and its principal beneficiary, the Soviet Union. Because truth like beauty is in the eyes of the beholder, I will say at the outset that my views are conditioned by over 20 years in scientific and technical intelligence, most of which time was devoted to assessing Soviet military capabilities.

One of the basic tenets of my profession is never to mirror image—unless, of course, all else fails. That is, one must refrain from a mindless attribution to others of capabilities developed and sought by the United States. What is becoming more apparent, however, is the deliberate, massive, and longstanding effort by the U.S.S.R. to acquire Western technologies for direct incorporation into their military and defense-related industry.

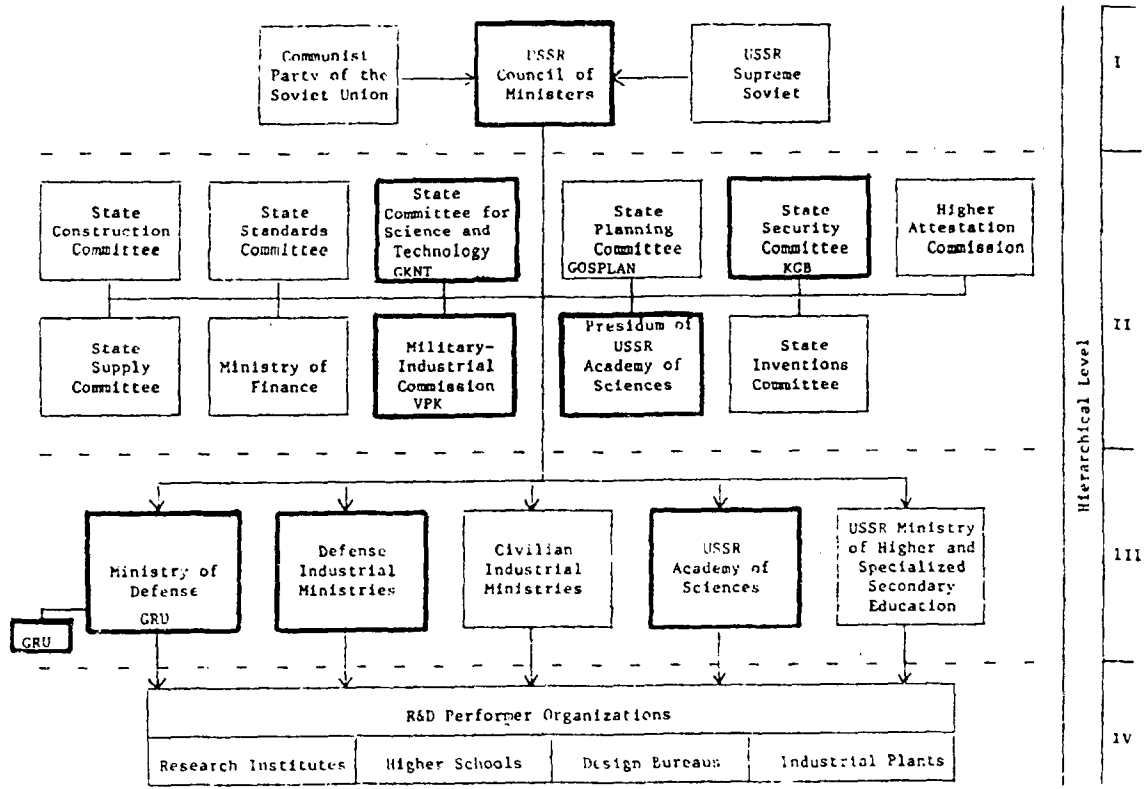
It would appear they are hardly at all afflicted with the not-invented-here syndrome, but, on the contrary actively seek out, acquire and implement our developments to a degree, even today, not fully appreciated.

If I were to characterize the Soviet effort to acquire U.S. technology, I would say that it enjoys very high priority, is centrally directed, specifically targeted, and employs every collection means imaginable.

All in all, a very comprehensive program.

Seen on this chart is the organizational structure of Soviet R. & D. at the all-union level. Those organizations marked in red are directly involved in technology transfer.

[The chart referred to follows:]



ORGANIZATION STRUCTURE OF SOVIET R&D
AT THE ALL-UNION LEVEL

Senator NUNN. What do you mean by "the all-union level"?

Mr. VORONA. At the national level, sir. You see that they reach the highest political levels—a fact which underlines how importantly Western technology is viewed from Soviet eyes.

I would like now to describe for you this program's basic modus operandi. First comes their exploitation of the world's open scientific literature. This involves the annual acquisition and translation of about 35,000 publications from 125 different countries in 65 different languages—roughly 1.5 million articles. This massive effort clearly serves as an excellent guide to the world's technical state-of-the-art, where it's being done and by whom.

This data is at the disposal of the State Committee for Science and Technology or GKNT—the organization responsible on the one hand for ascertaining Soviet technological and industrial weaknesses, and on the other, for their remedy. Thanks to the open literature, the GKNT knows exactly where to go to overcome their deficiencies.

The open literature itself answers some of their needs; many others are met by legal purchase. But they also invoke a wide variety of illegal maneuvers. These include evasion, diversion and the use of U.S. chartered but Communist-owned firms to acquire material normally denied them under export control laws.

Espionage is yet another tool—not only are the KGB and GRU heavily involved in acquiring our technology, so are the intelligence services of the pact nations, all centrally directed by the Soviet Union.

I would also mention the role of the Soviet Academy of Sciences in this beautifully orchestrated effort to acquire critical U.S. and Western technologies. There should be no doubt that this prestigious academic organization is a key and willing participant which, via such mechanisms as scientific and student exchanges, contributes significantly to the total take.

The Soviets in the post World War II period began a huge effort to acquire the industrial and technological wherewithal to support their military ambitions. For example, the impressive Soviet radar capabilities of today had their genesis with World War II lend-lease equipment sent them by the United States.

This along with the unclassified MIT radiation laboratory volume on radar theory were the basic ingredients for the early generations of Soviet radar design.

The Soviets are excellent radar theorists and have since added their own refinements. I would note, however, that the acquisition of U.S. microcircuitry very probably enabled them to package sophisticated radar concepts into a weight and volume suitable for the militarily critical airborne application.

I specifically refer to their look-down/shoot-down interceptor, the modified Foxbat, whose entry into the Soviet inventory was no doubt expedited thanks to acquisition of embargoed U.S. microelectronics.

Of course, we haven't begun to see the repercussions of the recent espionage case involving Mr. Bell and the Polish Intelligence Service. The classified data transmitted is no doubt right now being investigated to further Soviet radar capabilities and countermeasure our own.

Their initial chemical warfare capability came from Germany after the war. They simply transported two nerve-agent factories from Germany back to the Soviet Union.

Their TU-4 bomber was a direct copy of our B-29. Their first jet engine was from Rolls-Royce—the Nene—it powered their MIG-15 fighter.

The U.S.S.R. and East European family of general purpose computers known as the RYAD series are based substantially on IBM 360 and 370 computers that were illegally diverted into the U.S.S.R. Their decision to emulate U.S. computer design eliminated the time and risk associated with indigenous development.

It had the equally important effect of making available to them a tremendous library of computer software that was RYAD compatible.

Since the early seventies, the Soviets and East Europeans have legally purchased more than 3,000 microcomputers, some of which are being used in military-related organizations. They are also producing minicomputers that are direct copies of Western models.

Nuclear weapons design information clandestinely provided them by Klaus Fuchs was undoubtedly a key ingredient in their achieving workable weapon designs as early as they did. When the Soviets were unable to produce the fissionable material, U-235, in the post World War II period owing to inferior gaseous diffusion technology, they brought in a German scientist, Peter Thiessen, who was able to rectify their problem.

As a result, they were able to detonate their first U-235 bearing weapon years earlier than if left to their own devices.

These, and numerous other examples, we considered as but stop-gap measures by the Soviets—until their burgeoning indigenous R. & D. resources were able to pick up the slack. What we are coming to recognize, however, is a continuing and deliberate program to acquire Western technology which is integrated with or used in lieu of their own.

The acquisition of Western technologies and developments is thus a conscious Soviet policy which, in my estimation, has been extraordinarily successful. They have derived significant military gains from these acquisitions particularly in the areas of computers, microelectronics, signal processing, manufacturing, communications, guidance, and navigation, structural materials, radars and sensors of various types.

The extensive Soviet acquisition program has allowed them and their allies to save untold hundreds of millions of dollars in R. & D. costs alone and years in R. & D. development lead time, to reduce engineering risks by copying proven western designs, and to develop countermeasures to U.S. and western weapons, in some cases before our weapons have been fielded.

Most of the technology of direct and immediate military consequence has been clandestinely acquired by Soviet intelligence assets and their East European surrogates. However, the bulk of their acquisitions fall under the heading of dual use technologies, that is, technology having both military and civilian applications.

Because of the primacy of Soviet defense industry over the civilian sector, there is no doubt who will be the ultimate recipient, despite Soviet assurances to the contrary. By purchasing these capabilities, the Soviets are able to focus their own resources upon the strictly military undertakings.

For example, the Soviets recently bought two huge floating drydocks from the West which have already been put to use servicing their Kiev-class aircraft carriers as well as nuclear submarines.

Senator NUNN. Were those bought from Japan?

Dr. VORONA. One was from Japan, sir, and one was from Sweden. They are negotiating for others from those two countries.

Senator COHEN. I am sorry?

Dr. VORONA. They are negotiating for other drydocks from those two countries.

Senator COHEN. I was under the impression that Japan had learned the lesson about, on the one hand, complaining to the world that they are concerned about the Soviet buildup off their shores and, on the other, they have been providing them with the kind of assistance that will allow them to have those ships off their shores.

Dr. VORONA. One of these 1,000-foot-long drydocks is in the Northern Fleet, one in the Pacific Fleet. There is no doubt they themselves could have designed and constructed such a structure, but it would have taken longer and used resources that could otherwise be devoted to other needs.

However, despite their notable successes in acquiring Western technology, the Soviets for some time to come will be hard pressed to maintain their relative position to the West in the technical sophistication of their weapons.

Therefore, they will continue to seek Western technology. The Soviet Union will especially need equipment and technology for their electronics, aerospace, and shipbuilding industries. Future Soviet and Warsaw Pact acquisition efforts are likely to concentrate on the sources of such component and manufacturing technologies, including defense contractors, general producers of military-related auxiliary manufacturing equipment, and small and medium size firms and research centers that develop advanced component technology and designs.

I believe this last category of small companies to be a specially enticing target because it is where many of the emerging technologies are first discovered. Because of their newness they have not yet been incorporated into military programs and are thus unclassified and vulnerable.

In my estimation, the United States R. & D. establishment is viewed by the Soviets as a mother lode of important and very frequently, openly available S. & T. information.

In fact, they tap into it so frequently that one must wonder if they regard U.S. R. & D. as their own national asset. They have enjoyed great success in this endeavor with minimal effort, primarily because, as a nation, we lack the awareness of what they are about.

Senator NUNN. Let me ask you one question there.

Suppose we did have, let's say, reverse engineering on the Soviet espionage, overt and covert efforts to acquire Western technology.

In other words, we had a group of scientific experts within the Government who sat down, looked at what we had, looked at what was being developed, looked at what the Soviets had, their needs, spare parts, so-called half life, things they have already gotten from us and so forth and drew up a rather tight list of high priority items and suppose the Government went out and, first of all, distributed those lists within the agencies and, second, went out on a periodic basis and dis-

tributed those lists to the small businesses, the technical industries of the country.

Don't you think that that in itself would alert a whole lot of American businesses who are basically honest and patriotic as to what kind of technology would be most suitable to the Soviet Union?

Dr. VORONA. Yes. I certainly do. And, as a matter of fact, such an effort is already underway.

As you are well aware, the Congress directed the Department of Defense to develop a militarily critical technology list. This has been done. I cannot say exactly when, but I suspect in the very near term, it will be distributed to people such as you just mentioned. This list should give them a good appreciation of what technologies are militarily critical to the United States. Conversely, I would note that this list also reflects what the Soviets are targeting.

Senator NUNN. Is that going to be a standing effort by the Department of Defense to do this on a periodic basis to keep it updated or is that a one-time effort?

Dr. VORONA. It will be periodically updated.

Senator NUNN. Does this include dual use technology or is it military technology mainly?

Dr. VORONA. I believe it is primarily dual use technologies.

Senator NUNN. Dr. Baker from Los Alamos yesterday testified that he thought it would be a good idea to put a permanent standing group of 25 people at a cost of $4 million or $5 million a year in one of our labs for highly technical evaluations that would do this on a continuous basis.

Do you think that suggestion has merit?

Dr. VORONA. I would think that it ought to be done through a combination of efforts involving the intelligence community and the Department of Defense.

I cannot imagine a group of 25 people or so becoming expert in all the fields necessary for this.

Senator NUNN. He wasn't suggesting that. He was suggesting it was a clearing house, a central location so that all the defense intelligence community fed into there and that any inquiry, anything that people asked for, they would either be able to produce it there or be able to know where to get it.

In other words, a clearinghouse, not a comprehensive group.

Dr. VORONA. I would have to look at this proposal further, sir, to look into its ramifications. However, I believe we will soon have this capability within the intelligence community.

Senator NUNN. We would like to get your opinion on that as we deliberate some of these suggestions.

Thank you.

Dr. VORONA. We know the Soviets receive each of the 80,000 Government reports deposited with the National Technical Information Service—NTIS—of the Department of Commerce—75 percent which are from the DOD, DOE, and NASA.

In addition, classified Government research reports are subjected to automatic downgrading and declassification, so that, barring additional caveats, they are fully declassified in 6 to 8 years, immediately sent to NTIS and released with no consideration given to the possibility the report may still be of military significance.

The recent Executive order will substantially rectify this situation by giving to the report originator the ability to determine whether or not release should be made.

I should like to offer perhaps a less well known example, but one which both highlights the lack of awareness issue and Soviet ability to take advantage of it to our national detriment.

Specifically, two Soviet Embassy officials in 1979 went to the public library in Milan, Tenn., to reproduce pages from an environmental impact statement on file there concerning Government construction of a plant to manufacture military explosives, in particular, RDX/HMX.

As a result of this episode, an investigation was conducted to determine what the Soviets might have gleaned from the environmental impact statement. It was found that the document contained a wealth of technical detail which, when combined with already published material, would allow them to duplicate the entire manufacturing process.

This was clearly not the intent of writing the environmental impact statement. However, an awareness of the efficiency of the Soviet technology vacuum cleaner could have precluded such an occurrence.

In the past several hundred years, the Russians have upon various occasions imported Western technology. These were sporadic attempts to create an economy capable of supporting their foreign policy ambitions. But these efforts were not sustained and the economy lapsed into relative backwardness. Such is not the case today. The huge military R. & D. infrastructure they are creating, expressed both in terms of facilities and technically trained manpower, already the world's largest pool of scientists and engineers, indicates they are in this for the long haul.

And as the infrastructure matures, it becomes increasingly capable of extracting from and building upon Western developments, not to mention their own. For this reason, I believe it erroneous to conclude as some have, that Soviet efforts to acquire our technology somehow relegates them to a position of inferiority.

In closing, I would simply say that the Soviet leadership appreciates and has ofttimes noted the casual relation between science and technology and strategic superiority. To them, technology transfer is an important means to that end.

Mr. Chairman, this concludes my statement.

Senator NUNN. Thank you, very much, Dr. Vorona.

We appreciate all of your cooperation and we hope to keep in touch with you as we try to develop our recommendations growing out of these hearings which I hope will be in the very near future.

Senator Cohen.

Senator COHEN. Thank you, Mr. Chairman.

I assume you consider U.S. technology to be a national asset and that you have indicated, I think, even beyond that that the Soviet Union probably considers it to be their national asset as well.

Dr. VORONA. That is correct.

Senator COHEN. What is your evaluation of the U.S. leadtime of the Soviet Union in the area of technology?

Dr. VORONA. I believe in general the United States leads the Soviet Union in technology and has a distinct advantage, measured in years, in certain very critical military technologies, specifically computers,

microelectronics, signal processing and in general, production know-how.

This has to be maintained. Unfortunately, the Soviets through the various mechanisms we talked about have made significant inroads into this lead and one of these days we are going to find that the technological superiority which we have taken for granted is no longer going to be there.

Most importantly, once they acquire a technology, it is immediately incorporated into their military forces or defense-related industry.

So, measured in terms of which sides military forces have the superior technology our lead is diminishing even more rapidly and might even reverse in some instances as we go into this decade.

Senator COHEN. There is an old expression that a pigmy standing on the shoulders of a giant can see further than the giant. And, of course, that expression has been used in the past in terms of each of us being able to stand upon the accumulated body of wisdom from generations in the past. Therefore, we do not have to repeat the same errors and mistakes or learn the same lessons of the past and are able to look further into the future as a result of the benefit of collective experience. And what you are suggesting is that this is being translated into a new dimension, namely that the pigmy is now standing on the giant's shoulders, the giant being the U.S. technological development and capability and will be able to see that much further into the future by combining it with their own indigenous assets and development.

Dr. VORONA. Precisely.

Senator COHEN. What in addition to the list that is being put together, or has been put together, by the Defense Department can we do to alert the private sector about the dimensions of the problem and the extent to which they may be unwittingly contributing to it?

Dr. VORONA. As DIA's effort in that direction, Senator, we have since 1977 given 220 briefings to various groups throughout the country, including those in the Department of Defense, Department of Commerce, academic and industrial organizations. This was done in the hope of increasing their awareness of just how serious the Soviets are in this effort, how vulnerable we are, and the wide variety of mechanisms used by the Soviets to aquire our technology.

I believe that this effort has had some salutary effect.

Senator COHEN. The agencies who now have the responsibility for managing our export control operation, what sort of a data base do they have, what sort of corporate memory do these agencies maintain?

Dr. VORONA. I am not at all sanguine about the comprehensiveness of the data base resident in any particular agency concerning technology transfer.

I believe this is one of our serious shortcomings. However, we are making significant strides within the intelligence community and the Department of Defense to rectify this very shortfall. But unless and until we have the kind of data base to which you refer, any truly meaningful assessment of technology transfer and its impact on the Soviet military posture is merely arm waving.

Senator COHEN. What assessment do you make of our efforts to investigate the end users of the exports?

Dr. VORONA. This may be contrary to the conventional wisdom or some of the things that you have heard but in my estimation, our ability to determine whether or not dual-use technologies are being diverted for military purpose in the Soviet Union or in any closed society is woefully inadequate.

Furthermore, I am not at all optimistic that even with additional resources, could we significantly redress that situation.

Senator COHEN. Let me take it one step further.

Assuming you had the resources, significant resources to make that kind of determination, in your judgment, would it make any difference?

In other words, suppose you were to tell other countries, including our own exporters, that this technology would have a dual use. Whether it is the Kama River Plant, the Brazil plant or whatever it might be, do you think that would really be an inhibiting factor to a nation selling such technology to the Soviet Union?

Let me use Japan by way of example.

Do you think there is any doubt in the minds of the Japanese as to what use the Soviets will put to that large drydock?

Dr. VORONA. I'll probably never know the answer. I do know that the Soviets specified it was going to be for civil purposes. Of course they immediately diverted it for military purposes.

Senator COHEN. Now you are telling me that the Japanese and the Swedish Governments are considering selling even more?

Dr. VORONA. At least the Soviets have made overtures to them.

Senator COHEN. I guess what I am asking you is when it comes down to the choice between profits and national security, what has been the history that we have witnessed to date?

Dr. VORONA. It has not been terribly reassuring—it has been a concern.

Senator COHEN. It is all well and good for us to sit up here and talk about how we are going to possibly create a new agency to consolidate all the functions of analyzing the export value, commercial value, the diplomatic value and the defense value for a particular item. Then we talk about alerting the business world to the consequences of allowing that technology to be exported beyond our own boundaries. Then we have a more fundamental problem; that is, how do we weigh that against the experience of nations in the clear face of demonstrated conversion to military purposes since the motive for profit for export has overwhelmed whatever doubts may have been held by that particular firm.

I know time after time when Members of Congress have raised concerns about sale of computer technology to the Soviet Union, those companies will come to me and to others and say, how can you do this? How can you prohibit the sale of this particular computer technology to the Soviets where if we don't do it, the Japanese will do it or the Germans will do it, the British, surely the French, whoever has an opportunity to start a stampede for this technology, will pick it up. We will lose the profits from the sale of this system, the profits of which we could then reinvest into greater R. & D. to keep 5 or 6 years ahead of the Soviet Union?

How are we going to measure up to that particular problem?

Dr. VORONA. I don't know, Senator Cohen, but I would hope that in making countries aware of what the Soviets are about and how the technologies that they acquire are in fact enhancing Soviet military posture would have some sobering effect.

Senator NUNN. Senator Cohen, on that point, I don't think there is an easy answer to that. I think you put your finger on a very difficult question. But I do believe within the NATO structure itself, the military side of it, they ought to have a small group of people that interrelate to the backhome group so that NATO, when there is an impending sale, would be able to comment on it.

It is handled more or less at the Cocom level and it is not working. I think the same thing; we have a standing group with the United States-Japanese defense treaty of people that are in charge of making planned programs there.

I think we need a smaller group there, that don't do anything but alert the two nations. They have got to raise it to a decision level at an early stage. But right now, the Cocom arrangement simply isn't working.

Senator COHEN. I agree with that, Mr. Chairman. I am not trying to undermine the effort. I think you ought to be commended and I want to support every effort that can be made to change the way in which we do business. In another context, I am also perhaps realistic enough—perhaps even cynical enough—to look at what is taking place, for example, with the pipeline, which has nothing to do with the critical technologies list.

In my judgment, there is a classic case of where our European allies are undertaking a venture which is going ultimately to be detrimental to their future security because I believe that pipeline will be used as a lever against NATO taking any trade action, diplomatic action or potential military action. I have said this before and tried to pose it in deliberately dramatic terms, but it is my judgment that our European friends are marching toward the Berlin Wall with their eyes closed. I think if we continue to follow the procedure they have, they will be behind the Berlin Wall with their hands up.

That is the direction, I think, they are going. To me the Yamal pipeline closes in this most dramatic form exactly the point I am raising, namely providing technology to the Soviet Union which it doesn't have. Then you have to ask the question, why is the West 15 years ahead of the Soviet Union in oil drilling or gas drilling capabilities and technology?

The answer is pretty simple; they have been putting 15 percent of their money into military uses. And so what we are doing in effect is subsidizing their own domestic deficiencies or inefficiencies, allowing them to continue to spend the money for drydocks or for SS-18's, whatever it might be, while we supply the technology to ease their particular commercial difficulties. And I think given that sort of formula, then there is little prospect of the United States breaking out of this force which is almost centrifugal in the way in which it operates, pulling all of the technology into the Soviet Union.

Let me ask you, Dr. Vorona, what is the working relationship that you have, DIA and the Commerce's Office of Intelligence Operations?

Dr. VORONA. We do have a good working relationship with them, although it's essentially a one-way street. We provide them with what-

ever information they ask for. On the other hand, we have had precious little interaction with the Compliance Division.

Senator COHEN. How many times have you been called upon to use your own expertise with Commerce, Customs, or FBI to deal with export cases?

Dr. VERONA. To my knowledge, once, and that was to provide an analyst as an expert consultant to the Justice Department in the *Spahr Optical* case.

Senator COHEN. Before I go any further, I would just like to clarify something with respect to my comments about our European allies. I don't think the United States, frankly, myself included, is in any position to lecture the Europeans since we ourselves should be charged with the same sort of avarice or greed for consideration of our own national markets. I point specifically to the grain embargo as an example. It is very difficult for me to go to any of our allies in Europe and say you are making a fundamental mistake building the pipeline when in fact we are unwilling to forego the same sort of profits that we ourselves are seeking.

I don't think I am in the position to lecture the Europeans when we ourselves are unwilling to bear some of the pain that is necessarily involved in dealing with the Soviet Union. It is still my opinion that even if we were to shut off our supplies of grain, which I would support, that the Europeans at this point are still going to be buying gas. I think that is almost irreversible at this point.

Had different action been taken earlier, we might have diverted that. Any nation willing to feed the Soviet Union cannot lecture anyone who wants to derive gas from them.

Senator NUNN. Thank you, Senator Cohen.

In an editorial of April 12, 1982, the New York Times commented on technology transfer to the Soviet Union. The Times expressed the opinion that lowering the barriers to the flow of technology to the U.S.S.R. is not necessarily a bad thing. The Times editorial put it this way, and let me quote directly from that:

> A more relaxed policy would serve the West's best interests because a steady supply of foreign technology saps the Soviet Union's incentives to develop its own. It is better to have the Soviets stealing, copying and following a few steps behind than working independently in becoming able to deliver a technological surprise.

What is your response to that opinion in the editorial?

Dr. VORONA. Mr. Chairman, in a nutshell I think it is divorced from reality. The Soviets are bent upon achieving world preeminence, dominance, if you will, in science and technology and are building a huge R. & D. infrastructure with that goal in mind. The technology they are acquiring from the West is an important input to that process because it allows them to compare and build upon the best of both worlds, and they do.

A more relaxed export policy, rather than condemning them to second place as the editorial seems to imply, would only hasten their achieving world class status.

As a separate but related matter, I would again point out that our technological advantages may or may not find their way into military hardware but you may rest assured that if the Soviets go to the trouble to acquire a particular technology, it will post-haste be translated into

a military capability. As a result, the technological superiority we enjoy in the civil sector is significantly eroded when military hardware is compared. The concept proposed by the Times would exacerbate that situation as well.

Senator NUNN. Thank you very much, Dr. Vorona.

Senator COHEN. Yesterday, Dr. Vorona. I mentioned my unhappiness with the kind of rules under which we have to operate in terms of international athletics, specifically that our amateur athletes have to go up against the Soviet professionals, because they are, in fact, professional athletes in the Soviet Union and Warsaw Pact countries. They are supported by the state whereas our own athletes do come out of college and go into professional basketball or whatever the sport might be and support themselves through their contracts.

It was suggested yesterday by our first witness that the Soviets also have professional students who come into this country. You touched upon this just briefly in your own testimony. In other words, we send our amateur students to the Soviet Union to study humanities and the classics while they send professional students, people who are mature, would not be so taken in by what attractions our society might offer. Furthermore the students and that they already are well trained and are looking for certain technology.

Would you agree with that assessment, that in essence what they are sending here are professional students who are interested in acquiring the information from an academic institution that otherwise might be prohibited for sale or distribution or export to the Soviet Union?

Dr. VORONA. Yes, Senator, I completely agree with that assessment.

Senator COHEN. Thank you.

Senator NUNN. Thank you very much. We would like to be able to pose other questions to you for the record, if we may?

Dr. VORONA. Certainly, sir.

Senator NUNN. Thank you very much, Dr. Vorona.

Our next witness is John Maguire, president of the Software AG, Reston, Va.

It is the custom of this subcommittee to swear all witnesses appearing before it.

Do you swear the testimony you give before the subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. MAGUIRE. I do.

TESTIMONY OF JOHN MAGUIRE, PRESIDENT, SOFTWARE AG, OF NORTH AMERICA, INC.

Senator NUNN. I know you have a statement. Thank you for all your cooperation. We appreciate you being here today. We look forward to hearing your statement.

Mr. MAGUIRE. Mr. Chairman, Senator Cohen, as a member of America's high technology industrial community, I note with great interest the subcommittee's concern over the increasing loss of American technological know-how to the Soviets. I am pleased to be here this morning to share with you my personal experiences in confronting this problem in the computer software industry.

I am currently both president and chairman of the board of Software AG of North America, Inc., located in Reston, Va. Our company focuses on the production and sale of computer software, as opposed to computer hardware. Computer hardware, including microprocessor chips, can be and has been reverse engineered. As a result of Soviet use of that technique, Soviet hardware technology is now nearly equivalent to U.S. hardware technology.

By contrast, software cannot be so easily deciphered and duplicated. Software remains the key to future computer development as opposed to hardware where Jordan is even ahead of us now. Yet given the inability to reverse engineer, current Soviet efforts at software development are antique by comparison to those in the United States. Even the Japanese are many years behind the United States in development of computer software. Last year I met with the Minister of Information for Japan. I don't know how you would measure it, it is a figure of 8 years behind the United States in computer software.

The United States undoubtedly has both an enormous investment and a substantially important national resource in its technology lead in the software field.

In that context, my company has proven itself as a leader in the software field. Specifically, we have been responsible for the development and manufacture of ADABAS, a Data Base Management System, we use the expression DBMS, which constitutes the present state-of-the-art for this very important aspect of software technology. DBMS is the implementation tool used by programers to implement computerized information systems—with an increase in productivity of approximately 1,000 percent—as compared to conventional computer software technology. Between 1960 and 1980 I estimate over $1 billion has been spent on hundreds of projects to solve the DBMS problem. The current ADABAS source code represents the highest level of sophistication yet achieved in DBMS technology. It now includes over 200,000 detailed instructions.

Like other software, ADABAS is not susceptible to copying by the technique of reverse engineering. By analogy, one might consider ADABAS as the Coca-Cola formula of the computer software industry. It is, deservedly, a closely guarded secret: Possession of the source code, like the Coca-Cola formula, could only be obtained by competitors by the quirk of an identical, independent invention, sale, or theft of that source code itself.

Unfortunately, our task in guarding the source code as a private company does not stem only from the economic rigors of the competitive domestic marketplace. The most blatant and obvious attempts to secure the secrets of ADABAS have come, not from our American competitors, but from the Soviet Union.

Although the ADABAS source code is not classified, it is considered to be sensitive technology requiring a validated license for export. My story to you this morning will detail not one, but two, focused attempts to secure our computer software know-how for use in the Soviet Union.

In 1979 a Belgian national by the name of Marc DeGeyter contracted our marketing representative in the State of California. DeGeyter wanted the name of the most technologically expert individ-

ual in our company. He was referred to Jim Addis of our Reston, Va. office. Jim is one of two individuals in our company who have access to the ADABAS source code. DeGeyter personally approached Addis, offering him $150,000 cash for the purchase of the ADABAS source code on behalf of the Soviets. Addis told DeGeyter that he would have to discuss the offer with his superiors. When Addis told me about the approach by DeGeyter, I immediately contacted the FBI.

At their request, I agreed to cooperate by personally dealing with DeGeyter. As part of that cooperation, I agreed to the tape recording of my conversations with Addis, DeGeyter contacted me, confirming the original offer of $150,000 for the source code. He told me that he had many business dealings with the Soviets in their country; in order to insure continued good business dealing with them on other matters, he needed to obtain the ADABAS source code for them.

Working with the FBI, I negotiated with DeGeyter for a period of approximately 7 months, finalizing arrangements whereby I would transfer the source code to him for a price of $150,000. During those months, I had numerous telephone and personal discussions with DeGeyter. I personally met with him in Washington, as well as telephoning him in Belgium and vice versa.

There were a lot of calls around the United States—California, St. Louis, Silicon Valley area. I spent a lot of time there.

I recall that, in at least one conversation, DeGeyter told me that the Soviets had approached him with a specific "shopping list" of technological items needed from American sources. He told me that, as early as 3 years previously, they had included the ADABAS DATA Base Management System on that list.

Since he could not at first figure out a way to obtain the code, DeGeyter had initially bypassed it and gone after other technology items on the list. The Soviets had evidently changed their priorities and were now insisting that DeGeyter secure ADABAS on their behalf.

My own knowledge of DeGeyter was consistent with his description of his efforts for the Soviets. I knew that DeGeyter had personally approached software expert Charles Matheny some 2 or 3 years previously, attempting to hire him to steal selected IBM technology on his behalf. I later learned from a software representative in Amsterdam that DeGeyter had been caught stealing trade secrets and prints from their Belgian plant several years earlier. DeGeyter had taken the items while employed at the plant. Although he had been initially charged in the Belgian courts, he was never convicted of the offense in that country.

I also know that DeGeyter moved constantly in high technology circles. During my negotiations with him, he traveled in and out of California's Silicon Valley on numerous occasions. Certainly Silicon Valley might well have been the home of many of the items on the requested shopping list. When DeGeyter was eventually arrested at Kennedy Airport, Federal agents searching his briefcase found, among other things, numerous telexes from DeGeyter to individuals and companies in Moscow.

One such telex dealt with a payoff to DeGeyter. In connection with the payoff, the telex included nomenclature assigned to a new microprocessor chip in the process of development at Intel in Silicon Valley.

95-929 O - 82 - 9

The chip was not, of course, publicly marketed at that time. In his conversations with me, DeGeyter made no bones about his technology efforts on behalf of the Soviets. He told me that he was not alone in doing so; rather, technology transfer was simply their—the Soviets—way of doing business.

In discussing the sale of ADABAS source code, I voiced to DeGeyter my concerns that the source code might eventually be disclosed to our American competitors, in addition to the Soviets. In the contest of a highly competitive American market for computer software, it was certainly realistic to treat the threat of American companies acquiring ADABAS source-code knowledge as more economically frightening than Soviet development.

DeGeyter assured me that the source code would not be coming back to the States or to American competitors anywhere. He told me that he was purchasing the code on behalf of Techmash Import, a Soviet trading company and that the Soviets had no interest in furnishing the code to my competitors.

During the course of my negotiations with DeGeyter, I attempted to arrange for the delivery and sale of ADABAS source code to him in the United States. A planned delivery in this country was necessary in order to successfully prosecute DeGeyter under our export laws. Unfortunately, he insisted that I fly to Brussels for delivery of the code where he would make arrangements for payment of the cash price through a Swiss bank account. When I voiced hesitation to him about delivery abroad and, consequently, the entire transaction, DeGeyter upped the case price from $150,000 to $200,000 plus some California real estate, and later to $450,000. Of course, by comparison to the U.S. investment of $1 billion in DBMS technology over the years, the Soviets were still talking in terms of "bargain basement" prices.

Eventually, our negotiations broke down, due to his unwillingness to agree to delivery in the United States. DeGeyter later contacted Charles Matheny, the owner of a computer company in our building, and asked him if he knew of any other way to secure the ADABAS code on DeGeyter's behalf. The FBI again stepped in and, through the use of undercover operatives, eventually arranged a planned delivery of a dummy source code in New York. As a result, DeGeyter was eventually charged and sentenced for his efforts to steal the source code. I understand that Mr. Greenberg, the Federal prosecutor in that case, will describe that matter in detail for the subcommittee.

When the *DeGeyter* case ended, I assumed, perhaps naively, that ADABAS was relatively secured from Soviet attempts to buy or steal. In other words, keep it in a 1,500-pound safe on the 11th floor of the building out in Reston.

Senator COHEN. Don't tell us any more.

Mr. MAGUIRE. I forgot the combination.

The ADABAS was relatively secure from Soviet attempts to buy or steal. In the spirit of American free enterprise, I even used the fact of the Soviets' efforts for the potential economic advantage of Software AG. We subsequently purchased magazine advertisements boasting "ADABAS. The Russians weren't smart enough to invent it—but they knew enough to want it."

A copy of that I will show you in a few moments.

Senator NUNN. What would they be able to do with it once they got it? You say reverse engineering is——

Mr. MAGUIRE. It is impossible. It hasn't been done yet. The source code that the detail machine language and construction representing the basic logic for handling automatically all the information in a large data base, we take that source code and run it through the computer, what is called an assembler process, to create the machine object code which is just millions of bits and that is what we deliver, we sell a license for that and it works and it runs on a computer but no one can look at those millions of bits and figure out the logic.

What they wanted was the source code to understand the detailed logical steps in the logic, just like a chemical formula, the logic underneath the technology. Once they understand that, they could bring that logic to other computers or anything they want, but they would learn what has evolved to be a very successful technology, a value, dual use military and commercial.

Senator NUNN. Thank you.

Senator COHEN. It is subject to reverse engineering?

Mr. MAGUIRE. No, but you have to have the source code. You can get a silicon chip and reverse engineer and just peel away those layers and take a look at it with a microscope and there is the detail logic.

Senator COHEN. What the chairman was asking about, as I understood it, is why would they want that if in fact they couldn't duplicate it. If they get the source code which they attempted to purchase, they could go back and reconstruct the formula and use it to develop future systems.

Mr. MAGUIRE. It is worse than that. By having the source code, there's the secret.

Senator NUNN. That is the formula?

Mr. MAGUIRE. That is the technology right there.

Senator NUNN. You say no reverse engineering is necessary if they get back. What they can't reverse engineer, is what you sell?

Mr. MAGUIRE. That is correct.

Senator NUNN. Using the analogy of Coca-Cola, if you get the Coca-Cola, you can't get the formula. If you get the formula, you know how to make the Coca-Cola. Is that right?

Mr. MAGUIRE. Yes; we sell the license for $160,000 currently.

Senator NUNN. The FTC maybe ought to be called in on this. You said $450,000. Your add says $500,000.

Mr. MAGUIRE. I was replaced by the FBI agent eventually and then DeGeyter upped it up to $500,000. No; that is correct.

Unfortunately, despite DeGeyter's conviction, I soon discovered that the Soviets still wanted ADABAS and our other software and are, in fact, still trying to secure it. As with other technology companies, Software AG participates in trade shows on a regular basis.

In 1981 a Russian diplomat named Georgiv V. Veremey visited the Software AG booth in at least two separate trade shows in the Washington area. Since he was registered with the show and also provided us with his business card, we have a formal record of the trade show contacts. In both instances, Veremey asked numerous questions concerning ADABAS, internal logic of the system and the source code.

After the trade show contacts, Veremey personally visited the Soft-

ware AG offices in Reston, Va. On September 25, 1981, Veremey arrived, introducing himself as a member of the Soviet Embassy staff in Washington, D.C., and requesting to see various documentation on our products. He spoke to Sunday Lewis, a senior executive at the Reston office. He told Lewis that he wanted a complete bibliography of all Software AG products and their documentation. He disclaimed any particular purpose for the request, saying that he was just interested. He was extremely vague about the nature of his work with the Soviet Embassy. After Lewis gave him a standard bibliography and an order form, he left.

On September 26, 1981, Lewis told me about the incident. I told her that, as company policy, we would not sell products to the Soviet, even the object code. Moreover, I told her that to do so without a license was prohibited by Federal law.

On October 2, 1981, Veremey again arrived at the Software AG offices. While waiting for Lewis to return from lunch, Veremey continually wandered in and out of the Software offices despite the receptionist's request that he be seated. When Lewis arrived, Veremey gave her an order for all of Software AG's documents. At a price of about $400, the documents would fill about 12 boxes. This type of technical documentation tells one how to use various systems produced by our company. One would have no use for this unless you have the system or are planning on acquiring it; or you are attempting to develop the system via knowledge of user techniques.

In response, Lewis told Veremey that she could not sell him the documentation. She added that, if he insisted, she would have to first go to the appropriate Federal agency to secure the necessary licensing. Veremey laughingly asked Lewis, "What license was issued for the U.S.-U.S.S.R. wheat deal?" He left and, to my knowledge, has not returned since.

Our experiences with both Mr. DeGeyter and, most recently, Mr. Veremey, have increased my frustrations with the current lack of adequate legal protections for American high technology. Despite the fact that software technology is the recognized key to future computer development—and we have the lead—the United States has no current statute which, in my opinion, adequately protects this technology.

To the average businessman, the Export Administration Act and its concomitant regulations are, simply speaking, a terrible hassle. Most industry representatives know that a license is required for trade with the U.S.S.R. Few, however, know which other nations, if any, require export licenses from the Commerce Department. The U.S.S.R. is not, of course, alone in efforts to transfer technology: Our own company has also reecived inquiries on ADABAS from Hungary and Poland. In both instances, we have declined to transact any business.

As for the controlling export lists, when approached by DeGeyter I did not know if any of my products were specifically included on those lists; I strongly suspected, however, that they might well have been. The information currently available to business on U.S. export laws, regulations, and policy in this area is negligible, despite the fact that businessmen are the real key to detection and enforcement.

Senator NUNN. Based on your experience, do businessmen in this area have much knowledge of what the Commerce Department is doing?

Mr. MAGUIRE. No; and I am very active in the Trade Association and my knowledge is very limited but I deal with my peers and their knowledge is negligible.

Senator NUNN. Do most of them know about the law limiting export?

Mr. MAGUIRE. Most of them. They know about the existence of a law. While a few large firms like IBM may be extremely familiar with the lists and regulations, those firms account for only 40 percent of a software market of $2.5 billion annually—estimated 1985 sales of $8 billion—the remaining 2,500 companies have 60 percent of the market. I suspect that representatives of most of those companies are no more aware of these laws and lists than I was.

Last, when businessmen such as I do get involved in the enforcement process, the results are oftentimes even more frustrating. In the *DeGeyter* case, I spent nearly 7 months dealing with a man openly working for the Soviets to purchase one of the most significant trade secrets in the U.S. software industry. Despite that fact, he was eventually charged only with misdemeanors under commercial bribery statutes. In my mind, it is entirely incomprehensible that the man was finally sentenced to a jail term of merely 4 months.

By comparison, I read newspaper reports of a Celanese Corp. employee who in June 1979 was convicted and sentenced to a term of 40 years for selling trade secrets to Mitsubishi Plastics Co., a Japanese competitor of Celanese. From the scant newspaper reports, I can glean no evidence of national security interests or Soviet involvement. In sum, a businessman receives 40 years for selling trade secrets to a competitor while a Soviet agent receives 4 months for attempting to transfer one of our most guarded technology secrets to the U.S.S.R. It is, indeed, a sad state of affairs if those cases accurately reflect his country's priorities on technology transfer.

I would like to also point out in our industry the major trade association is called the DAPSA and they have put together a paper addressing the problem of trade secret protection and the difficulties with the current U.S. Copyright Act. We are submitting that position paper to the House Subcommittee on Courts and Civil Liberties, but I would be happy to make it available to your staff also because I think it is the kind of thing that we are looking for in terms of protecting—the basic problem is the new copyright law raises some issue as to whether we really have protection under trade secrets and to get a copyright we have to file the source card. Once you disclose, then you lose your rights under the trade secrets laws.

I don't have it with me today but I will forward it.

Senator NUNN. We would like to see that. It will be very helpful.

Thank you very much, Mr. Maguire. You mentioned the Software AG, your company, received inquiries on your source card from both Hungary and Poland. Were those made after the DeGeyter incident?

Mr. MAGUIRE. Yes, I have some thoughts on it. The Hungarian attempts were threefold. Initially the Hungarian Embassy in Washington, D.C., contacted our Reston office. We declined their request to purchase a license. I next learned that the Hungarian Diplomatic Corps in Germany contacted our German branch. In Germany, the Hungarians offered to pay up front the full license fee in advance for

a copy for license of ADABAS. Our company refused to sell. Finally, the Hungarian Embassy in Tokyo, Japan, contacted our Japanese distributor and made the same request. The distributor, on my instructions, declined to sell.

Senator NUNN. After that experience, was there any doubt in your mind the Soviets were working with the Hungarians and Polish in this effort?

Mr. MAGUIRE. There is too much of a coincidence. In a concentrated effort, this all happened within a period of 4 or 5 months, so when we refused here, it popped up in Germany and a couple of months later it popped up in Japan. The fact DeGeyter told me of the existence of a priority list that the Soviets were after and the source code of our program had been on there 3 years and the priorities just changed and they were pressuring him.

Senator NUNN. Thank you very much.

Senator Cohen.

Senator COHEN. An observation, Mr. Chairman. What is so striking about your testimony, Mr. Maguire, is that the fact the cynicism is so deeply ingrained and almost richly deserved. Apparently the Soviets and their agents, in this case, believed that you were prepared to sell out your company in order to beat out your competition. In other words, what I am saying is, you dangled out to Mr. DeGeyter the fact you were concerned about not letting this information get out to your competition. He apparently went along with you for some 7 months during the negotiations under the belief that eventually you would sell the ADABAS to the Soviet Union provided it wouldn't get out to the competition in this country.

What I am suggesting to you is the cynicism is so deep in the Soviet Union, to go back to the statement about they will sell us the rope to hang us, it just struck me as I sat here listening to you. They were under the belief that you would eventually sell out your country in order to beat out your competition provided your competition didn't get the system.

That is to me one of the most striking aspects of your testimony in addition to your own honesty and patriotism which I commend you for. We have seen, for example, another witness who did, in fact, sell out his country in order to achieve some measure of personal gain and you are to be commended for resisting that particular temptation.

Mr. MAGUIRE. Thank you.

Senator NUNN. Do you have any suggestions other than those you have made in your testimony about how the Government can better work with the private sector in protecting our technology?

Mr. MAGUIRE. The technology is changing very, very fast. It is very difficult to keep up with it in spite of the discussion this morning here about a group, a clearinghouse staying on top of it. But I think Government communication with high technology companies is the best way to spread this information about the risk to the national security and direct through trade organizations and specialized markets.

The computer industry happens—the ADAPS headquarters are right over in Rosslyn. I doubt whether that headquarters has had any dialog at all with Commerce.

Senator COHEN. I just make one other point, it is not only something that afflicts small businesses within the field. If you really want an edu-

cational experience, you ought to read the book called "The Snowman and the Falcon" which details the activities of one Christopher Boyce and friends of his who were successful in getting some of our most treasured secrets. The Rhyolite and the the ARGUS, are two satellite systems we spent a good deal of money on in terms of research and development and they ended up in the hands of the Soviet Union through their embassy in Mexico. That might be an educational experience to show you to what extent and how easy, how absolutely easy it was to penetrate the so-called black vault at TRW, one of our major companies in this field.

Mr. MAGUIRE. Thank you.

Senator NUNN. Thank you, Mr. Maguire. We appreciate all your help and we commend you for your alertness and for your patriotism and willingness to cooperate with not just this subcommittee but the executive branch in preventing this kind of transfer from taking place in your case.

Mr. MAGUIRE. Thank you.

Senator NUNN. Our next witness is Mr. Theodore Greenberg, Assistant U.S. Attorney, Eastern District of Virginia, Alexandria.

Mr. Greenberg was the prosecutor in the *DeGeyter* case we just heard about.

Mr. Greenberg, will you be accompanied by anyone else testifying or just you?

Mr. GREENBERG. Yes. I have John L. Martin from the Internal Security Section with me.

Senator NUNN. Of the Justice Department?

Mr. GREENBERG. Yes.

Senator NUNN. Will both of you be testifying? If so, I will have both of you hold up your right hand.

Do you swear the testimony you will give will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. GREENBERG. I do.

TESTIMONY OF THEODORE GREENBERG, ASSISTANT U.S. ATTORNEY, EASTERN DISTRICT OF VIRGINIA; AND JOHN L. MARTIN, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Senator NUNN. We heard about the *DeGeyter* case, and of course, you were prosecutor in this case. I know you have got a long statement which we will put in the record giving all the details on this case. We would hope you would be able to summarize it, tell us what you know about it, and then we will go to questions.[1]

Mr. GREENBERG. I have picked some significant parts of the statement, Mr. Chairman, and I would like to point them out to you.

On May 22, 1979, the Federal Bureau of Investigation received information from John Maguire, president Software, A.G., Reston, Va., regarding the attempted bribery of one of his employees by Marc Andre DeGeyter, a Belgian national, who stated that he was acting on behalf of the Russian Government. DeGeyter wanted to steal Software's trade secret, the ADABAS source code.

---

[1] See p. 432 for the prepared statement of Theodore Greenberg.

An FBI investigation, which included the use of an undercover agent and consensual monitoring, resulted in DeGeyster's arrest at John F. Kennedy International Airport on May 18, 1980, when DeGeyter gave an undercover agent a check for $500,000.

The investigation was monitored primarily by the Internal Security Section of the Department of Justice. Prosecution of the case was directed jointly by the U.S. Attorney's Office for the Eastern District of Virginia, and the Internal Security Section.

The investigation was originally conducted as a foreign counterintelligence operation and then as a criminal investigation.

DeGeyter was indicted on June 9, 1980, for violating title 18, United States Code, section 1952(a)(3), interstate and foreig[illegible] aid of an unlawful activity; that is, commercial bribery, in violat[illegible] laws of the State of New York and the Commonwealth of Virginia. Because of significant governmental considerations, DeGeyter was permitted to plead guilty to misdemeanor violations of the Export Administration Act and the Virginia commercial bribery statute. He was incarcerated prior to the hearing in the Alexandria City Jail and served his Federal sentence at the Federal Correctional Institution, Petersburg, Va. He served a sentence of 4 months, was fined $500; and as part of the plea agreement paid a $10,000 civil penalty to the Department of Commerce.

Senator COHEN. Mr. Greenberg, we can almost get that amount of fine and penalty for shooting a deer out of season in Maine.

Senator NUNN. I agree with that observation. You heard Mr. Maguire's testimony about how frustrating it is to be working on this problem for as long as he did, cooperating completely with the Government and DeGeyter ended up with a 4-month sentence.

We recognize there may be reasons that we do not know about in that respect. Could you tell us what the reasons are for switching from a felony to misdemeanor?

Mr. GREENBERG. There were significant governmental considerations which I would be happy to disclose to the subcommittee in a closed session.

Senator NUNN. We will respect that and any further questions about why we will go into closed session.

But I think it is very important for people like Mr. Maguire and others who have cooperated to the maximum extent possible to know what happened and why. After all, they are out there protecting the governmental secrets. He spent a lot of his time, and I am sure he felt at certain periods of time it might have been at his own risk financially, as well as otherwise, to bring this case. The Government has a lot of interest. One area of overwhelming interest is to get busin[illegible]ses to cooperate like Mr. Maguire did. So you have to weigh that against all the interests that the Government has.

We certainly would be interested in hearing that in closed session at the appropriate time.

Mr. GREENBERG. The interests were weighed. One of the things that we look to, in prosecuting, is the sentence that is given; which in the federal system is the sole prerogative of the district court. There was a 1-year penalty which could have been imposed. The court declined to do that. Nevertheless, there are other benefits from the prosecution.

The public becomes aware of it. There is a deterrent effect arising from the prosecution, and there is publicity and the public is informed.

Senator COHEN. I am not going to delay this too long. I know we have some time constraints. Frankly, I am aware of a young man who is being charged with tampering with an automobile vehicle right here in the District. He faces a $1,000 fine and 1 year in jail just for taking a tire off an automobile. I would say there is a much different level of threat to our society in terms of stealing an automobile tire and taking major trade secrets of this country.

You are not part of this, Mr. Greenberg, but Senator Nunn has been sitting on hearings in front of this subcommittee for a number of years now. We have had hearings on chop shops where we have a vast network of organized crime operating in this country. We have had hearings on illegal drugs coming into the country and we have had hearings now on technology transfer and there is a commonality of issues involved, Mr. Chairman, as you know. There is, very little risk of being detected, little risk of being apprehended in the commission of a crime; even if you are apprehended and charged, there is little risk of conviction; and when you are finally convicted, there is very little risk of getting a substantial penalty, all of which has contributed to the increase in crime in this country. It seems to me we have the same situation here where you have got a major attempt to acquire a very sophisticated system and you end up with a penalty that is less than you would get for taking a deer out of season in Maine.

Mr. GREENBERG. Senator, we share those concerns. The indictment exposed Mr. DeGeyter to 40 years in prison, had he been convicted on all counts, and a substantial fine.

As I indicated, in this case there were interests which required us to dispose of the case other than through a trial.

Senator COHEN. I understand. The same interests were also present during Christopher Boyce's trial. There was very serious consideration given to dismissing the trial altogether because they didn't want to get into disclosing the ways in which they apprehended the individuals. It is always the situation when you apprehend somebody who is engaged in espionage in this country that you might disclose the methods used to acquire that information. But it does not serve as much of a deterrent I wouldn't think, to a responsible businessman to spend 7 months, maybe more than 1 year of his time, cooperating with the FBI. It would certainly be frustrating then to have this individual who might have tempted somebody within his organization or another company that had access to that software and to realize that you can spend 1 year of your time and still see a fellow come out of jail 4 months from now with a $500 fine. That is not much of a deterrent.

Senator NUNN. Let me just add to that.

I agree with what Senator Cohen has said. I also recognize that in a case like this the policy is made at higher levels and that you have your own responsibility to comply with whatever the Department of Justice decides.

I also recognize the Department of Justice has to coordinate with other intelligence agencies.

My frustration is directed toward the overall policy. When we get into closed session, which we will, we will be looking very carefully at that because I am sure that there are overriding reasons in many of these cases involving perhaps sources, methods, and other things that have to be kept secret. But if in the final analysis the citizens of the country and the businesses of the country lose faith in the judicial system then the damage done to the overall protection of America's secrets and technology would probably be far greater than disclosure of a particular classified bit of information at that time. So there has been an overriding kind of protection of sources and methods or some overriding intelligence reason in my view to warrant the kind of very minimum sentence that came out in this case.

But again we repeat, I know that decision was not made at your level and we will talk to you about it and we will trace it right on up the line, see where the decision is made and we may agree with it when we get through. But we very well may not. I think Congress has a role to play in this overall kind of policy, too. Certainly not while the case is going on, but certainly after it is over we do and as far as policy in future cases.

Mr. GREENBERG. Senator, I would like to add, if I may, that there was consideration given in our internal deliberations as to whether or not the case should be dismissed in its entirety. We decided to proceed as set forth in the plea agreement. So I guess on balance it is not a total loss, as you would view it.

As I understand it, DeGeyter was the first individual to actually serve a prison term for violation of the Export Administration Act.

Senator COHEN. If I had that choice, I would make it a tough one. I would give him the maximum, just to make sure that the jail sentence is a deterrent; don't give him a 4-month sentence, give him a tougher one.

Mr. GREENBERG. The plea agreement did not permit the Government to choose the sentence. That was left to the discretion of the court.

Senator NUNN. Speaking of that, what was the bail in this case? I understand your original indictment was for a felony. Is that right?

Mr. GREENBERG. That is correct.

When DeGeyter was arrested in New York, the Government requested that the New York magistrate set bail at $500,000. When he was indicted in the Eastern District of Virginia, bail was also set at $500,000. When DeGeyter was arraigned on the felony charges, that is, the Travel Act, the bail was reduced over the Government's objection to $100,000.

Senator NUNN. Would you give me the name of the judge in New York? Was there a bail originally set in New York?

Mr. GREENBERG. Bail was originally set on the New York complaint.

Senator NUNN. That was $500,000?

Mr. GREENBERG. Yes.

That was set by a magistrate in New York, by the name of John L. Caden.

Senator NUNN. When bail was set, was it transferred to Virginia, was this a separate account?

Mr. GREENBERG. In New York, they filed a Travel Act complaint. We decided that venue was more appropriate in the Eastern District of

Virginia; and we filed a complaint with the U.S. magistrate in Alexandria, Va. An arrest warrant was issued on that complaint; and bail was set by the Virginia magistrate at $500,000. DeGeyter was afforded a removal hearing in the Eastern District of New York; and ordered removed to Virginia.

At arraignment on the indictment the U.S. district judged reduced the bail upon motion of the defendant's counsel to $100,000.

Senator NUNN. Who was that judge?

Mr. GREENBERG. That was Judge Albert V. Bryan, Jr.

Senator NUNN. Was there a reason he gave for making that reduction to $100,000?

Mr. GREENBERG. He stated that the Government had not charged DeGeyter with espionage and therefore he didn't feel that $500,000 was warranted.

Senator NUNN. What was the defendant charged with?

Mr. GREENBERG. The defendant was charged with eight counts of interstate travel to carry on an unlawful activity, in violation of laws of the State of New York and Virginia, that is, commercial bribery. The underlying offense of commercial bribery in both New York and Virginia is a misdemeanor. Nevertheless, the Federal statute provides in part, that if you travel in interstate commerce to violate certain State laws, including bribery, the travel constitutes a Federal felony.

We pointed out to the judge the circumstances of the arrest and the fact that this individual was a foreign national with absolutely no ties to the eastern district of Virginia or to any community in the United States; and that he had no American national who would speak on his behalf. Nevertheless, the judge made the determination that in his view $100,000 was sufficient.

Senator NUNN. Did you reveal anything else to the judge?

Mr. GREENBERG. No, sir.

Senator NUNN. What is that?

Mr. GREENBERG. No, sir. Not at that time. Subsequent to the judge setting the bail at $100,000 DeGeyter's attorney arrived, the actual dates are set forth in the statement, arrived in the clerk's office with a cashier's check for $100,000, just about the same time that I had received information from the New York office of the FBI, that DeGeyter had indicated that he was a KGB agent and that he would flee the United States if he was able to raise bail money.

I went to the judge——

Senator NUNN. Where did you get that from?

Mr. GREENBERG. That came from the FBI, informant information which was—the source of the information was never disclosed in court. What I am telling you now is a part of the public record.

I arrived at the courthouse about the same time that the $100,000 check did. I asked the judge to hold what is called a "Nebbia" hearing. Nebbia was a case decided by the Second Circuit Court of Appeals which deals with a judicial inquiry by the court to determine the sources of funds when cash is being used so that the court can assure itself that the money is sufficient to insure that the defendant will return for further proceedings.

The mere circumstances of somebody posting a large amount of cash in an anonymous fashion raises questions as to whether or not he will

flee the jurisdiction of the court. So there is a procedure to have a hearing. We asked for the Nebbia hearing as well as an increase in the bond.

The judge denied our request for an increase in the bond and held a hearing in which he allowed Mr. DeGeyter to explain that he would not flee the jurisdiction, but the judge would not permit me to make the defendant prove what the source of his funds was.

All we knew is that it was cash.

Senator NUNN. What happened after he was told that you had the informant or confidential source revealing DeGeyter himself was a KGB agent?

Mr. GREENBERG. We had a hearing on that. I put on an FBI agent who related that information to the court.

Senator NUNN. Before he got out?

Mr. GREENBERG. Yes.

DeGeyter took the stand, denied making the statement. The judge let him go.

In this particular case DeGeyter remained within the jurisdiction of the court and returned for further proceedings.

Senator NUNN. Are judges reluctant to grant those Nebbia hearings?

Mr. GREENBERG. It has been my experience in the Eastern District of Virginia that the judges have not been granting our requests for full Nebbia hearings.

Senator NUNN. Why is that?

Mr. GREENBERG. They don't feel that it is necessary. They really don't give us a reason for the denials. But the Nebbia hearing is a good idea. It would be my personal opinion—and the subcommittee might want to study an amendment to the Bail Reform Act which would require a judge to hold a Nebbia-type hearing where you have a foreign national who may flee the United States. That is something you might want to consider.

Senator NUNN. We certainly will consider that.

We have got a lot of legislation pending on that very subject. I don't know whether you are finished summarizing or not. We interrupted you.

Mr. GREENBERG. No; I didn't get very far. I wanted to set forth a number of points which are in my statement. I will just go through them quickly.

DeGeyter dealt both in the United States and outside of the United States through a number of corporations; he primarily dealt with a corporation called Commercial Engineering and Sales Agency, or CESA. He listed himself as the president of the TVS Broadcast Systems. All DeGeyter's corporations, with the exception of two California entities, which I will mention, are located at the same address in Belgium.

So we have TVS Broadcast Systems; he listed himself as the president of Afrabel, African-Belgium, a corporation from Brussels; managing director of Softelectronics in Brussels, then in the United States through investigation we determined that he was a partner in a joint venture called In-Mark Associates, in Irvine, Calif., and another joint venture called Inutec in Laguna Beach, Calif.

We have heard the testimony of Mr. Maguire. Just in summary, I would say that DeGeyter constantly upped the ante, if you will, they

started at $150,000, went to $250,000, talked about $400,000, DeGeyter finally offered them $500,000. It is absolutely clear from reviewing all of the evidence, including the transcripts of consensually monitored conversations, that DeGeyter wanted Maguire to steal from his own company and from himself a trade secret which we have determined through discussions with Mr. Maguire was worth about $10 million.

For instance, on July 20, DeGeyter is talking with Maguire and they are discussing how the payments should be made. He says, "Want a check in Zurich? You got it. It's yours. I couldn't care less. I'm not involved." Later in the same conversation he says to Maguire, "It's a one-time shot. No paper, no contract, nothing." Be straight, under the table. What he was saying was that the source code was going to Russia, that Maguire's competitors would never know about it. He insisted upon having the source code brought out of the United States. He explained to Maguire that it would be examined or verified by a Russian computer expert in Brussels, then the tape would be sent to Moscow.

Through subsequent investigation we determined that he said on another occasion that he intended to give the tape either to a Russian employee at the Embassy in Brussels or to an Aeroflot employee for direct transfer to Moscow.

He explained to Maguire that after the source code was verified he would take Maguire to Switzerland and Maguire could have the payment in any fashion he wanted it. He could put it in a bank account, he could have cash, DeGeyter even suggested that he could arrange for the transfer of land in California.

Anything that Maguire wanted, he would do. He suggested that if Maguire wanted to, he could even negotiate through Techmashimport, which is a Russian trade corporation which I will get into later, on whose behalf DeGeyter said that he was dealing for.

Maguire constantly raised a concern about whether or not this was a proper thing to do, the export of this source code and whether or not it could ever be traced to him. The transcript of one of the conversations, it is instructive on this point.

On August 7, 1979, there was a conversation between Maguire and DeGeyter. Maguire says:

> This source code, my understanding is that as far as moving something out of the United States, you know is maybe an administrative technicality. Do you know about the export licenses and everything? What if you get caught with that source code?

DeGeyter responded:

> I don't think there should be any problem in that. I would then take the whole responsibility for that. You are not supposed to know where it goes to and what I'm going to do with it.
>
> MAGUIRE. OK, is there any way they can trace it——
>
> DEGEYTER. No.
>
> MAGUIRE [continuing]. Back to us?
>
> DEGEYTER. No, no way whatsoever. There is really no way, nothing. But you know you have to trust me on it. I am telling you there is no way.

Then he goes on to say they will test it in Brussels and go to Zurich.

There comes a point in time where the negotiations between DeGeyter and Maguire break down. This is toward the end of 1979. The transaction is not going to take place. There is an impasse.

On February 4 and 5, 1980, special agents of the Federal Bureau of Investigation interviewed DeGeyter in his hotel room in New York and told him that they were investigating possible violations of the Foreign Registration Act.

Subsequent to that, DeGeyter changed his approach, if you will, and he goes to an individual by the name of Charles Matheny, who is in the same office complex as Maguire's software company. Matheny is president, and chairman of the Board of CENTC, which is a Virginia corporation. Matheny immediately reports the contact to the FBI. Like Maguire, he agrees to cooperate with our investigation by recording conversations and meetings with DeGeyter. DeGeyter uses a different approach this time. He now says that he is dealing with a Saudi Arabian sheik, that he has become involved in an Arab bank, and that they are going to implement a large-scale computer operation.

Senator NUNN. Was this before or after ABSCAM?

Mr. GREENBERG. This is before ABSCAM. In fact, there is no Arab sheik. What he does is he changes his approach in order to mask his efforts. He wants Matheny to act as a middleman. He wants Matheny to go out and compromise one of Software's employees and he offers Matheny a finder's fee, if you will, for doing that.

Matheny and Maguire sit down with the FBI and it is agreed that an FBI agent by the name of Timothy Klund will pose in an undercover capacity as an employee of Software AG. Mr. Klund used his own name, and posed as a computer expert working for Software.

Thereafter on April 16, 1980, April 18, and some additional dates, Klund met with DeGeyter at various places in northern Virginia and the same scenario, unfolds with Klund as had with Maguire. DeGeyter starts to escalate the price, starting with $200,000, and as Klund indicates his reluctance to go along, we finally have an offer of $500,000. DeGeyter insists again that the transaction take place overseas. Klund refuses.

It is finally agreed to meet in New York on May 18, at which time DeGeyter is supposed to be arriving from overseas with $500,000 in cash; although he had earlier expressed concern about coming through customs with that much cash. But he tells Matheny that he will come with the cash.

In preparation for that meeting, the FBI laboratory produced a set of dummy computer tapes in order to make the exchange. On May 18, DeGeyter arrived at JFK International Airport from Brussels, Klund and DeGeyter met. The meeting was surveilled by other special agents of the FBI. The exchange was made, except instead of $500,000 in cash, Mr. DeGeyter gave the agent a $500 000 check. Subsequent investigation showed that there was only $800 in that particular account.

Again, a clear intent to steal, even from another thief, the source code.

DeGeyter was arrested by the FBI and in my statement I set forth the chronology of subsequent legal——

Senator COHEN. Which account was that drawn on?

Mr. GREENBERG. That was drawn, it is attached as exhibit 1, I believe, to my statement, page 17. It was drawn on the Swiss Credit

Bank and it is a personal check of Mark DeGeyter. He put a signature across the front of the check to make it appear to be some sort of a bank check or cashier's check. But it comes from his personal account and when we made inquiries with Credit Bank's New York office, they advised us that at the time of the transfer there was only $800 in the account.

Senator NUNN. I am going to turn it over to Senator Cohen.

I am going to have to break until 1 o'clock at which time I will come back and Senator Cohen, if you could finish up Mr. Greenberg, whatever you would like to do, Mr. Southard is our next witness. I would think if you have to leave at that time, it would be better if we could come back at 1 o'clock for the next witness, Mr. Southard, deputy district attorney from Santa Clara, Calif.

Just a couple of questions. Was the Commerce Department involved in an investigation and prosecution of the *DeGeyter* case?

Mr. GREENBERG. No, Senator. They were not.

As I indicated before, the investigation was predicated first upon a foreign counterintelligence interest; it then moved into criminal violations of the Travel Act and Registration Act. The Commerce Department does not have jurisdiction under these criminal statutes. They did not become involved until the plea was taken. The plea included a provision for the Commerce Department to commence denial proceedings against DeGeyter.

Senator NUNN. Was the fine as part of the plea that Mr. DeGeyter was supposed to pay, payable to the Commerce Department?

Mr. GREENBERG. Ultimately, yes. The plea agreement worked out with the U.S. Attorney's Office, provided that he would pay a $10,000 fine. That was subject to the administrative mechanism of the Commerce Department, actually assessing that fine. He deposited with the U.S. Attorney's Office a $10,000 check, payable to the Treasurer of the United States. That was done in August. In December the Commerce Department formally assessed the $10,000 penalty pursuant to their administrative regulations and the check was forwarded to them.

Senator NUNN. So they did collect the money?

Mr. GREENBERG. Yes.

Senator NUNN. After how many months?

Mr. GREENBERG. Between December and—they collected it, I think, December 24.

The money had been deposited, the actual documents are in my statement, but my recollection is on or about August 1.

Senator NUNN. Did DeGeyter have to have an export license to operate in the field he was operating in?

Mr. GREENBERG. It is my understanding that the source code would have required a validated export license. It was not a classified item. So he would not have needed a munitions control license to export. But he would have had to check, because licensing is on an item-by-item basis.

Senator NUNN. If a foreign citizen engages in the export, do they have to get a personal account for an exporting license? Is he a licensed export agent? Is that the way he would be licensed, or is he licensed at all?

Mr. GREENBERG. I can't answer you directly, Senator.

Senator NUNN. Does the Commerce Department have any kind of list of export privileges.

Mr. GREENBERG. It is my understanding they have a published list of people denied export.

Senator NUNN. For various reasons?

Mr. GREENBERG. Yes, sir. I never examined the list myself. I don't know the form which it takes. I do know in this particular case, they intended to put him on the denial list.

Senator NUNN. Do you know if they put him on the denial list?

Mr. GREENBERG. It is my understanding that as of April 22, 1982, he has not been put on the denial list.

Senator NUNN. When was he convicted?

Mr. GREENBERG. August 1, 1980.

Senator NUNN. That is what, a year and a half later?

Mr. GREENBERG. Yes, sir.

Senator NUNN. And he is still not on the Commerce Department denial list as of August 22, 1981.

Mr. GREENBERG. Yes, sir.

Senator NUNN. That means DeGeyter can come back into this country and begin doing business again, as far as you know?

Mr. GREENBERG. As far as I know, he could come back into the United States. If he wanted to export something, he would have to apply for an export license and he is not on the denial list so I assume they would handle it in whatever procedure they follow.

Senator COHEN. What if he just wants to steal something?

Mr. GREENBERG. If he wanted to steal something again?

Senator COHEN. Didn't you recommend he be deported from this country?

Mr. GREENBERG. Yes, sir, I did.

Senator COHEN. What was the response to that?

Mr. GREENBERG. After he completed his sentence in Petersburg, he was released to an Immigration and Naturalization detainer which had been lodged because while he was incarcerated, his visa had expired. I requested that he be immediately involuntarily deported. INS advised me that because he had been convicted of a misdemeanor offense, not involving moral turpitude, that he was not required to depart the country involuntarily.

Senator COHEN. And then reenter the country voluntarily.

Mr. GREENBERG. That is my understanding.

Senator NUNN. What is your experience in dealing with the Commerce Department in this whole area? Do you have any observations, any personal viewpoint on that subject? Are they capable of handling the Export Administration Act as now charged by law?

Mr. GREENBERG. I don't think I would be the proper one to answer that, Senator. I just had the one case come up and I am currently assisting on another Export Act case. I just don't have a sufficient basis to answer that.

Senator NUNN. We have Justice Department representatives here this morning. Does the Justice Department have any comment on whether the Commerce Department is the right agency——

Mr. MARTIN. No, Mr. Chairman.

Senator COHEN. Let me ask you what your experience is in dealing with the Commerce Department as to whether the source code was even on the list?

No. 1, you were reluctant to prosecute the case under the Export Control Act, weren't you?

Mr. GREENBERG. The initial decision to charge under the Travel Act was made because we felt that at that time it would give us the greatest charging flexibility. During the course of the investigation, the penalties under the Export Act changed. Part of the penalties changed from a misdemeanor to a felony.

Senator COHEN. What did you originally charge him with initially?

Mr. GREENBERG. He was initially charged with violations of the Travel Act which carries a penalty of 5 years imprisonment and/or $10,000 or both. We felt at that time that gave us the greater flexibility in terms of proving the case.

Senator COHEN. Why did you avoid proceeding under the Export Administration Act?

Mr. GREENBERG. At the time the initial decision was made, we had some concerns about whether or not there was a sufficient factual predicate to show whether or not there was an export. As I say, the law was changing, it was complex, we had a number of different factors going at once and we just decided it was best to proceed under a different statute.

[At this point, Senator Nunn withdrew from the hearing room.]

Senator COHEN [presiding]. Was there any question in the minds of the Commerce Department as to whether or not the ADABAS source code was on the list of controlled items?

Mr. GREENBERG. It is my understanding through the FBI, the Commerce Department had told us that—in order to export the ADABAS source code, DeGeyter would have had to have a validated export license, and they make that determination on an item-by-item basis within the broad rubric of the definition set forth in the Export Administration Act which, as I recall, has a definition of technology, and so they made a determination that the ADABAS source code was high technology.

So to export it you would need a validated export license. If you look down the list of things for which you need an export license, you don't see the ADABAS source code, you see broad categories and then you have to ask them to make a determination, licensing determination, if you will.

Senator COHEN. Was there any hesitancy on their part to include the ADABAS as part of the controlled items?

Mr. GREENBERG. I don't think there was.

Senator COHEN. So from the very beginning they said it was subject to export license control?

Mr. GREENBERG. That is my understanding. When we in the investigative family finally understood ourselves what the source code was, the source code as opposed to the object code, the Commerce Department indicated to us it would require a validated license.

Senator COHEN. As I understand it, the negotiations broke down on the place of delivery, that it was to be delivered out of this country rather than in this country. Obviously you had been in touch with Mr.

95-929 O - 82 - 10

Maguire to be sure he hesitated and refused to go along with that aspect.

Why is that so?

Mr. GREENBERG. Once we decided that it should be pursued as a criminal matter we made a determination that it would be necessary to arrest him in the United States because if he left the United States, we would then have to deal with the problems of extradition; and extradition would depend upon which country he went to and what he was charged with. It is time consuming, and costs a lot of money to get somebody back. The offense was complete when they met at the airport and when the money was exchanged for the tape, we just decided to arrest him at that time rather than chase him over Europe.

Senator COHEN. I think it has been said this morning that our export laws are fairly outdated in view of today's level of technology. Specifically, it is very difficult to detect microchips. So assuming we create a new Office of Strategic Trade, assuming we put the control for inspection in the hands of the customs officials, assuming we enhance our inspection personnel at all exit points, what are the chances of those personnel detecting something as small as this or the tape in the case of Mr. Maguire?

Mr. GREENBERG. It is my understanding from talking with Maguire and other computer experts that it would be virtually impossible for anybody to detect the information contained in the computer tape being taken out of the country. Obviously, if on exit from the United States, a border officer opened the briefcase and saw the tape, he would know that it was a computer tape, but he would have absolutely no way of knowing what was on the tape. Even if he put the tape on a computer, it still would have only shown him a series of numbers.

Senator COHEN. You seized some other items in Mr. DeGeyter's possession indicating ties with the Soviet Union. What were those items?

Mr. GREENBERG. I will submit Xeroxed copies to the subcommittee. We seized, pursuant to search warrant, numerous items from his briefcase. One including his Belgium passport which had a Soviet visa in it which showed that he was traveling to the Soviet Union for commercial purposes; that the agency sponsoring him was the "Ministry of Internal Technology, Technical Machine Import," located in Moscow and that it was valid until May 11, 1980.

In addition to that, we found a number of telexes in his possession mostly to an individual known as Bolshakov, in the Soviet Union. Our understanding is that the telexes were directed to Techmashimport.

For example, one of the telexes is,

> Money has been received by my bank this morning. I need the money for Item 6 as agreed in Switzerland no later than May 8th in order to guarantee the replacements May 11. Best regards, Marc.

Another of the telexes sent to Mr. Bolshakov, read,

> Dear Sir, due to the holidays your embassy will provide my visa only by May 14. I will arrive in Moscow on May 19. Hope to catch you for dinner as usual. Best regards, Marc.

These were all in the time he was dealing with Maguire and Matheny. Another telex, again to Bolshakov,

> Dear Sir, 60 kilo samples will arrive May 15, flight."

And he lists the flight number.

Freight to be paid by you. Best regards, Marc.

July 24, 1979, again to Bolshakov.

Dear sir, after my last visit to the supplier, could you agree to accept next week? Release 3.1.4 regarding Item 4? Please confirm. Best regards.

And then there is one additional one, as I recall.

We also seized from him a copy of a contract in English between his company, CESA, on the one hand, and Techmashimport in Moscow on the other hand, and it called for the delivery of certain pieces of computer equipment. We seized from him what appears to be a credit document from the Swiss Volksbank showing that on March 19, 1979, in Zurich there was on deposit for his use $450,000 U.S. money.

We also seized from him what he called a "delivery acceptance protocol" dated April 11, 1979, showing that certain items were delivered to Russia and that he was to be paid $250,000 for that.

We also seized from him a number of airplane tickets which confirmed his travel to Moscow. In fact, one dated April 15, 1980, showed travel, Moscow to Vienna to Brussels to New York and to Washington.

Senator COHEN. Do you believe he was, in fact, a KGB agent?

Mr. GREENBERG. We will never know that, sir. All we know is what the documents——

Senator COHEN. I am just wondering. It seems to me kind of inconsistent, frankly, that any agent would be carrying these documents in his possession.

Mr. GREENBERG. We know he was in contact with the Russians and with this particular corporation. Exactly who or why they asked him to get these items we were not able to discover.

Senator COHEN. What have you done with respect to the other companies that are listed as his contacts?

Mr. GREENBERG. In going through his papers there were a number of other corporations we discovered, in particular six.

Senator COHEN. Would you identify them?

Mr. GREENBERG. Tritel Corp. and Flair Leasing, formerly Compufile in Irvine, Calif. During the time of our investigation, DeGeyter approached them and wanted to purchase what is called a Rolm, R-o-l-m, computer which has been identified to us as a military specification computer which is embargoed from export. He also wanted to purchase a microprocessor chip, and was known by that company to buy such things over the counter in cash, no sale was completed.

He approached Systems Magnetic Corp. in Anaheim, Calif., and wanted to purchase from them magnetic tape recorders which we have been told are used for satellite information retrieval. Each one of these recorders sell for $90,000-some odd dollars. The sale was not completed because the company was unsatisfied with his credit references.

He also approached a Keronix Corp. in Los Angeles, Calif. He approached Corland Corp. and Pay Television Corp. Both of those companies cooperated. They immediately advised the FBI, cooperated in our investigation and provided us with a taped conversation of a meeting.

He also approached the Industrial Machinery Division of Passauant Corp. in Birmingham, Ala. That was for the purchase of a magnetic tape slotting machine. My understanding is the corporation

did sell that machine to the Soviet Union and one of their officials traveled to Moscow and met with Techmachimport officials. DeGeyter was not present at the meeting but received a fee. He also approached the Intel Corp. in Norwich, Conn., and requested permission from them to represent their corporation at a trade show in Moscow; they declined.

Senator COHEN. With respect to each of those companies, I assume you have since contacted them to alert them to further attempts by people other than DeGeyter in contacting them for access to their technology?

Mr. GREENBERG. Yes, sir.

Senator COHEN. In your dealings with those particular companies, did DeGeyter indicate he was acting on behalf of the Soviet Union?

Mr. GREENBERG. He indicated he was acting for Techmashimport. He was quite open about telling everybody that he was working for this Russian corporation. What he made clear to Maguire, and I think it is instructive, is that if Maguire did not deal with him, there would be somebody else right behind him; somebody else coming along, and dealing for the Russians, who wanted to buy the same things. DeGeyter was saying, essentially, look, you might as well deal with me because there is going to be somebody, next place, next time.

Senator COHEN. What seems too brazen about it all, why didn't he just say he was representing a Belgium corporation or a Polish company or a Hungarian subsidiary?

Mr. GREENBERG. I think what he wanted to do, especially with the ADABAS code, about which he was talking about something that was a priority item. It was clear there was no way Maguire was going to release that thing in such a fashion so that it might fall into the hands of his competitors. By playing upon the fact that he was taking it behind the Iron Curtain, over to the Eastern Bloc, he sought to assure Maguire that he didn't have to worry about it. I think that was his selling point. Look, fellows, you don't ever have to see this stuff again. They are just going to use it over there and nobody will know about it, because if it was thought it was being sold to one of Maguire's competitors, it is clear a deal wouldn't even have been a possibility.

Senator COHEN. That is what I mentioned before about the cynicism being so deeply rooted that they would even approach it on this basis, sell out your country to beat out your competitor.

Tell me quickly about the Techmashimport, is it? Are they registered with the Justice Department and how does that operate?

Mr. GREENBERG. Yes, sir. Techmashimport is registered under the Amtorg Trading Corp. The Amtorg Trading Corp. serves as an umbrella for approximately 45 different Russian corporations. Amtorg's head office is in New York City. Their most recent registration statement was filed in April 1974. That has been reported in the Attorney General's submission to the Congress.

Techmashimport is listed on its registration statement as a foreign trade corporation which imports equipment and machines of various types. We can submit a copy of the registration statement.

Senator COHEN. Just for my own edification, are these private companies or are they arms of the state?

Mr. MARTIN. They are Soviet corporations.

Senator COHEN. What does that mean?

Mr. MARTIN. Corporations are independent entities formed under the Soviet law, but for all practical purposes, they are formed by or under the auspices of some of the ministries, the Ministry of Trade, Ministry of Finance.

Senator COHEN. I was under the impression that accumulation of capital wealth was not permitted in the Soviet Union.

Mr. MARTIN. I don't think they are capitalistic oriented, Senator. They are entities for the purposes of carrying out business, such as the export-import business.

Senator COHEN. But on behalf of the Soviet Union?

Mr. MARTIN. On behalf of the Soviet Union.

Senator COHEN. So, in fact, any company doing business with this particular Soviet corporation or any one of the 46, whatever, should be put on notice, in fact, they are doing business on behalf of the Soviet State?

Mr. MARTIN. That's correct.

Senator COHEN. Those are all the questions I have, gentlemen. I am just determining whether we need to hold you for any private briefing of the staff or members on the plea bargaining aspect.

I am advised at some future time we would like to have the briefings as far as the aspects involved in the plea bargaining but that won't be necessary this morning.

The subcommittee is going to stand in recess until the hour of 1 o'clock.

[Whereupon, at 12:23 p.m. the subcommittee recessed, to reconvene at 1 o'clock the same day.]

AFTER RECESS

[Member present after the taking of recess: Senator Nunn.]

Senator NUNN. The subcommittee will come to order.

Our next witness is Mr. Douglas Southard, deputy district attorney, county of Santa Clara, Calif.

We appreciate you being here today. We appreciate all of your help and all of your splendid work in this very important area.

I followed it with interest through the staff for some time. We swear in all of our witnesses. So if you will hold up your right hand, do you swear the testimony you will give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. SOUTHARD. I do.

TESTIMONY OF DOUGLAS SOUTHARD, DEPUTY DISTRICT ATTORNEY, COUNTY OF SANTA CLARA, CALIF.

Senator NUNN. Thank you.

You have a statement.[1] We will ask you to proceed.

Mr. SOUTHARD. Thank you, Senator.

My name is Douglas K. Southard. I am deputy district attorney for the county of Santa Clara, Calif. I have been employed by the district attorney's office, the chief prosecuting agency in that county, for a period of 5 years. Prior to that I practiced general civil law for a

[1] See p. 475 for the prepared statement of Douglas Southard.

period of 2 years in a small law firm in the county. I am a graduate of Stanford University with a degree in philosophy, and of Hastings College of the Law, the University of California, having attained a J.D. degree in 1975.

Like many people in law enforcement, I have no technical background in the area of semiconductor manufacture or electronics in general, but have, of necessity, learned some of the basics of the industry which was necessitated by my involvement in high-technology-theft prosecutions.

In the district attorney's office, I have been assigned for a period of 3½ years to felony prosecutions. For the last 2 years, my primary assignment has been high technology thefts, including trade secrets thefts, integrated circuit thefts, electronic equipment thefts and the investigation and prosecution of related criminal conspiracies.

In learning the technical necessities of this area, I have been greatly assisted by numerous people in law enforcement and in the industry itself; and particularly, have received training and assistance from Intel Corp., Signetics Corp., National Semiconductor, Synertek Corp., Hewlett-Packard Corp., and the NBK Corp.

Investigation agencies with whom I have closely worked investigating and prosecuting these cases primarily have been the organized crime and criminal investigation section of the Santa Clara County Sheriff's Office, the Federal Bureau of Investigation, and the Santa Clara County Police Department, with notable assistance from the Los Angeles and Orange County Sheriff's Departments, U.S. Customs Service and the Department of Commerce.

The preeminent police expert on these matters in our county is Detective Patrick Moore of the sheriff's office.

In the last 2 years, we have investigated literally scores of technology-related theft cases, resulting in numerous convictions, but also, sadly, numerous unsolved thefts or thefts wherein the property was never recovered.

Like you, we in local law enforcement are very concerned with the national security implications of the technology thefts that we have seen. However, as our expertise is in the field of investigating and prosecuting these crimes, and not in the international ramifications thereof, I will limit myself in my comments to the problem as seen by the local investigator and prosecutor and some suggestions as to where law enforcement has to go to help stem the tide.

Senator NUNN. I know we have Mr. Wu in the room. He has cooperated with our staff. He was scheduled to be our witness. The problem is we have got to get out of this room at 1:30. That means we will not have another witness today.

I also understand the Justice Department has problems with certain questions that we had planned to ask Mr. Wu. For that reason, I think what we will do is just put his statement in the record and we will dismiss Mr. Wu from being a witness today or in this hearing.

Senator NUNN. We do appreciate your being here. We appreciate your patience in waiting. I didn't want you to have to wait around to no avail. I understand Mr. Wu just walked in. I was just saying he was scheduled to be our next witness. We have got to give up this

room at 1:30. Therefore, we will not have time to have but one witness and I understand also the Justice Department had certain problems with questions we planned to ask Mr. Wu, particularly some of his personal opinions.

I don't want to put him in an untenable position. This was contrary to what my understanding was as far as his testimony. I think it is also contrary to what we had discussed with the Justice Department officials.

Nevertheless, I don't want to put Mr. Wu in that position. We will put his statement in the record and we will not need him as a witness.[1]

Mr. MARTIN. Thank you, Mr. Chairman.

Mr. SOUTHARD. Senator, I assume that the subcommittee might like to have some technical information regarding semiconductors devices. I have included in my written statement the brief overview of the processes.

For present purposes, however, I will omit that discussion. I would however like to present to the subcommittee for their inspection a board showing the brief example of the different types of materials which are used in the integrated circuit manufacturing process.

I also have a photograph about 100 times magnification of a standard integrated circuit memory chip. I would point out to the Senator the particular integrated circuit package that is in the bottom center of that board. Significant numbers of these were stolen in a recent $3 million theft in Santa Clara County. Those particular parts are specifically made for military application.

The integrated circuit was invented in the late fifties and is a uniquely American development. It was first marketed in 1961 commercially and now the sales worldwide of this type of device are over $5 billion per year.

Continued development of integrated circuit memory chips have reduced the cost of information storage in computers 100-fold in the last 10 years.

In the late 20th and early 21st centuries, integrated circuitry will be as basic to industrial society as steel was in the 19th and early 20th centuries. Leadership in this technology will be vital to any nation who would seek to be a world leader of economic and military power.

In the wake of this new technology has sprung an industry centered in what has come to be known as Silicon Valley, that is, Santa Clara County, Calif., which is amongst the most fast moving and competitive in the world.

An individual who can build a better electronic mousetrap using this technology has potential immediate access to great wealth and recognition. Companies oftentimes spring up overnight based on one good idea and sometimes die just as quickly when that idea is overcome in the marketplace.

In fact, the leading semiconductor manufacturers in this country and in the world are often companies which didn't exist 15 years ago.

Now some are billion dollar corporations. Up to now, in my view, the rapid growth of these companies have prevented a proper assessment of their security operations and has caused a substantial lag in public and official appreciation of the national security implications of the new technology.

[1] See p. 510 for the prepared statement of Theodore Wai Wu.

According to the available evidence, in the past 5 years alone, a conservative estimate is that $100 million or more in electronic technology and product has been stolen in the Santa Clara alone. We in law enforcement have only recently almost stumbled over the problem. At the time we were not totally prepared to deal with it. Now we are beginning to make some headway.

Most of the thefts that we are talking about are perpetrated by or with the assistance of employees. Cases we handle involve technicians, inventory clerks, draftsmen and engineers. Quite commonly, security personnel are involved. They steal circuit designs, process information, precious metals and the chips themselves. There is also increasing propensity finished goods such as computer disk drives and desktop computers.

The modes of thievery are many. Sometimes burglary is resorted to. Sometimes truck highjackings or even armed robberies. The most common fashion is merely to walk out the door of one's company with a tape or a set of glass plates upon which a chip designed is etched or the chip themselves in one's coat.

The interesting thing here is that with, for instance, the reticles or computer tapes, which depict these circuit designs upon them, a company or country which has not developed the technical expertise to actually design these products effectively from scratch, such as Eastern Europe, can get them by theft where otherwise, they would not be able to make them at all.

The most common problem we have is much more crude and direct, however, and this is the employee taking things out in his lunch bucket, in the lining of the jacket or whatever. He sells to a marketplace which has come to be known as the gray market. He can sell these parts that are stolen from 5 to 50 cents on the dollar to numerous fly-by-night independent distributors operating out of low-rent office suites, their homes or even the back seats of their cars.

Usually, no questions are asked.

As often as not, the buyer purchasing the stolen parts is otherwise respectable appearing businessmen. He uses his business as a front for criminal activity or just cannot pass up the opportunity to make some fast money.

In one recent case, in Santa Clara County, resulting in the conviction of two persons, an undercover officer offered to sell a local distributor purportedly stolen Intel memory chips which were in very high demand.

The officer flat out told the businessman these chips were stolen. After snapping up the parts for $10,000 in cash, which is the common method of payment, the defendants in the same day shipped these parts via air freight to Werner Bruchhausen, the nortorious international chip broker.

The principle in this particular case is no back alley crook. He is the handsome three-piece suited president of a successful parts distribution firm and, all in all, a very typical American success story. Yet here he was selling stolen integrated circuits to an internationally known fence. The reason is the same as always, greed. Greed has spawned what we think of as the gray market and to understand, I think, briefly, we will talk about the hierarchy in electronics commerce.

In between the manufacturer and the end user are middlemen. Usually we are talking about franchised distributors which are reputable firms dealing directly with the manufacturers but beneath the franchise directors has grown a market populated by the independent distributors.

They obtain their product either from a company which manufactures it when a surplus occurs or from franchised distributors or even end users when they have surplus parts.

What is created by this system is an "anything goes" marketplace where, especially in times of high demand and short supply, such as occurred in the 1977 to 1980 time frame, speculation runs rampant. It's really no different from pork belly futures. Brokers buy large quantities of parts at fire sale prices, hoping to be able to turn them over quickly if a need is found elsewhere. Numbers of these people made a lot of money doing just this sort of speculation during the parts shortage of 1977 to 1980.

An example of the gray market is a case which has been successfully prosecuted recently. This is the case of Larry E. Lowery. Larry Lowery first came to the attention of law enforcement in January 1978. In that month an employee of L&M Electronics, a distributor, was observed to steal $100,000 worth of late model circuits and transport them to one, David Henry Roberts. Roberts in turn delivered them to Lowery's house. Because of a series of miscues by law enforcement, he escaped prosecution. But, again, in 1979, Roberts, the middleman here was rearrested and convicted for two integrated circuit thefts. Again, he named Lowery as his instigator and fence but the police were able to acquire evidence other than Robert's statement with which to prosecute.

In April 1980, an undercover investigation was initiated which ultimately led to the arrest of Lowery in the search of his premises. Over 11,000 stolen integrated circuits valued at between $100,000 and $150,000 was seized. Legwork and forensic examination disclosed that the records that Lowery kept relating to his acquisition of these parts were entirely phony. Handwriting experts determined that in fact all the records were authored by the convicted thief, David Roberts.

While the prosecution was pending and just prior to a preliminary hearing in the matter, a key witness in the prosecution was lured out of his home, attacked and severely beaten.

Later on, the eve of the jury trial, Roberts himself, then under subpena by the prosecution, was murdered execution style and his body dumped in a shallow grave in the Santa Cruz Mountains.

Lowery was convicted in November 1981. Notwithstanding his sentence to prison, however, while he was still out on bail pending sentencing, another theft occurred from Monolithic Memories, Inc., in Sunnyvale, Calif.

That theft occurred over Thanksgiving weekend in 1981—$3.4 million worth of late model high tech integrated circuits were stolen, including a great number of the samples that you see on the board before you, Senator.

Many of these circuits were specially designed units with direct military applications. In all, about a ton of boxed, first line parts were taken, necessitating at least two truckloads to make off with all the booty.

Ultimately, three subjects were arrested and evidence was seized implicating both Lowery and his partner, Larry Kizer.

There was insufficient evidence to charge Kizer or Lowery.

The parts themselves have not been located or recovered and frankly it is feared they have been already transported overseas, most likely to a European location. It is worthy of note that Lowery had reportedly bragged to associates of his that he was the biggest fence in northern California and the evidence suggests he also made new European contacts with which to market his goods.

To date, the trial of investigation in this case is littered with dead bodies, assault, sophisticated thefts, drug sales and more. Scores of criminal conspirators appear to be involved. It represents the largest case of consistent, habitual, organized criminal activity aimed at Silicon Valley.

Another case worthy of note involves some characters already mentioned before to the subcommittee.

John Henry Jackson is a five-time convicted felon who, for the last 3 or 4 years, has been the proprietor of a P.C. board "stuffing" house and aspiring computer maker, with a parts brokerage business in the Santa Clara area.

Around November 1979, again, around Thanksgiving time, Intel Corp., a maker of the state-of-the-art type products, suffered a million dollar theft of approximately 10,000 units. These were state-of-the-art memory devices in very high demand throughout the world at that time.

After the theft, corporate inevstigators had no leads as to how these items had been stolen but shortly thereafter, it came to their attention a large number of these products had surfaced in Germany.

Specifically, Siemons A. G. of West Germany, a hugh electronics manufacturer, and one of Intel's best customers, had apparently just received a large shipment of 10,000 parts which were established to be the stolen parts.

Siemons purchased approximately 10,000 parts from E.V.B. Corp. of Munich, West Germany. E.V.B. received the parts from two sources, Republic of Virginia, here in Arlington, Va., and another parts broker, Mormac, Inc. of Torrance, Calif.

Each of these companies in turn purchased their portion of parts from Space Age Metals in Los Angeles who obtained it from John Jackson.

Luckily an employee of Jackson's came forward spurred in part by continuing revelations in the press regarding the seriousness of the stolen chip problem. The witness told, in a period of less than 1½ years, of having counterfeited tens of thousands of integrated stolen circuits for Jackson, primarily, Intel products.

With the cooperation of this informant, an undercover operation was instituted and eventually Jackson and one of his associates were arrested. His associate had been an Intel employee.

Concurrent with these arrests, extensive search warrants were prepared and served on various parties. In one business letter discovered at Space Age Metals, a Republic vice president told a Space Age official that he was amazed at the quantity and price of this product that was being offered, given their scarcity in the marketplace, but that he

wanted to close the deal and was not stupid enough to ask any dumb questions.

The *Jackson* case points out the difficulty of proving knowing receipt of stolen circuits, once we do uncover the theft case.

Although business records of the affected companies did indicate transactions among them and the particular kind of product involved, it is impossible to prove which particular items they sold to one another and, therefore, the chain of circumstantial evidence is very strained.

The recordkeeping systems employed by the brokers are not sufficiently specific to be able to trace the particular part, nor are knowing thieves likely to keep such records.

Another aspect of the theft problem which is potentially much more serious for national security purposes is the trade secret thefts, since such thefts provide the very means of obtaining the technology upon which to establish an industry and develop competitive expertise. I have heard authoritatively stated that the United States at one time possessed a 10-year lead over the Soviet Union in microelectronics technology, but that that lead has already shrunk to maybe 5 years based primarily on the easy access the Soviets have to our technology.

I am not in a position to attest to the veracity of that proposition but certainly what I have seen would not negate it. By their very nature, trade secret theft is the most difficult type of theft to detect and solve. What is taken is generally not a physical thing, but an idea.

Original documents, computer tapes, reticles, masks and technical drawings can be easily copied by any number of photographic or electronic means without anything corporeal ever being taken.

Hence, nothing is missed.

California, at least, is among the few States who have a criminal trade secret theft statute. I set it forth in my statement but won't repeat it here. I think it important to note a statute makes it a crime either to take an article representing a trade secret or copy an article representing a trade secret. It also makes it a crime to offer a bribe in order to obtain a trade secret.

Unfortunately, very few States have criminal trade secret theft laws.

I discovered that most of the Western States in this country where significant semi-conductor and defense plants exist, have no trade secret laws whatsoever.

I think this is a serious deficiency which perhaps can be addressed by legislation.

An example of a trade secret theft case of some importance is the case of Peter K. Gopal. Peter K. Gopal first came to the attention of industry security personnel in approximately January 1978, in connection with National Semiconductor Corp.'s unauthorized possession of a computer data base tape containing the design for a late model Intel microprocessor chip.

After an inconclusive investigation, the matter was put on the back burner. Thereafter, however, in September 1981, one Andrew Moore, an independent manufacturer's representative, indicated in conversations to a national semiconductor employee that he represented a principal who owned the original Intel design information available for sale. The national employee immediately contacted his superiors

and law enforcement authorities and an investigation ensued. During undercover negotiations, Gopal indicated that he had past and continued access to proprietary Intel design via insiders within Intel Corp. He stated he already sold his designs in Europe and customers were quite satisfied with their performance and authenticity.

The undercover operation culminated in late September with Gopal's arrest during a sale of Intel chip designs. Search warrants were prepared and served leading to the seizure for Gopal's business premises of hundreds of computer tapes, masks and other design materials for Intel, National, Semiconductor, Zilog, and other corporations.

The values of the items seized ran well into the millions of dollars. Some of the items seized were still in the research and development stage, and had never been marketed by their owners.

Also seized were personal and business record of Gopal's indicating trips to Europe in 1977 and 1978, including trips to the Soviet Union and Poland.

Business cards of numerous Soviet consular level and ministry officials dealing in technology exchange and purchase were found. I won't try to list them all because they are contained in my statement on pages 40 and 41. I will note there are two individuals there named Pavlov, which is the same name mentioned yesterday. One card bears, in Gopal's handwriting, the phrase: "Terms of contract negotiation."

Business records seized also indicated continuing international transactions between Gopal and Austrian and Swiss firms. The primary Austrian firm, Sacher-Gesellschaft AG, of Vienna, Austria, was headed by Dr. Rudolf Sacher. He was also a one-half shareholder with Gopal in Gopal's business, Semiconductor Systems, International, Inc. Subsequent investigation of the Swiss firms indicated they were probably nothing more than shell corporations, serving as middlemen for the transactions in which they were involved. Efforts to track the course of the transactions past the Swiss firms were fruitless. Gopal has refused to cooperate with the authorities.

The investigation continued after Gopal's arrest, however, and a business associate was located who told authorities that Gopal bragged of having purchased certain integrated circuit testing equipment and selling it to Poland via one of his Swiss intermediaries.

A check of business records confirms Gopal indeed acquired the equipment in question and sold it, but it's ultimate purchaser could not be determined.

My understanding is the Department of Commerce, after an investigation, concluded that it was unable to prove a violation more serious than a misdemeanor for which the only penalty was suspension of export licensing privileges.

By that time, Gopal had been blackballed in the industry and his license matter was rather moot.

Senator NUNN. Did Gopal ever go to jail?

Mr. SOUTHARD. He was convicted after a 6-month-long court trial. He was sentenced to 2 years, 8 months in a State prison in California.

I might note his prosecution was unusually difficult. Neither the prosecution nor defense was willing to risk a jury trial because the issues were so complicated.

At one point a judge threw out most of the physical evidence because the police officer serving search warrants were so ignorant as to what they were looking for they had to take technical people along with them just to identify what was stolen and what was not. Thankfully, the court of appeals reversed that, but the complexity of the case necessitated, for instance, actual court hearings and testimony being taken in the computer room at National Semiconductor. We had to adjourn and go to the massive rooms filled with computers just to view the evidence.

He was sentenced to 2 years, 8 months in State prison. He is, however, currently free on bail pending appeal which does not seem to be terminable in the foreseeable future. After a year and a half, the court reporter hasn't even finished making the transcript.

I have addressed the suggested responses, some suggested responses in my written statement, Senator. I won't reiterate those here except to mention generally it is the feeling of myself, as a representative of the law enforcement community in Santa Clara County, that we need increased investigative personnel in export regulatory agencies and the FBI to help us.

These matters are matters which are international in scope and just are not appropriately dealt with by a local sheriff's office with its limited background and limited resources.

I also believe the creation of a national regional high technology crimes task force or at least the information clearinghouse would be quite valuable in this context.

Senator NUNN. Do you agree with Dr. Baker's general suggestion there or did you hear him testify?

Mr. SOUTHARD. I did hear him testify and found his testimony very enlightening and I do agree with his suggestion; yes.

I have also suggested a system of mandatory crime reporting which would be similar to what currently exist in banking law as something that might be helpful. I have noticed a reticence on the part of some manufacturers to become involved in law enforcement.

Also, electronics broker regulation is a subject I think that should be investigated, and the possible enactment of Federal trade secrets laws to complement the Secrecy Acts, the Espionage Act. These, of course, are suggestions on my part seen from my perspective. It is for the subcommittee to put all the pieces of the jigsaw puzzle together and come up with its recommendations.

Thank you.

Senator NUNN. Thank you very much. You have been helpful and have a very impressive record in law enforcement particularly in this area.

From what I am told, you have had probably more experience in this area than most Federal people.

Mr. SOUTHARD. Unfortunately, I think that is true; yes.

Senator NUNN. You are saying there really is clearly a Federal role that is beyond the scope of what local law enforcement officials can handle?

Mr. SOUTHARD. Absolutely. For instance, in the *Jackson* case, which is still pending, if we were really going to go all the way to prove out the chain of evidence, tracing the parts from Germany back to their

theft source in California, it would require the exhaustion of entire witness budget of my county for the whole year.

Frankly, the public, who is more concerned about violent crime, doesn't want us chasing all over the world after white-collar crime.

Senator NUNN. Why would the mandatory crime reporting you suggest be needed for the national clearinghouse? What would be the advantage of this?

Mr. SOUTHARD. It is just a matter of gaining intelligence information.

What we have found since we started an active investigative role, which includes sting operations and continual undercover monitoring efforts, is you have to establish patterns here and there to know what is going on. I think it and mandatory crime reporting help us to establish patterns, recognize who the real thieves are, and therefore, establish priorities for enforcement.

Senator NUNN. How valuable and necessary is it for prosecutors, Federal and State, to have a technological background when prosecuting these advance technology type cases?

Mr. SOUTHARD. For someone in my position, it is not, certainly, absolutely necessary. It might be desirable. I certainly would not have the technological background. What you will find, however, is that industry, once aroused, is very interested in helping and will provide all of the training that is really necessary to understand what is basically a new vocabulary.

Senator NUNN. The general thievery amounted to $100 million in the last 5 years in Santa Clara County from high technology firms?

Mr. SOUTHARD. That is correct.

Senator NUNN. How much of it would you estimate comes from foreign sources trying to gain access as opposed to just cutthroat, unscrupulous competition of stealing secrets from competitors?

Mr. SOUTHARD. Frankly, I think most of the kind of thing over which our county has jurisdiction comes from normal street level thieves and a hierarchy of brokers who are criminally involved.

The important thing, however, is this provides a mode of acquiring products for illegal export.

We have seen it on numerous occasions. Mr. Bruchhausen, for instance, who was previously mentioned, had contact with three of the people I previously mentioned.

Mr. Gopal was concerned almost exclusively with overseas export of technology.

Senator NUNN. When you look at the overall problem, wouldn't it be more effective to have a concentrated law enforcement effort at the source, that is, at the manufacturer's level, rather than at the borders?

Mr. SOUTHARD. Obviously that would seem the simpler solution. We have given a lot of criticism to industry in terms of the lack of self-policing they have done. However, these products are designed for the marketplace. They are going to get out into the marketplace one way or the other. Therefore, if there were more security guards on the doors of the manufacturers it wouldn't help.

We need an effort to keep these from going over the borders.

Senator NUNN. Is there any way businesses and companies can be notified about people like Gopal, whose activities are known to law enforcement and many times are not known to businesses?

Mr. SOUTHARD. I think this is where the central clearinghouse or task force idea will come in handy.

Of course, they can be notified. They have to be, discreetly. They are not, so far as I know, on any regular basis.

Senator NUNN. What suggestions would you make to high technology businessmen who are patriotic and want to protect national security?

Mr. SOUTHARD. I think we have seen some such businessmen testify before this subcommittee.

You have got to question about the validity of the firm you are dealing with, especially a foreign firm. Go to the FBI, ask questions. The FBI has recently sought to publicize their efforts in this problem in our particular area by putting up billboards similar to the World War II type of thing about the walls having ears.

Senator NUNN. When you mentioned having an electronic broker's license, what do you think the resistance level would be to this in terms of business people saying this is just another Government regulation, and so forth?

Mr. SOUTHARD. I'd sympathize with them if they said that. On the other hand, the legitimate brokers are already doing business in a proper fashion. I don't believe it would be unduly negatively influenced by that kind of legislation.

What I am proposing is nothing different than the type of control that is almost everywhere already imposed upon pawnbrokers. You have to identify it as an area which is a type of enterprise which is particularly easy to abuse. Once you have done that, I think you can rationalize the controls.

Senator NUNN. How does law enforcement have any way of protecting knowhow? That being a very special part of what America has today that the Soviets don't have, how in the world can you devise a law enforcement mechanism or codify an overall approach to protecting knowhow?

Mr. SOUTHARD. I don't know that law enforcement activity in that particular area is what is most needed. In that particular area, on-site security by the manufacturers should be effective and, in fact, know-how or trade secrets tend to be more closely guarded than actual physical product because you can insure the physical product against theft. You can't insure the know-how. But the type of organization proposed by Dr. Baker, I think, would be very helpful in giving the Federal law enforcement community the appropriate technical input to understand whether know-how is really involved.

Senator NUNN. Do you think the companies in the Silicon Valley area are aware of the military significance of what they are developing in most cases?

Mr. SOUTHARD. I think somehow subliminally they are aware of it. Frankly, most of the market is the commercial market.

Recently one of the leading minds and figures in the area, the vice president of Intel was asked about that particular question, and his basic response was, "Hey, we're in the chip-making business. That's the Fed's problem to worry about where it goes afterwards." I was kind of surprised at his relatively callous answer there, but I think that may be somewhat representative of the field.

Senator NUNN. What would the Soviet Union have done with the technology Gopal was stealing? How would it be useful to them?

Mr. SOUTHARD. Nothing he had had direct military application.

The same kind of chip that can be used in a Pacman game can also be used in a cruise missile. What was interesting about what he had was he had very voluminous design information about current memory and microprocessor chips. What he had, if possessed by somebody else with the appropriate equipment and process information that is the chemical process type of magic that goes into making these chips—if you had those two precursors and designs, you could have gone into immediate mass production of these chips and modified them for specific military use.

Senator NUNN. You have been involved in this area a good bit. Have you had any contact or liaison with the Commerce Department?

Mr. SOUTHARD. Only with respect to the Gopal case. They sent an agent out for a few days who went through records in my files. Evidently he also made trips to Europe investigating the case, but they were unable to find a felony violation.

Senator NUNN. Have they encouraged you to coordinate with the internal information when you have it in this area?

Mr. SOUTHARD. There has been no encouragement other than this one agent. There has been no communication officially other than that.

Senator NUNN. Mr. Southard, we really appreciate your good work in this area. You are a credit to law enforcement; you are a credit to prosecuting attorneys. You have been a great help to our subcommittee.

We appreciate the summary you gave considering the time elements we were working against here today. We hope you will continue to keep in touch with us and give us the benefit of your views.

Mr. SOUTHARD. I certainly will.

Senator NUNN. Thank you very much.

Mr. SOUTHARD. Thank you, Senator.

Senator NUNN. Tomorrow morning at 9:30 we will resume the hearing. At that time we will hear from the Honorable James L. Buckley, State Security Assistance, Department of State; Edward O'Malley, Assistant Director, Intelligence Division, Federal Bureau of Investigation; Arthur Van Cook, Director of Information Services, Department of Defense, Chairman of National Disclosure Policy Committee; William Von Raab, Commissioner, U.S. Customs Service, accompanied by Mr. George Corcoran, Assistant Commissioner.

We will resume these hearings at 9:30 a.m. tomorrow.

[Whereupon, at 1:42 p.m., the subcommittee recessed, to reconvene at 9:30 a.m., Thursday, May 6, 1982.]

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

THURSDAY, MAY 6, 1982

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met at 9:30 a.m., in room 3302, Dirksen Senate Office Building, under authority of Senate Resolution 361, dated March 5, 1980, Hon. Sam Nunn presiding.

Member of the subcommittee present: Senator Sam Nunn, Democrat, Georgia.

Members of the professional staff present: Eleanore J. Hill, chief counsel to the minority; Katherine Bidden, chief clerk; Gregory Baldwin, assistant counsel to the minority; Jack Key, Glenn Fry, and Fred Asselin, staff investigators to the minority; and Kathleen Dias, executive secretary to the minority chief counsel.

[Senator present at convening of hearing: Senator Nunn.]

Senator NUNN. The subcommittee will come to order.

[The letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

Pursuant to rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the chairman, or any member of the subcommittee as designated by the chairman, to conduct open and/or executive hearings without a quorum of two members for the administration of oaths and taking testimony in connection with hearings on the transfer of U.S. high technology to the Soviet Union and Soviet bloc nations, to be held May 4, 5, 6, 11, and 12, 1982.

WILLIAM V. ROTH, Jr.,
Chairman.

SAM NUNN,
Ranking Minority Member.

Senator NUNN. Senator Roth is going to be coming in later this morning. He asked me to go ahead and begin the hearings.

Mr. Secretary, we are delighted to have you this morning returning to the Senate. We are pleased to have your associates.

If you plan to have testimony from all three of you here today, I will ask all of you to rise and take the oath. We swear in all of our witnesses before the subcommittee.

Do you swear the testimony you will give before the subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. BUCKLEY. I do.

Mr. JOHNSTON. I do.

Mr. BRYANT. I do.

95-929 O - 82 - 11

TESTIMONY OF JAMES L. BUCKLEY, UNDER SECRETARY OF STATE FOR SECURITY ASSISTANCE, SCIENCE AND TECHNOLOGY, DEPARTMENT OF STATE, ACCOMPANIED BY ERNEST JOHNSTON, DEPUTY ASSISTANT SECRETARY OF STATE FOR ECONOMIC AND BUSINESS AFFAIRS, AND CLYDE BRYANT, CHIEF, SUPPORT SERVICES DIVISION, OFFICE OF MUNITIONS CONTROL, STATE DEPARTMENT

Mr. BUCKLEY. Thank you, Mr. Chairman.

I will be the only one giving the statement, but Mr. Clyde Bryant on my right is thoroughly familiar with the munitions control apparatus and Mr. Ernest Johnston on my left is familiar with some of the technical details of Cocom.*

Senator NUNN. Good.

I know you have a statement, so we will be delighted to receive it.

Mr. BUCKLEY. Mr. Chairman, it goes without saying that I am delighted to have this opportunity to testify on the role of the State Department in controlling the transfer of militarily critical technology to the Soviet Union and the Eastern bloc. Whatever the record of prior administrations, Republican as well as Democratic, it is clear that this administration has placed a very high priority on improving the effectiveness of the executive branch in enforcing export controls. It has launched important initiatives which we believe will greatly improve their overall effectiveness while sharpening the focus on those elements of advanced technology and process know-how which are of the most critical importance to the Soviet bloc.

We freely acknowledge that much more needs to be done; and we are actively working with other agencies to improve coordination over a range of issues.

It will take time, however, for all these efforts to take hold in particular areas, especially because of the large amount of new data that has had to be gathered by various agencies.

In your letter inviting me to testify, you asked the State Department to respond to six specific questions. I have done so in the attachment to my prepared statement, which I would appreciate your including in the proceedings.

Senator NUNN. Without objection, they will be admitted into the record as if read.[1]

Mr. BUCKLEY. National security export controls are a basic element in overall U.S. policy toward the Warsaw Pact countries.

To put it plainly, these controls are a recognition of the fact that the global objectives of the Soviet bloc are inimical to our own, and threaten every value for which our Nation stands. Therefore, it is simply harmful for us to provide those nations with Western, militarily useful technologies, to be turned against us.

As most of these sensitive technologies are not within the sole control of the United States, it has been essential from the outset to achieve among the major Western industrialized powers fundamental agree-

---

* COCOM stands for Coordinating Committee for Multi-Lateral Export Controls—to which Japan and all NATO countries except Iceland belong.

[1] See p. 533 for Secretary Buckley's prepared statement with attachments.

ment as to what technologies are militarily critical and how their transfer to the Soviet bloc should be controlled.

The instrument that has been developed for this purpose is the coordinating committee for multilateral export controls, or "Cocom" to which Japan and all NATO countries, with the exception of Iceland, belong.

Cocom was created in 1949 by informal agreement among its members, and has thus been in existence for more than three decades.

Cocom has three major functions:

The first is the establishment and updating of lists of embargoed products and technologies. Although Cocom lists are not published, they become the basis for the national control lists administered by each member government. The member governments are now preparing for a major review of these embargo lists, which will begin in October.

Second, Cocom acts as the clearinghouse for requests submitted by the member governments to ship specific items to specified end users in the proscribed countries. (The Cocom-proscribed countries are the the Soviet Union, the other Warsaw Pact countries, China, and the other Communist countries in Asia.)

Third, Cocom serves as a means of coordinating the administration and enforcement activities of the member governments.

The Cocom lists set up fairly specific limits on the technical characteristics above which member governments agree that they will prohibit exports to proscribed countries, unless Cocom itself approves exceptions.

In agreeing to a national request to export items on one of the control lists, Cocom works on the principle of unanimity. No application, in short, is approved if any member state objects.

One of the evolved strengths of Cocom is that in over 30 years of operations, there have been very few cases in which a government has exercised its sovereign right to go ahead with exports over Cocom objections.

Senator NUNN. Mr. Secretary, when you say no application, in short, is approved if any member state objects. Does this mean that no technology is left off the excluded list?

In other words, there is no restriction unless everybody agrees, or does it mean just the reverse?

Mr. BUCKLEY. It means once a technology is on the list, any one member nation has a veto over its transfer to a proscribed country.

Senator NUNN. I see. So it is really a veto that protects the export of technology?

Mr. BUCKLEY. That is right.

Senator NUNN. One country can block all the rest.

Mr. BUCKLEY. With respect to those items on the list.

Senator NUNN. The crucial thing is what is on the list?

Mr. BUCKLEY. Exactly, yes.

This self-discipline is all the more remarkable given the absence of any treaty or executive agreement undergirding the organization.

Over those decades, Cocom has generally been successful in inhibiting the overt flow of strategic technology to our adversaries.

During the 1970's, however, in the honeymoon days of détente, the United States and the West relaxed controls over a number of em-

bargoed commodities. It was believed that wide-ranging trade would somehow alter the international behavior of the Soviets and moderate their military investment.

During this period, the United States went from being the least, to the most frequent, seeker of exceptions to multilateral controls. Cocom itself came to reflect such attitudes, and exceptions to the embargo were allowed to thrive.

We now know this was a mistake. During the period of détente, the world stood witness to the greatest military buildup in history, along with the increased Soviet adventurism that grew out of an increased self-confidence.

The Reagan administration came to power 15 months ago determined to stem the flow of the technology that the Soviet Union and its Warsaw Pact allies were using to improve their already vast warmaking capabilities. It was clear that the West's crucial qualitative edge in military systems was being undermined by the Soviets' increasingly aggressive efforts to buy or steal our militarily relevant technologies and equipment.

More precisely, we saw this well-orchestrated acquisition program giving the Soviets:

First, a very significant savings in time and money in their military research and development programs;

Second, rapid modernization of their defense industrial infrastructure;

Third, the opportunity to accelerate the closing of gaps between our weapons systems and theirs; and

Fourth, the chance to develop, with alarming speed, neutralizing countermeasures to our own technological innovations.

As a consequence, the administration has initiated efforts to fill in gaps in the multilateral export control system. At the Ottawa summit meeting last July, President Reagan raised the problem of Western technology transfer to the Soviet Union. An agreement at Ottawa to consult on this issue culminated in a high level meeting in Paris during January, the first ministerial level Cocom meeting since the late 1950's. The other Cocom governments have asked that the results of that meeting be kept confidential, as indeed are all Cocom proceedings.

I chaired the U.S. delegation to that meeting, however, and I can say that there was a concrete consensus that the member governments should increase their effort to improve Cocom effectiveness. We have been encouraged by what appears a new and more constructive attitude of other Cocom governments, and feel that this meeting forms a basis for a revitalization of the Cocom system.

Such a revitalization will take much hard work and it will take time, among other reasons because Cocom depends on the national administration of controls by 15 individual governments. But some specific steps are under way. Effectiveness, for example, requires precise definitions of many complex technologies. We have made progress toward agreement on a number of specific, technical proposals in this area to tighten the embargo.

Second, the United States is now working on proposals that will expand Cocom control lists of new priority industries. These include gas turbine engines; large floating drydocks; certain metallurgical processes; electronic grade silicon; printed circuit board technology;

space launch vehicles and spacecraft; robotics; ceramic materials for engines; certain advanced composites; and communications switching and computer hardware and software technology and know-how.

This process will continue into the triennial Cocom list review, which will take place this October, when a general reappraisal of everything on the control lists will take place.

Senator NUNN. Who is actually doing this reappraisal for our government, for instance? What group of people carry out our national input into that process?

Mr. BUCKLEY. We have the military, of course, and we also had a tremendous input from the intelligence services who are examining new concepts of what is really critical, what are the choke points, and what is it that the Soviets are most anxious to have. We also have a great deal of cooperation from industry in helping us in this process.

Senator NUNN. Is there a central clearinghouse on this? Is there one location that everything feeds through, or is it a rather diffused effort?

Mr. JOHNSTON. No, sir. We have something called the Economic Defense Advisory Committee which is chaired by the State Department. Under this committee there are 12 technical subcommittees depending on the kinds of products that we are talking about, that is where the decisions will be made on exactly which products we will try to have added to the list.

Senator NUNN. Are those people State Department employees?

Mr. JOHNSTON. Some of them are.

The chairman of the organization is. But there are members of the Defense Department, the Commerce Department, and the intelligence community.

Senator NUNN. So the central location is in the State Department, but you are bringing in other agencies on that?

Mr. JOHNSTON. That is right.

Senator NUNN. Is that both for the items on the export control list as well as export arms control list?

Mr. JOHNSTON. No. The arms control list is controlled by another section of the State Department. That is done essentially in collaboration with the Defense Department.

Senator NUNN. So this is a group that deals with the——

Mr. JOHNSTON. Export Administration Act.

Senator NUNN. Export Administration?

Mr. JOHNSTON. Right.

Mr. BUCKLEY. We have also developed workable proposals for harmonizing the export licensing procedures of the 15-member states so as to make Cocom decisionmaking more efficient. What we are seeking are ways to bring national enforcement practices to a level of equal effectiveness. These two matters will be addressed at a special Cocom meeting which will convene in Paris later this spring—and the fact that all partners have agreed to that special meeting is testament to our shared goals.

We have been cooperating with our Cocom allies to improve enforcement and investigative capabilities of illegal diversions.

The State Department, working closely with our intelligence and investigative agencies, has been channeling appropriate information

to other governments to alert them to potentially illegal activities within their borders. We have also encouraged them to increase the investigative resources and the sanctions available for export control enforcement. Commerce, and in turn customs, have detailed officers to the State Department to support this overseas compliance effort.

Cocom has thus, we believe, made measurable progress toward strengthening strategic export controls since this administration came into office. But it is also clear that the continuing revitalization process will be long and hard.

In attempting to strengthen controls on strategic exports to the Soviet Union and the other Warsaw Pact countries, we are faced with the perennial problem of securing agreement with all the other Cocom allies on just where to establish the technical cut-offs for commodities and technologies under embargo. Determining in many scores of different technical areas what is sufficiently strategic to warrant control is not an easy task. We do not always agree on what are militarily critical technologies, yet the purpose of the organization is limited to such technologies. Members exercise considerable care to avoid controls whose principal impact would be economic rather than military, and each has its own views and perspective.

Western European and Japanese economies would generally speaking, be affected more than the U.S. economy by sweeping controls on manufactured products. But such differences between ourselves and our Cocom allies should not be over-emphasized.

We should remember that our allies have cooperated with us for over 30 years to control significant amounts of equipment, material and technologies through Cocom. That is, first and foremost, because we share a common belief that such controls constitute an important element in our mutual defense.

As you know, the State Department is also responsible for administering munitions export controls which cover defense articles and services. Munitions are not approved for export to Warsaw Pact countries. Accordingly, the main issue in administering these controls, relate to security concerns and our foreign relations with other countries.

Your letter of invitation mentions that, in an executive branch more effectively organized to shape and enforce export control policy, you envisage a principal and expanded role for the Department of State. We, too, envisage such a role for the Department.

Upon taking office, this administration undertook a full review of our policy concerning the transfer of strategic technology to the Soviet Union and the other Warsaw Pact countries.

The State Department was a major participant in this review, which culminated in the Cocom high level meeting. The State Department led our delegation to that meeting. Since then, on a number of other occasions, senior officers at the State Department have discussed with our allies security concerns related to technology transfers.

We are persuaded that improved allied cooperation on sensitive technology transfer issues is a realistic objective. There will, of course, continue to be some differences on the details of controls and their application to individual cases. But, with hard work to identify clearly and to justify persuasively what needs to be controlled, and

how controls should be enforced and administered, such differences, we believe, will be the exception rather than the rule.

Senator NUNN. Thank you very much, Mr. Secretary.

We also appreciate your furnishing the material answering specific questions at the end of your testimony. We will study this with great care as we come up with any recommendations we may make for improvement.

I have a few questions I would like to pose to you and I will be glad for you to farm them out here in the particular area of expertise.

I will direct them to you. You handle it from there.

Are you generally satisfied with the level of cooperation we are getting from Western Europe and Japan in high technology area today?

Mr. BUCKLEY. Yes; we are.

One thing that we sensed was a really heightened awareness of the part of those countries as to the impact of technology purchases on actual military capabilities. And I would give high credit for that to briefings conducted by the CIA at the various Cocom capitals, in which highly classified detailed information opened lots of eyes to the impact of technologies to which people were not paying any attention. I think that has had the effect of increasing cooperation to a very significant degree.

Senator NUNN. Is it necessary for the United States to always be a leader in this respect? I am sure we want to be. But let's assume, for instance, we get rather sloppy in our administration. Have we had any instances of cases where the allies came to us and said, "Look, you are transferring technology which we think is useful in military application by the Soviet Union and we want you to crack down," or is it always the United States who has to save our allies?

Mr. BUCKLEY. My institutional memory is rather short, in this case, 15 months. I do know I can speak of one ally, I can't give names, because of the Cocom ground rules, that has begun to take on a role of leadership in these areas. The United States, I think, historically has been the key. But Ernie, do you know of other instances?

Mr. JOHNSTON. It is essentially the United States. I think that is right.

This subject comes up primarily in the review that we conduct. There we have also had suggestions from other countries about items that ought to be added to the list.

Senator NUNN. In other words, you could say it is a pretty general rule that based on historical experience that export controls are not going to be any tighter in any of the countries than they are in the United States?

Mr. JOHNSTON. I think that is generally true.

Senator NUNN. We are the leader and we are going to have to continue to lead?

Mr. JOHNSTON. That is right.

Senator NUNN. The State Department is not a law enforcement organization in the usual sense. When administration of the Arms Export Control Act was handed to the State Department, why did the Department give enforcement to the Customs Service?

Mr. BUCKLEY. First of all, customs is an organization in place with the people at all the points of export. Second, there is a rather easy

means of communication between bureaus and that is to require that licenses that are issued be filed at the relevant customs office before the actual shipment has taken place, and this facilitates the ability of customs to match the documents against what is being exported.

Senator NUNN. What is the relationship between the Export Administration Act, which regulates nonmilitary-type technology, and the overall Arms Export Control Act? Do you have two separate groups of people dealing with that all together?

Mr. BUCKLEY. Yes.

Mr. JOHNSTON. Yes. The Defense Department and the State Department work together to decide what goes on the munitions list. This is something defined, if you will, as an instrument of war or something which is related directly to making war. However, there is always a series of goods which could have a dual use. They can have a civilian application, or they could have a military application, for example, computers. These are the main things controlled by the Export Administration Act.

Senator NUNN. Of course, Commerce is responsible for that?

Mr. JOHNSTON. Yes, sir.

Senator NUNN. How much input does the State Department have with Commerce regarding the Export Administration Act?

Mr. JOHNSTON. On the list of strategic goods, which is essentially what we are talking about, the Defense Department and the State Department work very closely with the Commerce Department.

The Secretary of Commerce has the final authority, but the Defense Department and the State Department work very closely both in regard to deciding what gets on the list and what the licensing policy ought to be.

Senator NUNN. The munitions list has to consider certain gray areas, I am sure.

Mr. JOHNSTON. I would like to ask Mr. Bryant, who is our expert on munitions.

Mr. BRYANT. In compiling the U.S. munitions list, we, the Department of State, consult with the Department of Defense as required by Executive order, to determine what should be on the munitions list.

There are occasions when there are debates as to whether or not a specific item is on the list. The determination, generally speaking, is made on the basis of what that item was specifically designed to do.

Senator NUNN. When you examine that munitions list, do you go in the gray area, things that are really not what we would call conventional munitions, but which do involve high technology?

How much overlap is there between the Export Administration list and the munitions list?

Mr. BRYANT. There should be no overlap at all, either an item is controlled under the Export Administration Act or it is controlled under the Arms Export Control Act. In certain fields, particularly military electronics, the basic technology involved in both civil and military electronics may be the same.

For example, computer chips and the integrated chips are both used in military and nonmilitary items. When incorporated into a military item, the chips take on the characteristics of that item. The chips themselves, when exported, are not subject to our control, unless specifically designed for inclusion in a military item.

Senator NUNN. When you are getting your munitions list, your arms export list, do you have feed-in from the Defense Department?

Mr. BRYANT. Yes, sir.

Senator NUNN. Do you have feed-in, from some of the intelligence agencies?

Mr. BRYANT. Yes, sir.

Senator NUNN. The State Department makes the final decision?

Mr. BRYANT. That is correct, sir.

Senator NUNN. In the Export Administration Act, the Commerce Department makes the final decision?

Mr. BRYANT. I have to defer to Mr. Johnston.

Mr. JOHNSTON. Yes, sir, except that I do think there is a pretty close collaboration on a subject like this. The three agencies are working very closely together.

Senator NUNN. Do the Defense Department and the State Department both have a feed-up and input into Commerce on that?

Mr. JOHNSTON. Yes.

Senator NUNN. Does the division in the State Department that deals with the munitions list have a feed-in to the Commerce Department in terms of the export list?

Mr. JOHNSTON. If an item is taken off the munitions list, and occasionally there are bills in Congress which do this, we pick them up on the list that is administered by the Department of Commerce.

Senator NUNN. What group in the State Department feeds into the Commerce Department in terms of the Department's final decision-making on the export control list?

Mr. JOHNSTON. It is the Bureau of Economic and Business Affairs.

Senator NUNN. That is a separate group from the group on the munitions list?

Mr. JOHNSTON. Right.

Senator NUNN. You say the Bureau of Economic Affairs?

Mr. JOHNSTON. Yes.

Senator NUNN. Does that group also feed into the Cocom deliberative process?

Mr. JOHNSTON. Yes.

Senator NUNN. The same group?

Mr. JOHNSTON. Yes. It is essentially the same. It is the same office. We have an Office of East-West Trade which devotes, I would say, probably 75 percent of its efforts to this.

Senator NUNN. The State Department does not try to enforce the Arms Export Act as such. You make the decision about what goes on the list and then you leave the enforcement up to customs; is that right?

Mr. JOHNSTON. That is correct.

Senator NUNN. The State Department does not have investigators going around to determine if compliance is taking place?

Mr. BRYANT. No, sir. Whenever we receive an allegation of willful wrongdoing, we refer the allegation to the U.S. Customs Service for investigation.

Senator NUNN. How does that work? Is that working well?

Mr. BRYANT. We find that that is working quite well.

Senator NUNN. Do you find any disadvantage, any big disadvantage in having the enforcement of the Arms Export Control Act under customs whereas the licensing is under State?

Mr. BRYANT. No, sir. Rather we find it an advantage. Willful violations are investigated much more rapidly, we think, than would be the case if we were doing our own investigations.

Senator NUNN. In other words, you think you are getting along well with that divided kind of responsibility?

Mr. BRYANT. We think the coordination between the two offices is excellent, sir.

Senator NUNN. What level of technical expertise do you need in licensing at State in that function, in the Arms Export Control Act? What kind of person and background do you have to have in that function?

Mr. BRYANT. The licensing officers are generalists, sir. We draw upon the technical expertise of the Department of Defense whenever we have questions as to the level of technology of an item.

Senator NUNN. Is there a certain group in the Department of Defense that you look to for that?

Mr. BRYANT. We have a central office to whom we refer everything and then they refer out to the various services as the need arises.

Senator NUNN. So you do not try to provide all the technical experts in the State Department and you have people with broad policy-type experience?

Mr. BRYANT. No; in the Department of Defense we can draw on defense research and engineering and the technical expertise in the services.

Senator NUNN. Do you have a computerized operation in your munitions function?

Mr. BRYANT. The present system is to some extent computerized and we are now in the process of installing what is called a data-based management system computerizing our whole operation.

Senator NUNN. When will that be operative?

Mr. BRYANT. It is hope that will be operative before the end of the fiscal year.

Senator NUNN. What will that do for you?

Mr. BRYANT. Any application coming into our office will be assigned a number, as it is now. That application enters through a terminal into a minicomputer, and is tracked throughout its whole period of time in the office where it is, what is being done with it, what problems may have arisen with regard to that particular application and when it goes out, what action we took with regard to that application and why.

Senator NUNN. What number of applications would you handle on your munitions control, say, in a year?

Mr. BRYANT. 36,000.

Senator NUNN. That would be the gross number that you look at?

Mr. BRYANT. That would be the gross number of all types of applications.

Senator NUNN. Of the gross number, how many different items will end up being on the munitions list?

Mr. BRYANT. Approximately 95 percent of them, perhaps higher than that.

We deal with a very small community.

The applicants come to us generally speaking, knowing that the item that they are seeking to export is on the U.S. munitions list.

Senator NUNN. What does a manufacturer do if the item is not on the munitions list? What is the difference in what they have to do if it is on the list and if it is not?

Mr. BRYANT. If it is not on the U.S. munitions list, that he goes to the Department of Commerce to seek authorization for export.

Senator NUNN. Then that would get into their function on licensing export?

Mr. BRYANT. That is correct.

Senator NUNN. If it is on the list, they have to go through the State Department?

Mr. BRYANT. They have to go through the Department of State.

Senator NUNN. What about the operation in the Bureau of Economic Affairs? Is that computerized?

Mr. JOHNSTON. We do not really computerize the operations that we do. I should explain to you that the Department of Commerce receives very large numbers of license applications. I do not have the number, but I think it is in the neighborhood of 50,000 to 60,000. They do not call all of these cases to the attention of the State Department or to the Defense Department. There are criteria which are set down and only if those criteria are met are those license applications furnished to one or the other Department. Accordingly, the number of specific licensing requests that we look at is small compared to the number that the Department of Commerce receives.

Senator NUNN. Has the State Department generally been able to work well with the Customs Service in coordinating enforcement efforts under the Arms Export Control Act, both in this country and abroad?

Mr. BUCKLEY. Yes; we have.

As I mentioned in my testimony, they have assigned people to us abroad. All of these mechanisms, of course, are under review to make sure that we get the most effective enforcement possible.

Senator NUNN. Is the United States requesting many exceptions from the Cocom list?

Mr. BUCKLEY. We have an odd phenomenon. Because the Commerce Department put in a very special effort to clean up the backlog, we have a bubble of items before the Cocom at the present time. This is compounded by the fact that where we are most competitive in our trade with the Soviet Union and in the Eastern bloc is in some of the high technology level of dual uses, particularly the computer area.

So combining these two factors, we have a large number of exceptions relative to the number of cases that are up for discussion.

I would say this, though, that we do not ask for an exception except where we have very good evidence to our satisfaction that it has a commercial end use and we have the knowledge that these items will not be used for military purposes.

Senator NUNN. Have we approached Cocom for any exceptions since the Polish crisis came up?

Mr. JOHNSTON. Yes; we have, but not for the Soviet Union.

Senator NUNN. What countries are involved? Or is that a confidential matter?

Mr. JOHNSTON. No; it is not.

The Cocom control list applies to the Soviet Union, to the European Communist countries, with the exception of Yugoslavia, and to China.

We have approached the Cocom for exceptions in regard to those countries other than the Soviet Union.

Senator NUNN. Briefly what countries are included in the restrictions for Cocom? In other words, if you have got a list of things that Cocom agreed to, what countries are excluded from being able to receive those items?

Mr. JOHNSTON. The countries to which the Cocom directs its efforts are the Soviet Union, the Eastern European countries, China, and I believe the other Asian Communist countries.

Senator NUNN. Those are the ones that are on the restricted list?

Mr. JOHNSTON. That is right.

Mr. BUCKLEY. Albania, North Korea, Vietnam, Kampuchea, and Mongolia.

Senator NUNN. Do we have any agreement in Cocom on any non-Communist country?

Mr. BUCKLEY. They are all Communist.

Senator NUNN. So the question of shipping goods to Libya, countries of that nature, would be strictly a national decision?

Mr. JOHNSTON. That is right.

Senator NUNN. Where is that national decision made on those kinds of shipments?

Mr. JOHNSTON. The Export Control Act has three grounds for refusing to let goods out of the United States. One is for strategic purposes, and those are the items that we have been talking about. Those are directed mainly toward the Communist countries. The second is short supply, if we decide that we need a good to stay in this country because we don't have enough of it. That is another possibility. The third is for foreign policy reasons. It is the foreign policy controls which you are talking about with respect to Libya. In those foreign policy controls we have got a number of subdivisions. One is if there is a regional problem because of some military activity that is going on; the second one is human rights controls, if we think that a country has not been behaving as well as it should on human rights; a third is terrorism control.

Senator NUNN. Mr. Secretary, if you had to point out two or three weaknesses in our present policies that you are most concerned about, how would you list those? What areas of improvement are you most concerned with?

Mr. BUCKLEY. I think that there is room for improvement in coordination and we are working on that. In fact, just yesterday we had a meeting of a number of involved agencies, to address precisely those questions. There are 12 different agencies in the Government involved in this area, 42 groups. And a lot of them are very specialized.

We need to have a better idea of what each one of us is doing.

Another area, and this is what I had in mind when I referred to some of the inevitable delays, is in having a better idea of what really is critical. One of the dangers we have to avoid is that we put too much into these lists. Then you have two things: First, you splinter time for enforcement; second, you raise resistance on the part of our allies. An innovative industrialist such as Fred Bucy of Texas Instruments has been very useful in emphasizing the importance of things like manufacturing processes, not the goods, but how the devil do you make those

goods—right. We have asked our intelligence services to focus in these areas and also to focus on the techniques by which the Communists sniff out what we are doing. Here is another area of a more precise definition of what it is we should be controlling. Finally, an area we have under discussion is the person to person transmission of ideas and technologies, the visitors who come to this country and attend universities, and so on.

There is the leakage that comes out of businessmen going around the world, not being conscious of how precious their concepts are. So I think this is another area where we have to come up with procedures and mechanisms for enforcing policies; in heightening the understanding of the American manufacturing community and foreign manufacturing communities of the dangers of leakage through observation of manufacturing processes and also trying to figure out that delicate line between pure academic, research, science, and applied science in the potential military area. This thought leads me to a final area where I think we have yet to come to grips with sufficient precision; that is, identifying the emerging technology that usually starts out with the commercial use but nevertheless predictably will have military applications.

Senator NUNN. There was a suggestion earlier in the week in our hearing by Dr. Lara Baker of Los Alamos that a group of technical experts away from Washington could serve as a strictly technical nonpolicy clearinghouse where everything could channel through there in terms of technical questions without any reference to policy. I know that there are some people in the intelligence and defense communities doing that. I am not certain where that should be housed. There was a strong opinion it ought to be done away from Washington so it doesn't get caught up in the Department of Defense policy versus the Department of State policy, or the Commerce policy on export versus the others.

That is an idea that ought to be looked at. The feeling was there wasn't any one central clearinghouse for technical expertise, not that they would all be housed there, but that they would serve as the focal point for that.

The estimate was it would take about 20 professional people and about $5 million a year and that an awful lot of the expertise would already be there in working in other areas.

There also was a suggestion made by Dr. Lara Baker exactly what you just alluded to, that we ought to spend more time narrowing down the list of what is critical to the Soviet Union; in other words, sort of reverse engineering espionage efforts so that we would have a much narrower list and try to do what we do well, rather than trying to control too much and not controlling anything well. I think that is what you are saying.

Mr. BUCKLEY. Yes.

Senator NUNN. I would bring that suggestion about one central clearinghouse on technical information to your attention.

Mr. BUCKLEY. I would appreciate that.

Senator NUNN. I am not looking for another agency, but it might be the voice for any policymaking kind of persuasion. DOD always is willing to take a more restrictive approach. That is their job. Com-

merce is going to take a more export-minded approach, which is natural. That is the business they are in. The State Department is going to look from the foreign policy aspects.

All of these agencies, as good a job as they do, are very much involved in the policy type application.

I would throw that out for your consideration.

Mr. BUCKLEY. It is a very interesting idea. We should follow up on it.

Senator NUNN. Mr. Secretary, I want to thank you and your associates for being here this morning. We appreciate the good job you are doing. I know that this administration is very much concerned about the policy in this area.

The purpose of these hearings is not so much to determine policy, but rather to determine how it is we carry out that policy and how does the Government work once the President makes his pronouncements.

One of the interesting things we had early in the week was a pretty thorough examination of the Commerce Department's own internal numbers of people dealing in each one of these agencies. They are trying to revoke the license and enforce the law with a very small number of people. Another thing you would find of interest is that after former President Carter announced the grain embargo, the people responsible for going out and investigating violations and pursuing those totaled one person in the Department of Commerce. Interestingly enough, I guess it follows that having one person involved in that whole investigative effort that there was 100 percent compliance, according to the statistics. No one violated the grain embargo.

Mr. BUCKLEY. I think, Mr. Chairman, that this last area is one that ought to be looked at, the resources to do the job.

Senator NUNN. Thank you very much.

Our next witness is Mr. Edward J. O'Malley, Assistant Director, Intelligence Division, Federal Bureau of Investigation.

Mr. O'Malley, we swear in all witnesses before our subcommittee. Would you hold up your right hand?

Do you swear the testimony you will give before the subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. O'MALLEY. I do.

TESTIMONY OF EDWARD J. O'MALLEY, ASSISTANT DIRECTOR, INTELLIGENCE DIVISION, FBI

Senator NUNN. We know you have a statement. We will ask you to proceed with that.

Mr. O'MALLEY. Thank you very much, Senator.

I appreciate the opportunity afforded me to appear before you today to review the FBI's role and responsibilities in the area of technology transfer.

As you are aware, we covered some of this ground in our previous correspondence with you. I will expand on those issues and respond to any other specific questions you may have concering the FBI's role. My responses and comments here today will, of course, be unclassified. Much of the counterintelligence activity we engage in to counter the

activities of the hostile intelligence services to acquire our tecnology is classified. Therefore, to be more specific and responsive to your interests, I have furnished to you certain written comments which are classified.

We, in the intelligence community in general and in the FBI in particular, are acutely aware of the legitimate concern of the various congressional committees in this area of technology transfer and appreciate the efforts you are expending to bring these concerns out front and before the public.

We hope that by the additional exposure of this issue through these public hearings the magnitude of this problem will be more fully understood.

Basic to the understanding of this issue is the need to recognize and acknowledge the nature of the U.S. society—a free and open society. It is within the framework of this openness that the FBI must operate to counter the activities of the hostile intelligence services to acquire U.S. technology.

Our counterintelligence activities are conducted in accordance with a recently signed Executive order—E.O. 12333—and within the framework of the Attorney General guidelines which are currently being revised.

There is nothing contained within the parameters of those two documents which adversely affects our ability to carry out our counterintelligence responsibilities. Being a law enforcement agency, our agent personnel are thoroughly trained in the judicial process necessary to successfully prosecute a case.

We realize the importance and necessity of obtaining sufficient evidence to prosecute a case if that, in fact, is the ultimate objective of a particular counterintelligence investigation. Prosecution resulting from a counterintelligence investigation would normally be under the espionage statute. Though the espionage statute does not stipulate that only cases involving classified information can be prosecuted, legal precedent has established such a requirement.

Diplomatic immunity, of course, precludes prosecution; therefore, in those counterintelligence investigations involving officials with immunity the counterintelligence objective against such officials would probably be to have the subject declared persona non grata.

Naturally the elements of proof for such action are not as stringent. There are, of course, benefits other than prosecution and personal non grata action that accrue from other counterintelligence investigations. These include the identification of intelligence officers, their agents and contacts, modus operandi of the hostile intelligence services, and their targets—all meaningful counterintelligence objectives.

The Soviets correctly view the United States and several other Western countries as a continuing source of important and openly available scientific and technical information, to which they take every opportunity to obtain access.

Some of the unclassified documents so acquired are previously classified materials which had been declassified through U.S. procedures providing for automatic declassification after a stipulated period. When collected on a massive scale and centrally processed by the Soviets, this information becomes significant because it is collectively used by Soviet weapons designers and weapons countermeasures experts.

The Soviets also regularly attend high-technology trade shows and visit commercial firms in the West, particularly small- and medium-sized firms that are active in developing new technologies. These apparent trade promotion efforts often mask Soviet attempts to acquire emerging Western technological know-how before its military uses have been identified and Government security controls have been applied. Emerging technologies are particularly vulnerable to foreign collection efforts of this type.

Because of the ease by which unclassified technology and proprietary information is obtained, the gain is very substantial. Soviet acquisition efforts are massive, involving many Soviets traveling outside the Soviet Union.

Literally thousands of Soviet bloc persons enter this country each year—trade delegations, students and other academic exchange participants, diplomats, and seamen—and all have the potential to collect information/technology, most of it open source and unclassified.

Those efforts are well rewarded and in an open society such as ours there will undoubtedly be no degradation of those efforts. The acquisition of classified information falls more to their trained and experienced intelligence officers.

It is in this area that the FBI's counterintelligence activities are mainly concentrated.

Illustrative of those collection efforts of unclassified information is an incident that occurred Ely, Nev., in late 1979, and comments which appeared in the Washington Post. (Additional information concerning this is being made available to you in classified form.)

In October 1979, two Soviets, dressed in jeans and sport shirts and almost 2,500 miles from their posts in Washington, D.C., visited Ely, Nev., a potential basing site for some MX missiles. They identified themselves as Vladimir Kvasov and Vladimir Militsyn, listed respectively by the Soviet Embassy as a lieutenant commander/assistant military attaché and as a civilian employee of the attaché's office. The assistant librarian at the Ely Public Library was previously notified by the FBI as to a possible visit by them. They showed up at the library dressed very casual and described themselves as travelers from Washington.

The younger Russian went to the newspaper rack while his friend asked for books on industry in Las Vegas. Las Vegas is a restricted area for Soviet Embassy personnel because of its proximity to Nellis Air Force Base and the Nevada nuclear test site.

After browsing, they both came back with a book on the Nevada sites—a 300-page environmental impact statement for the Nevada site where the U.S. Government conducts underground tests of its nuclear weapons. They received permission to copy the volume which was done at a cost of $47 at a nearby store. The Russian who did the copying identified himself as an energy engineer from Washington. The two Russians subsequently made several other stops inquiring about the area and the kinds of industry in the area.

An important aspect of our counterintelligence approach to limit or attempt to negate technology loss is the need to develop an awareness of the problem—the threat posed by the activities of the hostile intelligence services.

We in the FBI have a dedicated program which we call DECA—development of counterintelligence awareness—which was instituted some 4 years ago to address this issue.

This awareness program is targeted at defense-related companies involved in U.S. classified contracts—at the secret and top secret level—some 11,000 throughout the United States. These firms are identified to us through the Defense Logistics Agency. We work closely with the Defense Contract Administration Services regions throughout the United States in coordinating our awareness programs. Each of our field offices has at least one special agent who is responsible for this program.

The essence of the program is to alert company management and security personnel of the possible threat to that company—because of its classified contract—posed by the hostile intelligence services.

Senator NUNN. Do you take the initiative in contacting these companies or do you go through trade associations?

Mr. O'MALLEY. We contact the companies directly. We have identified the companies in each one of our field divisions which have classified contracts and we then approach them directly.

Senator NUNN. What kind of cooperation are you getting?

Mr. O'MALLEY. It has been excellent. We are there in a sense that we are not concerned about the legitimate approved trade they have with the Warsaw Pact countries but to alert them to the threat posed by the services especially the hostile intelligence services of these countries, their efforts to obtain illegally, clandestinely, their technology.

Senator NUNN. Do you have a list when your agents call on them? Do you have a list of critical technology that may be involved?

Mr. O'MALLEY. It depends on the industry. We are aware of what technologies the other side is looking for. If we approach somebody in the aerospace industry, we will alert them as to our knowledge of what the other side is seeking which may be relevant to their particular company.

It is hoped that the threat information imparted will be incorporated into the routine security briefings each of those companies is required to give its employees. Additionally, articles such as one prepared by the FBI entitled "Secrets, Spies and Citizens" are made available to the company for distribution to its employees.

In addition to the field level participation, senior Bureau Headquarters personnel including Director Webster and me address this awareness issue in speeches to senior industrial management personnel throughout the country. A recent example was Director Webster's comments to the Electronic Industries Association at Boca Raton, Fla., in January of this year.

Electronic expertise in Silicon Valley is widely recognized in the United States and abroad. Technology transfers within and from Silicon Valley can occur in different manners. The Santa Clara County sheriff discovered a vast black market in stolen electronic chips. Many of these stolen chips are sold and used in the United States, but some find their way abroad. When illegal exports have been uncovered in Silicon Valley, Federal agencies become involved in the investigations.

Federal involvement can result in several ways. If the technology is classified for national security purposes, the FBI will investigate

95-929 O - 82 - 12

charges of espionage. If unclassified technology, valued at more than $5,000 is stolen and transferred across State lines, the FBI can investigate under Interstate Transportation of Stolen Property statute. The U.S. Department of Commerce and the U.S. Customs Service investigate violations of the Export Administration Act, which normally involve the sale and export of technology listed on the commodity control list without obtaining specific authorization from the Department of Commerce. The U.S. Customs Service also investigates violations of the Arms Export Control Act, which normally involve the sale and export of arms, ammunition, weapons platforms and special military equipment without obtaining specific authorization from the State Department.

Although the FBI does not initiate investigations of violations of the Export Administration Act or the Arms Export Control Act per se, foreign counterintelligence and other authorized criminal investigations can uncover violations of these acts. When a foreign counterintelligence investigations uncovers such a violation, it can be easily integrated into the ongoing investigation. Our primary interest in these cases is the activity of foreign intelligence services in the United States.

Senator NUNN. What if the Commerce Department picks up the phone and tells them they have an Export Administration Act violation, do you have jurisdiction over this?

Mr. O'MALLEY. It is clearly an export violation, we don't have jurisdiction.

Senator NUNN. Let's say they suspect it may eventually be going to a Warsaw Pact country?

Mr. O'MALLEY. In that case we would have an interest from the counterintelligence standpoint. We do have foreign counterintelligence cases where we have developed information which would also be a violation of the Export Administration Act.

Senator NUNN. Even if it is not classified, you still have jurisdiction if it involves foreign?

Mr. O'MALLEY. If we investigate the activities of all hostile intelligence services in the United States, we do not have to wait until there is a violation of some law to initiative an investigation of these hostile services. We are interested in whatever they are doing in the United States and if it involves sensitive but unclassified technology we certainly would be interested in that.

Senator NUNN. Suppose it is a citizen of West Germany with a legitimate export license, on a nonclassified, item. Commerce tells you they suspect that eventually this may find its way to the Soviet Union. What is your justification in that?

Mr. O'MALLEY. In a case like that we would be interested in the sense of a counterintelligence investigation that the odds are that if something is being transshipped, something that has been legally exported to a Western European country is being transshipped to the Soviet Union, the odds are that there is some involvement by a hostile intelligence service. Within that context, we would certainly have interest.

Senator NUNN. When you say you have an interest in it, does that mean you would actually pursue it, investigate it? Do you think you have the jurisdiction?

Mr. O'MALLEY. Yes; we would. We would pursue that.

We have an excellent day-to-day relationship with the Compliance Division of the Department of Commerce.

Senator NUNN. Are you saying the relationship is being upgraded and expanded with the Commerce Compliance?

Mr. O'MALLEY. I am saying our relationship with the Compliance Division, Department of Commerce, is being enhanced at the current time. I understand that measures are being taken within the Compliance Division to expand its own capabilities.

We also enjoy an outstanding working relationship with the U.S. Customs Service.

In the Boca Raton speech, Mr. Webster called the *William Holden Bell-Marian Zacharski* case a "textbook example of espionage, or the illegal transfer of technology."

The scenario of the "textbook example of espionage" as depicted by Mr. Webster in his Boca Raton speech in general terms, was vividly seen in the development of the *William Holden Bell-Marian Zacharski* case.

The chance social meeting took place at the Cross Creek Village apartment complex, Playa Del Rey, Calif. in the fall of 1977. Both Bell and Zacharski resided at this complex with their wives. A personal friendship between Bell and Zacharski developed. A mutual interest in tennis which resulted in almost daily sessions contributed greatly to the relationship.

During the next few months Zacharski skillfully cultivated Bell, a man 30 years his senior. This cultivation process was so thorough that it even included their tennis activity. Zacharski insisted on playing Bell regularly despite the fact he was a far superior opponent, and he purposely adjusted his game to match Bell's lower level of ability.

More importantly, he discovered that Bell had experienced a costly divorce in 1976 and had declared bankruptcy the same year, making him a most vulnerable recruitment target. During the sounding out period, Zacharski learned that Bell was privy to a great deal of classified information concerning airborne radar systems and related military equipment. Zacharski requested and received from Bell copies of a Hughes Aircraft Co. newsletter entitled "Hughes News" and another Hughes publication called "Vector," both publications unclassified and available to the public.

The "moment of truth" for Bell occurred in late 1978, when the apartment complex converted to condominium status. Because of his precarious financial situation Bell was unable to produce a down payment to purchase his unit. At this point Zacharski offered to help in the form of cash in return for more technical documents generated by Hughes Aircraft.

Although reluctantly, Bell accepted the offer and the illegal transfer of technology began. The rest of the story reads like a spy novel—special camera provided by Zacharski to photograph classified documents, secret meetings between Bell and Polish intelligence officers abroad, cryptic telephone contacts using code names and payment in gold. Bell testified to having been paid almost $170,000—a sum for which he sold out his company and his country.

I might add that it is my understanding that Mr. Bell testified earlier this week that the FBI had sat around for 2 or 3 years and watched him pass classified documents to the Poles. I categorically

reject that. We would certainly not stand by and watch anybody pass classified documents to any hostile intelligence service or to anyone else for that matter.

In conclusion, I would like to state that the FBI will continue to pursue the counterintelligence implications of technology transfer and provide intelligence support to those law enforcement elements outside the FBI that have statutory responsibilities for export control. Technology loss can be reduced through these concerted and coordinated efforts even within the framework of our open society and current operating procedures.

Senator NUNN. On that latter point, I think what Mr. Bell was saying was that he was under surveillance at the time he passed certain valuable information. Are you denying that?

Mr. O'MALLEY. I am not denying that he was under surveillance. What I am saying is that it was our observation that he was not at any time passing classified documents where we had no information at the time of our surveillance that he had passed any classified information. What we need, Senator, as you are well aware, is proof, hard proof that he has passed those documents and the instant we had such proof, of course, we prosecuted him and Mr. Zacharski.

Senator NUNN. Of course only a law enforcement agency can make that judgment. We are not here trying to make that judgment. We are certainly not being critical of the FBI in the *Bell* case. But as I understood it, what he was saying was that he was under surveillance while he was passing that information. Also I understand there had been a wiretap on him for some time during the period when he was passing information. The wiretap doesn't necessarily tell us that he was passing it.

Mr. O'MALLEY. There are ramifications of what you are asking now. I would be happy to talk to you in closed session.

Senator NUNN. I am not even asking you. That is not a questionmark. Nevertheless, I know it is a difficult thing in getting proof. The point that he did make, though, that should have come through pretty loud and clear is that there were all sorts of suspicious circumstances that someone should have known during the entire period of time that this was going on.

I think he was somewhat amazed with all the circumstances that he wasn't caught sooner. I think it is a lesson to be learned. I don't know by who. Perhaps the FBI did everything possible in the case. Perhaps the private companies involved could do more in alerting law enforcement on specific circumstances when it comes up.

I don't think there is any doubt about the fact though that Mr. Bell did pass certain critical information.

Mr. O'MALLEY. No doubt at all.

Senator NUNN. How important is it for the law enforcement agencies, in cases like the *Zacharski* case, and the *DeGeyter* case, to have a presence abroad and liaison with the foreign law enforcement authorities?

Mr. O'MALLEY. It is absolutely crucial. We have had a long history of such relationships with intelligence agencies and law enforcement agencies abroad. I think it is particularly important in the area of technology transfer, but I think it is well established that more and

critically in Europe, that more and more of the illegal technology transfer is occurring through these European countries. Technology, equipment, dual use products that may be legitimately licensed to European countries are being diverted to Warsaw Pact countries. I think with that in mind it is absolutely crucial that we have close relationships with our counterparts abroad.

Senator NUNN. The FBI is primarily domestic in terms of the overall jurisdiction and enforcement. What is the nature of your relationship with the foreign governments and foreign agencies?

Mr. O'MALLEY. We have no investigative jurisdiction abroad, Senator, but we do have a legal attaché system and those individuals who operate in our behalf in foreign countries have strictly a liaison responsibility. If we determine there is information say in the United States that a certain crime has been committed or about to be committed in Europe we will furnish that information to our counterpart service through our legal attaché. He will conduct no investigation himself but will furnish the lead, if you will, to the local service and the results of that investigation will be furnished back to him to be given to us if it involves U.S. interests.

Senator NUNN. You say you are very pleased so far with your informational program to the business community. Do you think that is working well?

Mr. O'MALLEY. Yes, sir. It is.

Senator NUNN. Could you furnish for the record some statistics that would indicate the degree of briefings that go on between the FBI and private companies?

Mr. O'MALLEY. Yes; for the record I can say that the 11,000 companies that we identified which have or may have secret or top secret contracts, we have so far have talked to 6,000 of them.

Senator NUNN. 6,000?

Mr. O'MALLEY. 6,000.

Senator NUNN. That is by personal visit?

Mr. O'MALLEY. Personal visit.

Senator NUNN. Do you try to contact people who are head of security in those companies primarily?

Mr. O'MALLEY. Yes; particularly the security people or other senior officers who are in the position to pay attention to what we say and to listen to our suggestions and implement them within the company.

Senator NUNN. How many referrals of evidence indicating criminal activity does the FBI receive from the Department of Commerce Compliance Division in a year? Do you have any statistics on that?

Mr. O'MALLEY. I don't have any statistics at hand but I checked and to my knowledge we have not gotten any criminal referrals from the Department of Commerce in the past year.

Senator NUNN. In the past 12 months?

Mr. O'MALLEY. Yes.

Senator NUNN. Would that be calendar year 1981?

Mr. O'MALLEY. I responded to the question I thought you had asked within the past year. But I am not sure in the past few years that we have gotten any criminal referrals.

Senator NUNN. So your records don't reveal any or at least you don't know of any criminal referrals from the Compliance Division of Commerce to the FBI?

Mr. O'MALLEY. That is true.

Senator NUNN. How about criminal referrals by the U.S. Customs Service?

Mr. O'MALLEY. We have a very close working relationship with Customs, both at headquarters and with their field divisions throughout the United States and there has been, although I don't have statistics on it, a number of referrals from us to Customs and vice versa. At the current time we have a number of very, I would say, defined it as substantial cases that we are working jointly with Customs in the technology transfer area.

Senator NUNN. Do you have an established procedure for liaison between the FBI and the Commerce Department in high technology cases?

Mr. O'MALLEY. It is not a written document as such but we do have, I think, fairly well structured relationship with Commerce. We have a liaison officer. We also have, I think, excellent liaison from the very highest levels of Commerce down to the lower levels, and with several different divisions within Commerce. Particularly in the last year we have had a number of meetings between the FBI and Commerce at fairly senior levels, to brief them on our responsibilities, particularly in the counterintelligence area, and to exchange ideas on the whole technology transfer issue in general.

I think they have been very worthwhile. At the present time we are in the process of negotiating with the Department of Commerce a memorandum of understanding which will, I think, enable us to avoid problems that we have experienced in the past of 12-C of the Export Administration Act where we ask for certain information and according to that particular section it was either not forthcoming or there were lots of delays. I think, though, as a result of the meetings that I have been talking about, and the relationship that we have today, that hopefully at least there will be a memorandum of understanding that in the future when the Bureau approaches Commerce requesting certain, particularly licensing-type information that that request each time does not have to go all the way up to the Secretary of Commerce but can be handled let's say at a routine but albeit——

Senator NUNN. You mean at the present time under the present procedures any FBI requests for information have to go all the way to the Secretary of Commerce?

Mr. O'MALLEY. That is required by the Export Administration Act.

Senator NUNN. That is the law?

Mr. O'MALLEY. Yes.

Senator NUNN. What provision of the law is that?

Mr. O'MALLEY. 12-C of the Export Administration Act.

Senator NUNN. Is that proprietary information?

Mr. O'MALLEY. It basically says, licensing information or requests for licensing information cannot be made public without the expressed authority of the Secretary of Commerce unless he decides that it will be in the public interest I gather to release such information. The problem is——

Senator NUNN. Making it public is giving it to the FBI——

Mr. O'MALLEY. That is the way the Commerce has interpreted it in the past, that making it public is synonymous to giving it to other agencies within the Federal Government.

Senator NUNN. Does the Justice Department to your knowledge agree with that interpretation of the present law?

Mr. O'MALLEY. They do not agree with that.

Senator NUNN. So the Justice Department believes that the Commerce Department without changing the law could actually share that information with the FBI?

Mr. O'MALLEY. Yes; I believe the Justice Department has prepared, the Office of Legal Counsel, has prepared a study on that and communicated the results of that study to the Department of Commerce.

Senator NUNN. I am informed by staff that that law was amended last year, in December specifically to permit that information to be passed for investigative purposes. Are you familiar with that?

Mr. O'MALLEY. I am not.

Senator NUNN. Could you ask the Justice Department to furnish us their position on the current law, whether there is a change in the law needed to permit that kind of cooperation?

Mr. O'MALLEY. I will ask the Department.

Senator NUNN. I will pose the same question to the Commerce Department when they testify next week. Your own view is so far as you know the Justice Department believes the Commerce Department has it within their authority to permit that under existing law?

Mr. O'MALLEY. Yes.

Senator NUNN. Do you know how many technology transfer cases have been worked jointly in the last year by the FBI and the Commerce Department?

Mr. O'MALLEY. I don't believe we have worked any cases jointly. We normally contact the Commerce Department where we have a question regarding certain licensing information or whether or not a given item is on the commodity control list and therefore embargoed for transport abroad, particularly to a Warsaw Pact country.

Senator NUNN. How about the Customs Service? Do you have cases that you work jointly with them?

Mr. O'MALLEY. We certainly do. We have a substantial number of such cases going on at the present time.

Senator NUNN. How do you explain the lack of having any referrals from the Compliance Division of the Commerce Department to the FBI and how do you explain the lack of having any joint cases you are working with the Compliance Division? Is there a reason for that that is not readily apparent?

Mr. O'MALLEY. I think it is probably because in the past Commerce has been understaffed. They do not have, compared to Customs, the number of investigators out in the field or the people with the same kind of law enforcement training, that people in the field in terms of Customs would have. We have a tradition which transcends the technology transfer issue of working very closely with Customs. They have a large presence as the Department of State indicated throughout the country of all the key ports. So I think these are the general reasons why we exchange information more frequently with Customs than we would with Commerce.

Senator NUNN. Are you familiar with the *DeGeyter* case?

Mr. O'MALLEY. Yes; I am.

Senator NUNN. Was that an FBI case?

Mr. O'MALLEY. Yes.

Senator NUNN. Did you work with Commerce on that?

Mr. O'MALLEY. No. We did not work the case jointly with Commerce. We consulted Commerce as to whether or not the information being sought by Mr. DeGeyter was on the commodity control list, or something within that data base management system would have qualified it as sensitive enough to bring it within the parameters of the Export Administration Act.

Senator NUNN. So the Commerce Department simply answered inquiry by you on that case?

Mr. O'MALLEY. That is right.

Senator NUNN. Were you aware that the *DeGeyter* case was listed in the Commerce Department's annual report as a "criminal proceeding handled through the Compliance Division"?

Mr. O'MALLEY. I have been told that it was. I am a little mystified as to why it was said, perhaps there is a reason why they said that. I am not sure. I haven't discussed it with them.

Senator NUNN. What areas would you point out where coordination can be improved between the FBI and the other Federal agencies in this area?

Mr. O'MALLEY. I think an awful lot has been done in the past year, 18 months, Senator, on this issue, both within the intelligence community itself and between the intelligence community and the export control community. There are a number of committees in the intelligence community and outside the community that we all sit on and I think that it is working very well. Commerce sits on it, State sits on it, Customs, all the export control community agencies as well as ours and other members of the intelligence community, including Defense and CIA. So I think a lot has been achieved in terms of coordination, but I think like anything else, there still can be more achievements. I think even more coordination in the future.

But I can say, with a fair degree of certainty, that there is no issue of greater importance in the intelligence community today than the technology transfer issue.

Senator NUNN. I certainly agree with that. Do you have any difficulty getting people in the Commerce Department who have security clearances so you can deal with them in your counterintelligence informational exchange?

Mr. O'MALLEY. There was a problem in the past on that issue. We brought it to the attention of the Commerce Department and appropriate clearances were obtained for people within the Compliance Division.

Senator NUNN. So you think that problem has been smoothed out?

Mr. O'MALLEY. I think it has been.

Senator NUNN. We were told during the grain embargo that at one of the high level meetings someone was excluded from the meetings because of clearance?

Mr. O'MALLEY. That happened initially. That is the exact situation I was discussing with you. That happened in the initial meeting. We found out he did not have appropriate clearances. We brought it to the attention of Commerce and they saw to it that these people were given clearances and thereafter they sat in on our meetings.

Senator NUNN. So you don't think that is a problem at this point in time?

Mr. O'MALLEY. I do not. I think the Commerce Department has tightened up its security substantially over the past 2 years.

Senator NUNN. Do you feel in your personal opinion that the Commerce Department is capable of—the Compliance Division in the Commerce Department—is capable of effectively enforcing the Export Administration Act as it is presently constituted?

Mr. O'MALLEY. I mentioned earlier some of the problems that Commerce would acknowledge themselves in terms of a lack of sufficient personnel, a lack of training, a lack of presence throughout the United States and abroad. There is one or two ways that that can be resolved, either increase or improve the capabilities of Commerce in the areas that I mentioned or consider transferring it to another agency.

Senator NUNN. Would the Customs Service be better able to handle the enforcement of the Export Administration Act than the Compliance Division?

Mr. O'MALLEY. The only thing that I can say in regard to that question, Senator, is that the Customs Service does have a larger presence, both here in the United States and abroad. Their training is better. They have law enforcement powers which Commerce people do not have. I believe it would be inapproprate for me to publicly——

Senator NUNN. I understand, but your relationship with the Customs Service in this overall area is very professional, very good?

Mr. O'MALLEY. It is excellent.

Senator NUNN. What about the Silicon Valley problem? We have heard testimony that there is a huge theft problem in the Silicon Valley. An awful lot of the enforcement in the past has been left up to both police and sheriffs and local prosecutors and so forth. Has the FBI moved into that area in recent months?

Mr. O'MALLEY. Senator, I understand what you are saying, that there has been a tremendous amount of work done by the local authorities in the Silicon Valley area. But I must add also that there is a substantial Federal presence in that area also in terms of our own operations and the operations of customs. Silicon Valley is a cause of concern for us. It is of obvious interest to the Warsaw Pact countries. As serious as it is, it is one of many problems that we have throughout the country in the technology transfer area.

Our presence there as I indicated is substantial and I would be, I think, very happy to go into closed session with you for the details on that presence.

Senator NUNN. Fine. We are going to need to have a closed session because we had certain questions that came up yesterday about misdemeanor pleas on a very serious case that involved national security and we are going to have to hear that in closed session. So we would like to talk to you in closed session on the other too.

I want you to understand that we have not taken a look at the *Bell* case from the point of view of determining whether law enforcement efforts were excellent, good, or fair. We are making no finding or implication. Nothing I said should indicate that we are in any way criticizing the FBI on the *Bell* case. We did hear testimony from him yesterday.

Mr. O'MALLEY. I understand that, Senator, but I saw the newspaper piece regarding Mr. Bell's testimony. That is the only reason I responded to that, not because of anything that you have said or anyone else.

Senator NUNN. The implication I got from his testimony was that there were a lot of signs there that his own company should have

caught or someone should have caught earlier. But I certainly am not making any statement to that effect. We just haven't looked at it in that aspect. We have looked at it in the aspect of whether this tells us something about our overall capability in this area and whether the business community can do more themselves.

Have you been a member of a working group on export controls?

Mr. O'MALLEY. Yes; I have.

Senator NUNN. What is that group?

Mr. O'MALLEY. It was a group, as a matter of fact, you mean the FBI or me personally?

Senator NUNN. Both.

Mr. O'MALLEY. The FBI is currently a member of four or five such groups on export control. As I said, both within the intelligence community and combined with the intelligence community and the export control community. I also chaired a committee about 3 years ago looking into the entire problem of export control.

Senator NUNN. Has that group had recommendations?

Mr. O'MALLEY. Yes; it has.

Senator NUNN. Whom did the recommendations go to?

Mr. O'MALLEY. Those recommendations went to the National Security Council.

Senator NUNN. When did they go to the National Security Council?

Mr. O'MALLEY. If my recollection serves me it was in December 1979.

Senator NUNN. December 1979?

Mr. O'MALLEY. Yes.

Senator NUNN. Have those recommendations or some of those recommendations been acted on?

Mr. O'MALLEY. Yes; they have.

Senator NUNN. Have some of them not been acted on?

Mr. O'MALLEY. That is also true.

Senator NUNN. Are these classified recommendations?

Mr. O'MALLEY. Yes, they are.

Senator NUNN. At the appropriate time in a closed session, are you permitted to go into that?

Mr. O'MALLEY. No; that is a national security document and I cannot comment even though I chaired the committee, I cannot comment on anything that is in that report and the only thing I would do would be to recommend that you approach someone in the National Security Council for that document.

Senator NUNN. You are familiar with it?

Mr. O'MALLEY. Yes.

Senator NUNN. But you have to get permission from them?

Mr. O'MALLEY. I cannot discuss it.

Senator NUNN. We will pursue that with the National Security Council and perhaps go into that in closed session also. It is certainly relevant to the hearings, if you have an expert group of people looking at it and coming to conclusions. We will pursue that. We appreciate very much your being here. We appreciate the cooperation of the FBI.

Mr. O'MALLEY. Thank you, Senator.

Senator NUNN. Thank you.

Our next witness is Mr. Arthur Van Cook, Director of Information Security, Department of Defense, and Chairman, National Disclosure

Policy Committee. Do you have anyone else with you this morning?

Mr. VAN COOK. I have one of my staff.

Senator NUNN. We would be glad for him to come up. If he is going to testify, I will swear him in.

Mr. VAN COOK. He is not going to testify.

Senator NUNN. Will you hold up your right hand? Do you swear the testimony you will give the subcommittee to be the truth the whole truth, and nothing but the truth, so help you God?

Mr. VAN COOK. I do.

Senator NUNN. We appreciate you being here this morning. We appreciate your cooperation. We look forward to getting your testimony. You go right ahead.

TESTIMONY OF ARTHUR VAN COOK, DIRECTOR OF INFORMATION SECURITY, DEPARTMENT OF DEFENSE, AND CHAIRMAN, NATIONAL DISCLOSURE POLICY COMMITTEE

Mr. VAN COOK. Thank you, Mr. Chairman. I do hold the position of Director of Information Security in the Department of Defense. I am also designated as the Chairman of the National Disclosure Policy Committee and I am the U.S. representative to the NATO Security Committee.

In these capacities and with these titles I am responsible for policy development and oversight of DOD activities in the areas of information security and foreign disclosure.

Senator NUNN. What did you say your position was in terms of NATO?

Mr. VAN COOK. I am the U.S. representative to the NATO Security Committee, sir.

Senator NUNN. Does that committee interrelate with Cocom?

Mr. VAN COOK. No, sir.

Senator NUNN. It has no relationship with that?

Mr. VAN COOK. No.

Senator NUNN. Is there a body in NATO that has any feed into the Cocom decisions on export?

Mr. VAN COOK. Not to my knowledge, sir. As a NATO body.

Senator NUNN. I would like to pursue that with you. But go ahead with your statement. We will get to it.

Mr. VAN COOK. Yes, sir.

I welcome this opportunity to discuss the problem of technology transfer to the Soviet Union and other Soviet bloc nations. The Department of Defense has been concerned for some time about the virtual unremitting flow of unclassified defense information to our adversaries. This hemmorrhage of information to hostile nations, particularly technology and technical data with military applications, is one of the more serious problems confronting the Department.

Soviet bloc acquisitions of unclassified national security related publications greatly enhances their capabilities to design, produce and field weapons systems of all types, as well as develop measures to counter U.S. weapons systems. It cuts their production costs, shortens their production times, and improves the quality of their product.

A Soviet scientist who defected several years ago and others told Congress that the majority of Soviet information collection require-

ments can be openly obtained in the United States. The Federal Bureau of Investigation has estimated that as high as 90 percent of the Soviet collection requirements can be satisfied through open sources. A recent unclassified CIA report states that Soviet intelligence organizations have been so successful at acquiring Western technology that the manpower levels allocated to this effort have increased significantly since the 1970's to the point where there are now several thousand technology collection officers at work.

We are painfully aware of Communist bloc efforts within the United States to obtain technology, mostly through legal means, that is, through open literature, which we are powerless to stop. Prior to February 1980, for example, we stood helplessly by as the Soviet Union purchased 80,000 technical documents from the National Technical Information Service (NTIS). Although their access to the NTIS has now been officially terminated, their surrogates undoubtedly continue to exploit this source of extremely valuable information.

Members of Congress, industry spokesmen, and the media frequently lament this state of affairs, and ask is there nothing that can be done. Generally, these activities are carried out overtly and do not violate existing U.S. law. In fact, it has always been presumed that little could or should be done to limit such acquisitions, relying instead upon the ability of the publishers of such documents to properly secure sensitive information by using the existing security classification system However, much of this information is not classifiable under existing rules. The existing classification criteria does not provide adequate protection to a large body of sensitive national security information, particularly militarily critical technology and operational data developed solely for the use of our Armed Forces.

Classification of such information has been neither possible nor practical. Although such sensitive national security information fits the categories permitted to be classified, it does not rise to the level of the "damage" standard of the Executive order governing classification. Disclosure of the technical characteristics of electronic components used in a missile guidance system, for example, may not appear to damage the national security, and yet may well provide our adversaries with precisely what they need to produce a more effective missile. It is this "damage" standard that is applied by originators in deciding whether to make their documents unclassified or to protect them by security classification. Uppermost in their minds is the realization that the test for classification could receive judicial review.

Consequently, if a determination is made not to classify, this information is vulnerable under the Freedom of Information Act [FOIA] since the information does not fall within one of the nonsecurity exemptions to mandatory disclosure. It therefore becomes available and this valuable technological and operational information can be utilized by our adversaries to the military benefit.

Senator NUNN. Is it correct that foreign citizens have access to information in America under the Freedom of Information Act?

Mr. VAN COOK. Yes; they do, sir.

Senator NUNN. If President Brezhnev sends over a freedom-of-information request to the Department of Defense and it is not classified, what is the law on that?

Mr. VAN COOK. The law would be if it is not exempt under the nine exemptions of the Freedom of Information Act, classification being one, that he would get the information he asked for.

Senator NUNN. So if the President of the Soviet Union sent over a request for 100 different items under the Freedom of Information Act, signed his own name, signed as President of the Soviet Union, he would be entitled to that information under present law?

Mr. VAN COOK. It would be interpreted to be a member of the public under that act.

Senator NUNN. Have there been any recommendations made by the Department of Defense or any other agency in respect to access of foreign citizen to that?

Mr. VAN COOK. There have been by the executive branch. The Privacy Act provides that the information can be asked for by a U.S. citizen or permanent resident alien and that same language was proposed for the Freedom of Information Act. My view would be that it would be helpful to have that language in the act if in the initial request the individual is identified as a foreign national. But I think it would be very difficult to enforce.

Senator NUNN. Why is that?

Mr. VAN COOK. Any citizen or anyone who wrote in, we would be in the position of probably asking them for their birth certificate to prove that they were a U.S. citizen.

Senator NUNN. Shouldn't there at least be a prima facie showing of citizenship on the application?

Mr. VAN COOK. It would be very difficult to enforce. I think it would be helpful nevertheless. There are——

Senator NUNN. We are saying right now if Fidel Castro wrote in to the Department of Defense and said he wanted 200 items that were unclassified, that you would have to send them to him?

Mr. VAN COOK. That is correct, sir. If the items were not covered by the exemptions.

Senator NUNN. Qadhafi in Libya. Is that correct?

Mr. VAN COOK. That is right.

Senator NUNN. The ayatolla of Iran?

Mr. VAN COOK. Yes, sir.

Senator NUNN. Don't you think on the face of it that is ludicrous?

Mr. VAN COOK. Yes, sir. I do.

Senator NUNN. So do I.

Suppose there is a hypothetical spy trial going on in West Germany. Two or three East Germans are being tried for espionage. Suppose during the course of that trial they write into the Department of Defense and ask for certain information under the Freedom of Information Act. What would be the law under that circumstance?

Mr. VAN COOK. The law would be that they would be entitled to the information that they requested but we would certainly be reluctant to give it to them with the knowledge that they were on trial for espionage in their own country.

Senator NUNN. You would be slow. You would put that request at the bottom of the pile?

Mr. VAN COOK. I think we would handle that very carefully, sir.

Senator NUNN. Let's say the situation developed in this country where there were people who were charged, as being spies and were

being tried under the Espionage Act. Would they still be entitled to the Freedom of Information requests?

Mr. VAN. COOK. Yes; they would.

Senator NUNN. How about the case we heard earlier this week, the *Bell* case? He is convicted of violating American law and giving away national security secrets and he says very openly that he did and so forth. What is his status under the Freedom of Information Act?

Mr. VAN COOK. He would be eligible to request information under the Freedom of Information Act and if it could not be withheld under the provisions of this statute, he would receive it.

Senator NUNN. So if he were to write in, ask for certain high technology items and so forth, that are not classified, he would be entitled to that?

Mr. VAN COOK. Yes; he would be entitled to receive it under the Freedom of Information Act. Yes, sir, if there were no other restrictions, no restraints under the act.

Senator NUNN. Are there any other restraints under the law?

Mr. VAN COOK. There are nine exemptions under the Freedom of Information Act, the first of which is classification.

Senator NUNN. But it relates to the material itself and not to the applicant?

Mr. VAN COOK. That is correct, sir.

Senator NUNN. So, Mr. Bell, a convicted felon, would have the same rights under the Freedom of Information Act as the New York Times reporter or the Washington Post reporter?

Mr. VAN COOK. Yes; we have the experience of a Norwegian citizen, I believe the name is Gletich, who was an access professional you might say. He asked us on 23 different occasions for information under the Freedom of Information Act. This man was put on trial for espionage in his own country and was convicted. To some of those requests we did respond favorably and some we did not.

But this is an example——

Senator NUNN. Would you have responded favorably on some after he was convicted?

Mr. VAN COOK. No; this was prior to the time that he went on trial.

Senator NUNN. But he has been convicted now?

Mr. VAN COOK. He has been convicted.

Senator NUNN. Would he still be entitled to get the information?

Mr. VAN COOK. Now that we know that the individual is tried and convicted, I would suspect that we would work that case very carefully but nevertheless I believe under the law——

Senator NUNN. If he had a good lawyer he could go to court and get it?

Mr. VAN COOK. He could go to court and get it; yes.

Senator NUNN. Go ahead.

Mr. VAN COOK. As Admiral Inman has remarked, a "cottage industry" has been created by the Freedom of Information Act. Access professionals and data brokers use the act to gather information, repackage it, and market their information product in the United States and abroad. Openness is a desirable social and economic commodity, but we must not lose sight that such openness comes at a cost. It has been presumed that the rapid dissemination of information is socially

and economically good because it avoids duplication of effort, fosters competition, and beneficially spreads technology.

But, there is a hidden cost. While it may be argued, for example, that a full and free exchange of information is necessary if the United States is even to maintain its technological world leadership, it is my concern that it is this very full and free exchange of information that may be causing that technological lead to wane.

I have just mentioned a case where we received requests under FOI from the Norwegian access professional who was, at the time of his request, being tried in court in his country for espionage. This dramatically illustrates the point.

Senator NUNN. Is there any other country in the world that has this same kind of law, that foreign citizens are entitled to request information? Could you, as a U.S. citizen, request information in Britain and be entitled to it?

Mr. VAN COOK. I would expect not, sir. In Britain, they have an Official Secrets Act. The information, official information, in government records is the property of the Crown. In our country, our Government records are the property of the people, the public. We are just protecting those records for the people.

Senator NUNN. There presumably would be the people of this country, not the people of the Soviet Union?

Mr. VAN COOK. That is correct, people of this country.

Senator NUNN. Have you ever heard an argument that would have the logic to it that the President of the Soviet Union or the ayatollah in Iran, or Qadhafi in Libya ought to have access to information under the Freedom of Information Act, does anybody have an argument that that is necessary to protect our own right to know in this country?

Mr. VAN COOK. No, sir, I have never heard such an argument.

Senator NUNN. If you hear it, let me know. I am really curious about what the argument would be.

Mr. VAN COOK. I share your curiosity, sir.

The Soviets view the United States and several other Western countries as a continuing source of important and openly available scientific and technical information. In some cases, according to an unclassified CIA report, their acquisitions satisfy deficiencies in Soviet technology such as smart weapons, electro-optical and signal and information processing technology for Soviet air defense systems. Also, the Soviets appear to have concentrated their tactical systems acquisitions on Western tank, antitank, and air defense related technology to benefit their weapons programs and to design countermeasures to Western systems.

Even with classification there have been instances of difficulty caused by judicial review of such determinations pursuant to FOIA litigation. A requester sought access to records entitled "Technical Abstract Bulletin" [TAB] indexes produced by the Defense Technical Information Center. The TAB is a bibliographical reference document that indexes technical reports prepared for the Department of Defense. It was an entity classified confidential. Most of the reports indexed in the TAB were unclassified and although some of the reports indexed in the TAB were in themselves classified, their titles had been rewritten so that each title was unclassified. The basis for its overall classifica-

tion of confidential was that the compilation of research and development information contained in and revealed by the TAB index would allow a foreign nation to develop, improve or refine similar items of war potential, or would provide such a nation with a base upon which to develop effective countermeasures or weaken or nullify the effectiveness of a defense plan, project or system which is vital to the national security.

The court ruling in this so-called Florence case did not even reach to the question of whether the documents were in fact properly classified, and thus not subject to disclosure. In the court's opinion, other provisions of the FOIA were overriding. The FOIA stipulates that: "Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt." The effect of the court's opinion and its order to release the segregable portions resulted, in this instance, in the release of the entire document.

In 1980, Senator Sasser brought into focus the problem of unlimited dissemination by making inquiries into the international exchange program. It was discovered that a large number of unclassified U.S. Government publications were being automatically distributed to foreign governments such as the Soviet Union, Cuba, and Iran under this exchange program. A large portion of these documents were defense-originated publications including field manuals and technical manuals developed for the use of the Armed Forces.

The international exchange program is under the direction of the Library of Congress, and the distribution of these unclassified documents is made pursuant to law and in accordance with some 55 bilateral agreements negotiated by the Department of State and foreign governments. The laws governing the supply of U.S. official publications for international exchange are section 1718 of title 44 of the United States Code, "Distribution of Government Publications to the Library of Congress," and section 1719 of title 44, "International Exchange of Government Publications."

The intent of this legislative policy is to make the widest range of U.S. official publications available for exchange. The only documents considered in this process are those published by the Government Printing Office, and the publications made available for the exchange program are generally identical to those that are made available to designated public and academic libraries in the United States under the depository library program established by section 1902 of tit[illegible] 4.

The trend toward openness in Government has run virtually uninterrupted for the past 30 years. It is a trend that the Department of Defense certainly has supported over those years. It has long been the Department's policy not to constrain information the public requires to be informed sufficiently about the activities and operating functions of the Department. We were concerned, however, that there appeared to be no compelling reason for permitting Government publications that are required solely for official use or for strictly administrative or operational purposes to be freely transferable to all countries participating in the exchange program even though the publications were not classified for reasons of national security.

Therefore, the military departments and defense agencies were asked to revise their policies and procedures with respect to the ap-

proval and issuance of unclassified field manuals, technical manuals and other publications containing valuable technical data to assure that these publications required solely for official use or for strictly administrative or operational purposes were clearly identified. Further, the Library of Congress and the Government Printing Office agreed not to include defense documents so identified in the international exchange program. Our aim was not to exclude all defense documents from the program but to provide more positive control over a certain class of such documents. This we did.

Senator NUNN. You are really saying that you took these documents out of the circulation list that were automatically sent abroad; is that right?

Mr. VAN COOK. By identifying those documents as those which had technical data and operational data for the use of the Armed Forces, by identifying them with a notation, the effect of it was that we did take them out of the exchange program.

Senator NUNN. But that doesn't mean they aren't obtainable under other methods?

Mr. VAN COOK. They could be reached under the Freedom of Information Act for example, yes, sir.

Not satisfied that we had done all we can within the Department to limit the availability of such unclassified information, General Stilwell, Deputy Under Secretary of Defense (Policy), established a DOD working group on technology transfer. This group which I was asked to chair, was directed to address: (1) what the Department of Defense can do now to effect more positive control of such defense information, (2) what Department policies and procedures ought to be changed to effect more positive control, and (3) what can we ask others outside the Department to do to assist in these efforts.

The issues involved in such an undertaking are not unfamiliar and center around the countervailing principles of openness in Government and the Government's legitimate need to protect from disclosure certain information in the interest of national security. What we are seeking is a more equitable balance between the need to protect certain information and the competing need to keep the public properly informed about the activities of its Government.

One of the initiatives that has emerged as a result of the technology transfer working group was a proposal to authorize the Secretary of Defense, by Executive order, to classify at a level lower than confidential, defense information the unauthorized disclosure of which could reasonably be expected to be prejudicial to the national security because it would result in the loss to the United States of a military, technological, or operational advantage. This proposal did not receive broad executive branch support, however, and has been abandoned.

Another initiative appears in the defense legislative proposal to amend the Freedom of Information Act where it has been recommended to exempt from disclosure technical data that may not be exported lawfully outside the United States without an approval, authorization, or a license under Federal export laws. This recommendation is now a part of the administration's proposal to amend the act.

Senator NUNN. Are you saying that under the existing law and interpretations that something under the Export Administration Act has to have a license and approval from the Commerce Department

95-929 O - 82 - 13

or otherwise it can't go out of the country, would be obtainable, the same information would be obtainable under the Freedom of Information Act?

Mr. VAN COOK. Yes. That is entirely possible.

Senator NUNN. I don't understand that. I don't understand how we get to that spot.

Mr. VAN COOK. Under the Freedom of Information Act, there is no exemption that deals with technical information. There is an exemption, the third exemption, under the Freedom of Information Act which provides that information can be withheld from public release because it is exempt from disclosure by statute. So if something is subject to export control laws under the Munitions Act or under the Export Administration Act, I would think that could be withheld under the B(3) exemption under the Freedom of Information Act. But there may be certain elements of information not clearly covered by statute that might be released under the Freedom of Information Act. I say it is probable, possible.

Senator NUNN. You are saying that if someone were careful in applying that exemption that relates to the statutory restrictions that the Freedom of Information Act could not reach that material?

Mr. VAN COOK. That is correct.

Senator NUNN. You are saying it needs to be clarified?

Mr. VAN COOK. I think it needs to be clarified.

Further internal proposals to provide more positive control of this type of information that is allowable under existing policies and procedures are being developed, but it would be premature to discuss them at this time since they have not yet been fully considered by the Department.

Thus far I have been dealing with the problem of technology transfer from an information security perspective. However, in 1978, in addition to my responsibilities as Director, Information Security for the Department of Defense, I also became responsible for the implementation of the national disclosure policy. I should like now to discuss technology transfer from my other perspective, that of the chairman of the National Disclosure Policy Committee.

Under the basic national disclosure policy issued in 1971 by the National Security Council, with Presidential approval and each subsequent President's reaffirmation, the Secretaries of State and Defense are jointly responsible for controlling the dissemination of classified military information to foreign governments. The interdepartmental committee which I chair was established to implement the national disclosure policy and includes representatives of the Central Intelligence and Defense Intelligence Agencies, the Department of State, the Organization of the Joint Chiefs of Staff, and the three military departments.

The most important aspect of the national disclosure policy is the realization that classified military information is a national asset, an asset that must be conserved and protected. In determining whether classified military information, including technology, will be provided to a foreign government five policy objectives or criteria must be considered. The first is that the disclosure must be consistent with the U.S. foreign policy toward the recipient nation. The second ob-

jective is that the disclosure must not seriously jeopardize U.S. national security.

Third is the assessment of the foreign recipient's ability to protect the information as we protect it. Fourth is whether the information to be provided is sufficiently limited to only that which is necessary to accomplish the purpose of disclosure. And finally, the benefits to the United States must be at least equivalent to the value of the information disclosed.

Each year there are approximately 10,000 disclosure decisions made in the Department. Obviously the National Disclosure Policy Committee itself cannot handle this volume. Consequently disclosure authority is delegated to principal Department of Defense officials as the Secretaries of the military departments, the Chairman of the Joint Chiefs of Staff, the Director, Defense Intelligence Agency and a few others.

These are, in turn, authorized to redelegate this authority to the levels that they believe are necessary to meet operational requirements. People authorized to make decisions with respect to the release of classified military information to foreign governments are guided in their decisions by the National Disclosure Policy Document issued by the Secretary of Defense. This document lays out in clear terms the criteria for disclosure which must be met and specifies the levels of eligibility for each country with whom we exchange classified military information.

In those cases where the criteria cannot be met for one reason or another or the information to be disclosed exceeds the level of eligibility for the country concerned, an exception to the national disclosure policy must be considered before the disclosure is authorized. The role of the National Disclosure Policy Committee is to consider and act upon any request for exception to policy.

To assist in keeping track of the Department's disclosure decisions we have an automated data system called the Foreign Disclosure Automated Data System or Fordad.

Four types of data are recorded in the Fordad system:

1. All delegated disclosure decisions of documentary information or material that are normally made within the guidelines for the national disclosure policy.
2. All decisions on requests for exceptions to policy initiated because the disclosure falls outside the normal guidelines for disclosure.
3. All disclosures involving top secret information.
4. All DOD decisions on munitions license applications.

This data base is used on a routine basis to provide decisionmakers with the background of previous, similar cases by weapon or country. However, in a 1979 study, we found that this system had significant problems of completeness, timeliness, quality, and accessibility. In May 1979, the Deputy Secretary of Defense tasked the military departments and other agencies to assist the Deputy Under Secretary of Defense (Policy) (my boss) in improving the system. We then initiated a project to develop the Foreign Disclosure and Technical Information System (Fordtis). The objective of Fordtis is to assist the U.S. Government in meeting its national security responsibilities in the disclosure of classified military information, import and export

control, international armament cooperation, and assessment of U.S. technology posture.

Analysis has shown that automation can be effectively applied to the caseworking process by providing caseworkers a common frame of reference within which to make decisions. We found that the system must include foreign military sales and munition licenses to give a complete picture of munitions leaving this country. We also found that commercial commodity licenses sent to DOD by the Department of Commerce and Cocom cases sent to DOD by the Department of State must be included in order to make rational decisions on the export of militariiy critical technologies.

In addition to these historical files, the caseworkers need reference information such as the militarily critical technologies list, country assessments, and weapon systems reference lists. Fordtis will contain this information and will interface with the Department of State systems and one Department of Commerce system.

We expect an initial operating capability this month with a full operating capability supporting a network of users 1 year later. We anticipate that Fordtis will reduce staffing of routine cases and allow more time for precedent-setting critical cases. Fordtis will allow the U.S. Government an unprecedented capability to control the export of information, munitions, and technology.

Mr. Chairman, this concludes my prepared statement. I shall be happy to respond to any questions you or your subcommittee may have at this time.

Senator NUNN. Thank you very much, Mr. Van Cook.

We appreciate your excellent statement. Because of the Soviets' activities in Afghanistan the United States will not allow the Soviets to obtain information from the Technical Information Service. Does this mean the Soviets really are locked out of this or can they find other ways to get to it?

Mr. VAN COOK. The Soviets directly are locked out of it but we expect that their surrogates are certainly providing the information to them and using the service.

Senator NUNN. Is this more of a symbolic act than it is something that can really be enforced?

Mr. VAN COOK. Yes, sir.

Senator NUNN. You mentioned the so-called "cottage industry" that has sprung up regarding the Freedom of Information Act. Would you tell us how you define a cottage industry? What do you mean by that?

Mr. VAN COOK. These are organizations that have been in the business of accessing Government records under the Freedom of Information Act, asking for a wide range of Government records, reproducing them, and selling them, here and abroad.

Senator NUNN. They are actually in the business?

Mr. VAN COOK. They are in the business, yes, brokers.

Senator NUNN. Do any of these so-called cottage industries have computerized operations that you know of?

Mr. VAN COOK. Yes. They do, sir.

Senator NUNN. Would you describe that?

Mr. VAN COOK. You know, in this age of microfiche and microforms and computers, the data bases are easily organized and they can be

accessed in minimum time, within a matter of minutes. So that these data bases are utilized by industry throughout the United States, certainly by these people, where they have a complete data base of all of that which they have obtained through their requests under the Freedom of Information Act.

I believe there is one outfit called INFODOC overseas that makes great use of these data bases. I have an example of some of their publications which I will be glad to provide for the subcommittee's review.

Senator NUNN. Do you regard our technology as a national asset as you do our military information?

Mr. VAN COOK. I believe that there should be no question in anyone's mind that the U.S. technology and technical know-how is the best in the world. It should be treated with a sense of worth. Yes, I believe it should be treated as a national asset.

Senator NUNN. Regarding the Freedom of Information case in which an individual was able to obtain the technical abstract bulletins index, is this really an equivalent to a road map of U.S. technology, directions, capabilities, advancements, and future intentions?

Mr. VAN COOK. Yes. In that particular case, Senator, we classified the document, the total document, the index on the basis that it would give an indication of our level of effort because it did outline in some detail, although each entry being unclassified, the subject matter that was in existence. So the compilation we felt revealed a level of effort and classified on that basis. The court made a decision that it did not need to reach to the validity of the classification but merely get to that portion of the Freedom of Information Act which says that the requestor is entitled to the unclassified segregable portions and the court ordered that he be provided with all of the unclassified entries. Consequently, we provided him with the document.

Since, based on that court decision, we have since declassified that document. It is no longer a classified document. So it is available.

Senator NUNN. So that was the combination of the Freedom of Information Act plus the court decision?

Mr. VAN COOK. That is correct, sir.

Senator NUNN. Is this administration going to have any recommendations on the Freedom of Information Act?

Mr. VAN COOK. Yes. There is a legislative package in the Congress at this time.

Senator NUNN. Now pending?

Mr. VAN COOK. Now pending, yes.

Senator NUNN. Does that cover any of these areas we have talked about? Does it cover the access by foreign citizens?

Mr. VAN COOK. My understanding is that it is in that package. Yes, sir.

Senator NUNN. Could you furnish that package to us for the record? We can get it?

Mr. VAN COOK. I will be glad to.

[The material referred to was marked as "Exhibit No. 32," for reference, and may be found in the files of the subcommittee.]

Senator NUNN. Has the Department of Defense participated in that?

Mr. VAN COOK. Yes.

Senator NUNN. Do you think this package does plug up most of the loopholes that you are dealing with?

Mr. VAN COOK. The one that we are principally concerned with now and which we are addressing today, technology transfer, we think it would go a long way if under the Freedom of Information Act we would have the authority to withhold that type of information. I think it would help considerably, sir.

Senator NUNN. What about the index of military specifications? Is that currently available under the Freedom of Information Act?

Mr. VAN COOK. Yes. The index of military specifications and standards is a two-part document, alphabetical listing and numerical listing of our military specifications and standards. It is for sale by the Government Printing Office. By subscription, $40, I think, domestic and $50 foreign.

Senator NUNN. Is this something that should be classified?

Mr. VAN COOK. It is very difficult to classify this, Senator, to reach the damage criteria for one thing. For another thing, it sometimes is not practical to classify. Example, you might take a military standard and specification of a Jeep tire which is listed in this book and if you went to the classification route, the fellow who has to change tires would have a clearance, you know, you get into all of those safeguard rules and it is just impractical to do it.

Senator NUNN. So this is something no matter how we change the law, regulation, something like this is going to always be available. Right?

Mr. VAN COOK. Not a matter of how you change the law and regulations. I think if the laws were such that if we could withhold this information properly and use it for the people who need to use it, in the Department of Defense, in the Government in fact, possibly the contractors, that is what we are looking for.

Senator NUNN. Is there any kind of proposal by the administration that would allow you to do that?

Mr. VAN COOK. Yes. I think this amendment to the Freedom of Information Act would give us that license.

Senator NUNN. But I thought you were saying that this is a document that is printed by the U.S. Government Printing Office and can be subscribed to?

Mr. VAN COOK. Under the Freedom of Information Act, if we could withhold it, under a statute, under the Freedom of Information Act, for example, we would stop that, that would no longer be available for subscription.

Senator NUNN. One of the huge problems in classification is that the people at the top, or even the second echelon or third echelon, don't have time to go through all of these documents and classify. Consequently any comprehensive system of classification has people way down the line making those determinations. Is that correct?

Mr. VAN COOK. Sir, in the Department of Defense we make very extensive use of what we call security classification guides, so the people down the line that you are speaking of work under these guides. They don't make original classification decisions, nor do they have to. They merely need to determine that the information they are dealing with fits this guidance and they mark it as the original classifier

wants it marked. We have over 1,200 such guides in the Department of Defense covering classified programs, projects, plans and systems.

Senator NUNN. We thank you very much for your cooperation and your testimony. We want to stay in touch with you as we begin to make suggestions in these areas.

Mr. VAN COOK. Thank you, Senator.

Before I go I would like to say I have 39 years in the Government service and I have dealt with many of the committees, both in the House and the Senate side. But I just want to say that the cooperation that was extended and the courtesies that were extended to us by the staff people on this subcommittee was above and beyond. I think they are truly professional and specifically Mr. Fry of your staff, Mr. Asselin who dealt with us on the preliminary inquiries, were completely cooperative and the Department expresses its appreciation to the subcommittee for that.

Senator NUNN. Thank you very much. We appreciate that. I know the staff appreciates that. I agree with your evaluation of them and I am delighted that they were received that way in the Department of Defense. We hope to have some constructive recommendations and we certainly have benefited very much from your input.

Mr. VAN COOK. Thank you, sir.

Senator NUNN. Our next witness is Mr. William Von Raab, Commissioner, U.S. Customs Service. I believe Mr. Von Raab is going to be accompanied by Mr. George Corcoran, Assistant Commissioner—border operations—U.S. Customs Service.

Mr. VON RAAB. That is correct. One other individual possibly. We have some charts.

Senator NUNN. That will be fine. If the people who are going to testify, if you could introduce them for the record, then we will ask all of them to be sworn in.

Mr. VON RAAB. George Corcoran is at my right, Assistant Commissioner for border operations; Pat O'Brien, who is our Director of General Investigations under which most of these activities take place. They may be asked a question.

Senator NUNN. If you will all hold up your right hand, do you swear the testimony you will give before this subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. VON RAAB. I do.

Mr. CORCORAN. I do.

Mr. O'BRIEN. I do.

TESTIMONY OF WILLIAM VON RAAB, COMMISSIONER, U.S. CUSTOMS SERVICE, ACCOMPANIED BY GEORGE G. CORCORAN, ASSISTANCE COMMISSIONER—BORDER OPERATIONS—U.S. CUSTOMS SERVICE; AND, PATRICK O'BRIEN, DIRECTOR, GENERAL INVESTIGATIONS, U.S. CUSTOMS SERVICE

Mr. VON RAAB. I brought a few charts here which might make my presentation a little clearer, if it is all right with you.

Senator NUNN. That will be fine.

Go right ahead.

Mr. VON RAAB. Let's make sure that the Senator can see them over there.

Senator, I appreciate this opportunity to discuss with you the problem of Soviet acquisitions of critical technology. Since you are all well aware of the magnitude and seriousness of the matter, I will take this opportunity not to discuss the critical technology issue but rather what the Reagan administration and Customs is doing to address it.

Historically, the Customs Service has played a role in export control enforcement since the birth of our Nation. In 1793, President Washington, in order to avert American involvement in the French Revolutionary Wars, issued the first proclamation of U.S. neutrality and directed enforcement by officers of the Customs Service.

Since that time, numerous proclamations and statutes have been promulgated involving neutrality and other areas of export control. Some of these enactments were for specific political or policy purposes, such as bans on the export of critical technology to the Soviet Union and others were for general purposes such as the licensing of all munitions for export whatever their destination. Regardless of their nature, Customs has always played a principal role in the enforcement of these provisions.

Until 1973, Customs investigations regarding illicit exports were mostly reactive and centered around various exile groups in the United States, who, at times, would try to organize expeditions to invade their former homeland

Cases involving other areas of export control were almost nonexistent and, of the few that were conducted, most concerned the export of stolen articles or commercial goods. During the mid and late 1970's, more and more emphasis was placed on export control enforcement and several significant investigations were successfully culminated, including some cases involving the illicit transfer of critical technology. These critical technology cases have been provided to your staff in written summation.

Under the Reagan administration, a strong emphasis has been placed on thwarting the flow of high technology to the Soviet bloc and other unfriendly nations. In response to this mandate, I directed the U.S. Customs Service to launch new initiatives aimed at combating the trafficking in illegal exports.

The result of these efforts is called by us in Customs Operation Exodus, a national enforcement program which integrates the various operational units of the U.S. Customs Service. The program has three distinct objectives, each of which is essential to the national interest.

The first objective is to halt, to the maximum extent possible, the illicit flow of critical technology to the Soviet bloc and other unfriendly nations. By critical technology, we in Customs means those items which represent technological advances to the Soviet bloc whether they be revolutionary or merely evolutionary in nature. This, of course, is necessary if we are to regain and retain military parity with the Soviet Union.

The second objective is to disrupt the flow of high technology to the Soviet Union. By high technology, we mean those items which the Soviet Union can manufacture themselves but choose to acquire from the United States in order to reduce costs and improve quality. By intercepting such shipments, the Customs Service can significantly disrupt the Soviet military complex.

The Soviets will eventually be required to produce their own high technology rather than relying on ours and will thereby be forced to divert resources from other military areas.

The full significance of this becomes apparent when one realizes that the Soviet Union does not have the massive civilian market for this technology and must absorb the entire cost of building and operating manufacturing facilities without being able to offset the expense through large-scale commercial sales.

The final goal of the program is to intercept shipments of other commodities which are being exported in violation of various sanctions and embargos, such as the present embargos against Cuba, and Libya, as well as the recent sanctions against Argentina. Effective and credible enforcement is essential if the sanctions are to achieve their desired end.

Operation Exodus is being coordinated from the national command center located at the Customs headquarters in Washington. The command center is staffed with special agents and intelligence analysts who coordinate the interdependent intelligence, inspection, and investigative activities both here and abroad. The effective correlation of these three disciplines has been one of the prime underlying factors contributing to the early success of Operation Exodus.

In our intelligence efforts, we have been very fortunate. We have found that most manufacturers and exporters are also importers amongst whom we have developed sources in relation to our import smuggling and fraud programs.

Likewise, the sources we have among shippers, brokers, and freight forwarders as well as our extensive network of contacts within the foreign Customs Services have all been very productive in the area of illegal technology transfer.

We have also done very well with U.S. Government agencies. Here, our reputation in investigating illegal exportations and the focus provided by Operation Exodus have combined to play a critical role in the administration's efforts to block the transfer of technology to the Soviet Union.

Due to the fine efforts of Assistant Secretary Lawrence Brady, we have been able to establish an analytical unit within the Department of Commerce. This unit which is headed by a special assistant to Mr. Brady and staffed by Customs and Commerce employees, has developed an innovative intelligence approach dependent upon the application of link-analysis techniques to the Department of Commerce license application files.

The analyses produced to date have been outstanding in identifying firms engaged in diverting critical technology to the Soviet Union and in pinpointing new diversion routes. This intelligence is being used in developing profiles for the Exodus inspection teams and as the basis for major criminal investigations into Soviet diversions.

The Department of State has given us extensive access to their files both in their Office of Munitions Control and their Office of East-West Trade, where the sheer volume of information available has required us to place a full-time analyst. We are also receiving maximum support from the U.S. intelligence services and the FBI who is providing intelligence and participating in joint investigations with us throughout the country.

Our inspectional activities are progressing equally as well. The Exodus teams are now operational throughout the Nation examining cargo at airports, seaports, and land borders. What they encounter most are fraudulent exportations. That is goods being misdescribed to lead the shipper and Customs officials to believe that they do not require a license; or goods being shipped under either a fictitious license or one that covers a different commodity or different destination.

When one of our inspection teams locates a suspicious shipment they contact the command center to determine whether the shipment requires a license, whether any license associated with it is valid, and whether the firms or commodities involved are suspicious and should be monitored overseas for potential diversion.

In addition, to facilitate matters further, two special agents and two import specialists have been detailed to the Department of Commerce to assist in responding to licensing inquiries. This not only improves the efficiency of our operation but also minimizes delays of legitimate exportations.

The inspectional teams also on occasion encounter goods being clandestinely smuggled out of the country or being diverted to third countries, however, by and large, smuggling and diversions are detected only through good intelligence and thorough investigations.

The results of our Exodus inspections have been outstanding. The chart on display indicates the number of shipments being detained by our inspection teams since we established our Exodus Command Center.

These figures, we have found to be an accurate measurement of our field activity. You will notice the sharp increase in early February, this is when formal Exodus teams became operational.

The high level of activity in March, on the other hand, is the result of the President's Libyan embargo which became effective in stages between March 12 and March 28.

The next chart indicates the export seizures being made. The high number of seizures in March is again due to the Libyan sanctions. So far this fiscal year, we have made over 300 export seizures valued at more than $20 million. The more notable seizures have involved lasers, computers, and highly sophisticated military technology destined for the Soviet Union either directly or through other nations.

We have also made numerous seizures destined to Libya and other nations against which this Nation has imposed sanctions and embargos.

In just the last week, we seized a shipment of 32 military aircraft engines destined for Argentina and have also placed several shipments, including a high performance helicopter under detention.

As I previously stated, our most significant results can be expected in the area of investigations. The intelligence being provided by the CIA, FBI, and other Government agencies, both foreign and domestic, the information being provided by Commerce and gathered from our contacts in the import/export and shipping industry, again both here and abroad, and the leads being developed through the efforts of our inspectional teams have led to numerous significant investigations involving the diversion of technology to the Soviet Union and other commodities to Libya, Cuba and other sanctioned nations.

Our investigations are aimed at criminal prosecutions which we hope will provide an effective deterrent to those engaged in this illicit trade. The techniques we use, that is confidential sources, surveillances, data base analyses and foreign investigations are those that we have always used in smuggling and fraud investigations.

At this moment, we are conducting over 40 major criminal investigations involving illegal diversions and are monitoring several significant shipments abroad which we believe are intended for the Soviet bloc.

While I cannot publicly discuss the details of most of these investigations, I am free to discuss one of the more significant ones with you, due to the nature in which the investigation has progressed.

Early last month, the Custom attaché, Mexico City, acting upon information from a confidential source, located a multispectral scanner which had been smuggled out of the United States on a corporate jet belonging to a Los Angeles-based firm.

The scanner is designed for use by the military in tracking the movement of troops and supplies by airplane and satellite. It works by emitting infrared and thermal light waves that strike objects on the Earth and transmit electronic data to computer equipment at a ground station which converts the data into photographs.

Using false documentation describing the merchandise as photographic equipment from Panama, the violators booked the shipment to Zurich, Switzerland on KLM Airlines. A rapid investigation in Europe quickly determined that the consignee had only a mail drop in Switzerland and was actually located in East Germany.

Consequently, the Customs attaché in Mexico City determined that the shipment was placed on a flight that stopped in the United States enroute to Zurich.

When the plane landed in Houston, the cargo was off-loaded, seized by Customs agents and replaced with sandbags. The shipment was permitted then to proceed to Zurich via Amsterdam.

Two days later, special agents in Los Angeles executed a search warrant at the exporter's premises, and seized two sophisticated computers also destined to the same customer as well as documentation establishing the true destination as Moscow. This investigation and many others equally important, are being pursued this very moment by Customs special agents.

Consequently, from an almost nonexistent and purely reactive Federal export control program focusing on illegal arms exports; Customs, with the support, cooperation, and encouragement of the entire export control enforcement and intelligence communities, has successfully launched a major initiative to combat the illicit transfer of technology and other commodities to hostile nations.

We attribute this success to our unusual role in the international enforcement community. Our authority, structure, contacts, and experience in smuggling and fraud investigations have placed us in the position of being able to reach out and almost instantly provide to the Nation a capability which is sorely needed.

I believe that in the coming years, the U.S. Customs Service can continue to be very effective in addressing the problem at hand and disrupting, the Soviet acquisition attempts which the intelligence community has projected throughout the 1980's.

Thank you for this opportunity to describe briefly some of our efforts to stem the loss of critical and high technology and I would be happy to answer any questions as would Mr. Corcoran or Mr. O'Brien that you may wish to put to us.

Senator NUNN. Thank you, very much, Mr. Von Raab. Is the enforcement of the Export Administration Act a long-term priority of the Customs service? I gather from what you have said here today it is.

Mr. VON RAAB. Yes, sir.

Senator NUNN. Can you provide to the subcommittee an approximation of the amount of resources devoted to controlling the export of critical technology by the Customs service?

Mr. VON RAAB. At the present we have approximately 125 Customs inspectors, 50 special agents, and 25 support personnel, who are assigned exclusively to Operation Exodus. We are also drawing upon on a regular basis the daily responsibilites of almost 4,000 other Customs inspectors, and just under 600 other agents where and when the need arises.

Senator NUNN. Plus all your people out there in the field, I guess, are theoretically available when the need arises?

Mr. VON RAAB. That is about all our people. I would say as far as our inspectors and agents are concerned, there is not a single one of them who has not spent a fair amount of time, if not just being trained in Operation Exodus, having some personal experience with that.

Senator NUNN. To what extent does Customs have liaison with the Department of Defense in this technology area?

Mr. VON RAAB. We have a number of contacts with the Department. We have individuals who are identified to work with the Department of Defense. We have excellent liaison with the Department of Defense.

Senator NUNN. Where do you go for your expert technical opinions when you run across a technology case?

Mr. VON RAAB. If we can't answer it ourselves—we are getting better at doing that—we then make an inquiry of the Commerce Department and we consult with them over the telephone if we can handle it that way. If not, we will go into it in more detail in person or bring a sample or documentation with us. Therefore, we receive the ultimate technological support from the Commerce Department.

Senator NUNN. You say that you have assigned certain personnel from Customs to the Commerce Department?

Mr. VON RAAB. Yes.

Senator NUNN. How many?

Mr. VON RAAB. Seven.

Senator NUNN. What is the reason for that? What do they do?

Mr. VON RAAB. The reason is simply to merge where possible our expertise and theirs. We are experts on the way cargo is passed across borders. They are experts on the particular requirements involved in licensing of particular matter. We are often faced with a question of whether something needs a license at the border.

It is easier for us to have people in the Commerce Department who can deal directly with the Commerce experts and to be able to ask them those questions.

It saves us time and energy and we get better answers as a result.

Senator NUNN. Mr. Von Raab, if you were given total responsibility under the law, to enforce the violations of the Export Administration Act, would Customs be able to carry out that mission in your view?

Mr. VON RAAB. Yes; we would. We would continue however to rely heavily on Commerce's expertise to provide us with assistance.

Senator NUNN. In terms of what expertise that they have?

Mr. VON RAAB. They make the decisions as to whether something should be licensed.

Senator NUNN. If they were doing the licensing that would be where you would get your information as far as what should be enforced?

Mr. VON RAAB. Yes; often we are asking the question of ours at the border as to whether something requires a license. Often, it is a difficult question. Therefore we do rely on them.

Senator NUNN. Would the Customs Service have to employ additional people in order to handle the enforcement part of the Export Administration Act?

Mr. VON RAAB. As I indicated, we have exactly what the numbers were, but between 200 and 300 individuals already assigned directly to that with the ability to call on the rest of our forces. We would not need to hire additional individuals because I don't believe that Commerce really has more than 20 or so that would have to be replaced.

Senator NUNN. Do you think it is possible for the Commerce Department to have a viable export control program in terms of enforcement with 8 to 12 investigators and 5 inspectors in the compliance division?

Mr. VON RAAB. No, sir. Obviously, those numbers are much too low for a reliable enforcement effort. I would say, however, that those individuals do make an important contribution to the enforcement effort.

Senator NUNN. How can Customs insure that violators of the Export Administration Act will adhere to the administrative sanctions such as denial of export privileges?

Mr. VON RAAB. The way—I don't fully understand you.

Senator NUNN. Let's assume you took over the enforcement end. How would you insure that when there is a violation that the administrative sanctions can be administered? Would that be a Commerce function?

Mr. VON RAAB. We would refer that to Commerce.

Senator NUNN. Commerce would handle that end of it?

Mr. VON RAAB. Yes, sir.

Senator NUNN. Could you in Customs, if you were required to by law, assume the administration of the Export Administration Act such as conducting licensing operations in adjudication of noncriminal violation? Would that be something you could also undertake?

Mr. VON RAAB. I would not like to ever say that the Customs Service is not capable of doing anything, but I think it is reasonable to say that that activity certainly fits much better into Commerce with its close association with the business community.

Senator NUNN. If there was a determination to give you jurisdiction over the enforcement end of the Export Administration Act, you think it makes sense to continue to have the licensing in the Commerce Department?

Mr. VON RAAB. Yes, sir.

Senator NUNN. We understand that in the CTC case that West Germany cooperated and that was facilitated through the establishment of

a working agreement between the U.S. Customs attaché in Bonn and West German Customs; is there as specific agreement on that?

Mr. VON RAAB. On the case? We have mutual assistance agreements with Canada, France, Austria, Mexico, and West Germany; I think that is it.

There are five. There are five specific mutual assistance agreements that the Customs Service does have with the proper agency or government of five other countries. I don't know if I gave you five or not. But there are five.

Senator NUNN. You have the authority under the law in certain cases to make arrests without warrants; do you not?

Mr. VON RAAB. Yes, sir.

Senator NUNN. What kind of cases do you have that authority in?

Mr. VON RAAB. Those are typically border searches, mostly on incoming border searches.

Senator NUNN. Incoming?

Mr. VON RAAB. Yes, sir.

Senator NUNN. Do you have any authority on outgoing?

Mr. VON RAAB. We have no specific statutory authority on outgoing. However, we have received a succession of favorable cases implying that we have very, very strong authority in that are under State statutes or under, in some cases, posse comitatus.

Senator NUNN. How about large amounts of cash being taken out of the country? Is that something that you can make an arrest in when it violates the law without a warrant?

Mr. VON RAAB. We require probable cause in the case of currency seizures.

Senator NUNN. But you don't have to have a warrant?

Mr. VON RAAB. Only on search, not on the arrest.

Senator NUNN. What about the export control cases? Do you have authority to make arrests without warrants in these cases?

Mr. O'BRIEN. I am Pat O'Brien, Director of General Investigations with the Customs Service.

While not having needed explicit search or arrest authority we have done very well in the courts and they have ruled that we have implied authority to conduct the searches and the arrests.

The difference in the currency area is that the currency statute itself says that searches will be conducted pursuant to a warrant based upon probable cause.

So, the currency statute actually limited our authority beyond what we had prior to the statute.

Senator NUNN. Do you need authority under the law to conduct searches of persons leaving the country as well as coming into the country?

Mr. VON RAAB. We have implied authority to conduct searches of those individuals.

Senator NUNN. So you don't need any changes in the law in that regard?

Mr. VON RAAB. Of course we would prefer to have wherever explicit statutory authority to conduct those searches. We have been successful, however, in receiving as Mr. O'Brien indicated, very good and supportive decisions based upon our implied authority.

We would certainly like to have the issue of the currency seizure cleared up and we would like to have the level required to reduce the suspicion as it is in most others.

Senator NUNN. Is there a pending bill on that? I thought Senator Proxmire had a bill on that; do you know?

Mr. CORCORAN. Yes, there is a bill on the arrest authority, but not on the search and seizure.

Mr. VON RAAB. The Treasury is preparing some legislation and I would expect that if we can move it through OMB, we will probably make it up here at some point.

Senator NUNN. We understand that Customs has experienced difficulty in receiving information due to a restricted interpretation of section 12(c) of the Export Administration Act by the Department of Commerce.

Could you tell us what——

Mr. VON RAAB. In the past, Customs Service has had some problems receiving information from the Commerce Department. However, a recent decision by the Secretary made, I believe, some time during March has opened up our access to the files with respect to specific cases that we may be working on. So Commerce has shown a tremendous amount of increased cooperation, I believe largely through the intercession of the Assistant Secretary Brady, who has been working very hard to improve our working relationship.

Senator NUNN. Are you familiar with the *Richard Mueller* case and the *Volker Nast* case?

Both of those cases, I think, were made by Customs? The *II Industries* case?

Mr. CORCORAN. Yes.

Senator NUNN. We understand that both of these men were indicted and are now in West Germany; is that right?

Mr. CORCORAN. They have both been indicted and that is right, two of the individuals are in West Germany. This was one case we jointly worked with the Commerce Department.

Senator NUNN. Was this a violation of the Export Administration Act?

Mr. CORCORAN. Yes, they were indicted for the violation of the Export Administration Act and found guilty of exporting semiconductor manufacturing equipment.

Senator NUNN. Who was found guilty?

Mr. CORCORAN. Three individuals and the company in southern California, II Industries.

Senator NUNN. Are these extradictable offenses under the Export Administration Act?

Mr. CORCORAN. They are not for American citizens.

Senator NUNN. How about foreign people?

Mr. CORCORAN. I don't think so, sir. I would have to check.

Senator NUNN. Could you furnish something in the record on that?

Mr. CORCORAN. Yes.

Senator NUNN. Particularly these two cases.

Mr. CORCORAN. The company was fined $10,000 and the three individuals were fined $25 000 apiece in addition to being found guilty.

[The information follows:]

Violations of the Export Administration Act and the Arms Export Control Act are not extradictable offenses.

Senator NUNN. Mr. Von Raab, we understand that customs has experienced certain difficulties with the Commerce Department in criminal investigations. These difficulties were outlined in an October 30, 1980, memo from William Green, Deputy Assistant Commissioner of the Office of Border Operations. That was to Mr. Robert Keuch, who is the Associate Deputy Attorney General and Chairman of the Interagency Group on Export Control.

This is the memo that we have on that subject and I quote from it:

> What is particularly significant is Commerce's OEA CD continued action to impede cooperation and investigation even while it states that it wishes to fully participate in all cooperative ventures.
>
> Commerce continues to take unilateral and uncoordinated action concerning either joint or Customs initiated investigations by requesting foreign inquiries through various U.S. embassies and consulates without consulting with either Customs attachés or headquarters. Such action is causing serious problems.
>
> These problems are not limited to hampering instant investigations but also compromising the U.S. Customs foreign government sources, damaging the previously close and long relationship between the United States Customs Service and their foreign counterparts and directly impacting on national security.

Senator NUNN. This memo is October 30, 1980. Have you seen that memo?

Mr. VON RAAB. No, sir. I have not. But I have spent a lot of time discussing the problems that have existed in the past between the Customs Service and the Department of Commerce, both with the individuals at Customs who are responsible and also with the number of officials at Commerce.

As I indicated, Assistant Secretary Brady and I have taken this as a personal campaign to improve the cooperation of the two services and particularly to improve the Commerce Department with respect to our activities.

I believe that he has made a number of changes within the Commerce Department. He is trying very hard. It takes a long time to turn around a bureaucracy like the Commerce Department. I, fortunately, am lucky enough to have an enforcement organization of extremely responsive and extremely dedicated individuals and therefore we have been able to respond to Exodus very quickly.

But I would like to indicate that the environment between Commerce and the Customs Service has improved immeasurably. And I have great hopes for the developing relationship.

With respect to foreign investigations, I do believe that there are problems with Commerce conducting certain foreign investigations.

Customs does have much better connections with the police agencies that these investigations would typically use.

Unfortunately, Commerce is burdened with a number of other responsibilities that other nations find offensive, particularly antitrust, some antitrust investigations but more particularly some of our antiboycott as a result of which it is very difficult for a Customs or for Commerce officials to work effectively with police agencies and in other parts of the world where they fear that the Commerce officials are not only interested in stemming the flow of critical technology which they regard as a legitimate exercise but they are also afraid that the Com-

merce officials may be visiting certain businesses for purposes of enforcing some of the U.S. laws that those countries do not like.

So it is a real problem for Commerce abroad in my opinion. Occasionally we stumble over each other but I think the bigger problem is that the police organizations don't like the Commerce attachés.

Senator NUNN. In your personal opinion, doesn't it make sense to shift the enforcement part of the Export Administration Act to the Customs Service leaving the licensing in the Commerce Department?

Mr. VON RAAB. We are already doing a large part of the enforcement. I don't know that it is necessary that only one agency have the total responsibility for enforcement.

Senator NUNN. If you were trying to devise an efficient method, though, you wouldn't split the same responsibility between two agencies, would you, one with an overwhelming capability and the other with very little capability at all?

Does that makes any sense at all from an administrative point of view?

Mr. VON RAAB. I unfortunately do not know enough about the universe of Commerce's responsibilities. I have to assume that there are certain aspects of investigations or enforcement that they do bring particular expertise to bear on. I certainly wouldn't suggest that they need to increase their forces in any way. But if I were Assistant Secretary Brady, I would hate to lose any power I had over enforcement because there are particular cases in which I feel that I might find it necessary.

Senator NUNN. You are not Assistant Secretary Brady. We will hear from him later. I am asking for your opinion.

Mr. VON RAAB. I have to agree with him on this. I think he will probably say that to you. I think we should carry the major share, the 95 percent, but I don't believe that it is necessary to snatch it totally from Commerce.

Senator NUNN. Would you see that there would be any damage done to our overall export capability in enforcing the law by putting it all into Customs?

Mr. VON RAAB. As I indicated before, I have great faith in Customs. So my answer to that would be, No, I don't see that it would cause a problem.

Senator NUNN. But because of your fondness for Mr. Brady and your sensitivity to the Commerce's Department's feelings in this subject, you would not advocate shifting?

Mr. VON RAAB. That is correct.

Senator NUNN. Is Mr. Corcoran free to give his opinion?

Mr. VON RAAB. Absolutely.

Senator NUNN. He can give his own personal view without being in any difficulty? Is that right?

Mr. VON RAAB. Yes, sir.

Senator NUNN. Mr. Corcoran——

Mr. VON RAAB. At least for now he is.

Senator NUNN. Do you think it makes sense, Mr. Corcoran, to have two different agencies responsible for enforcement under this?

Mr. CORCORAN. I think on the basis that you mentioned of effectiveness and efficiency it makes sense to have one agency when we are so predominantly involved.

S-929 O - 82 - 14

Senator NUNN. You think it makes sense to put it all in Customs?

Mr. CORCORAN. Yes.

Senator NUNN. Is Mr. O'Brien free to give his opinion?

Mr. VON RAAB. They are both free to.

Senator NUNN. For the time being?

Mr. VON RAAB They don't have control over this decision.

Senator NUNN. What is your personal view on that?

Mr. O'BRIEN. Being under oath, I must give my personal view.

I believe it can only improve the effectiveness and efficiency operations to centralize it.

Senator NUNN. Put it all under Customs?

Mr. O'BRIEN. Yes.

Senator NUNN. You don't believe it would damage our overall ability to enforce the Export Administration Act to take it out from under Commerce altogether except leaving the licensing there?

Mr. O'BRIEN. Absolutely.

Senator NUNN. Would you agree leaving the licensing there makes sense?

Mr. O'BRIEN. Yes; I think it is important to keep the administrative, especially the policy determinations separate from the enforcement function. They make their determinations based on national interest rather than enforcement.

Senator NUNN. I have a memo here the origin of which I will not give at the moment but it says:

> The Commerce Department has to wear two hats. On the one hand, it must serve the interest of the exporting community by assisting them in opening foreign markets, by advising them on proper procedures for exporting, by offering advice, making determinations concerning export licenses and in general assisting exporters.
>
> On the other hand, however, the Commerce Department must police the same group to ensure the laws and regulations have been complied with and take punitive action. This, of course causes a somewhat incongruous situation which can lead to conflicting internal policy and management decisions.
>
> Customs now enforces the Arms Export Control Act with the delegation of the Department of State and has done so for many years

and so forth.

Do you, Mr. Corcoran, agree with that?

Mr. CORCORAN. I think my feeling is that very much as Pat O'Brien just mentioned, I think that we as the enforcement agency should be the factfinding agency.

I do think that even though there seems to be a conflict there that Commerce should retain the licensing and administrative function. I think overall policy and considerations in the Commerce and the oversight of the movement of products in and out of the country——

Senator NUNN. Should retain the licensing function?

Mr. CORCORAN. Yes; I think they should retain that function and the policy and administrative actions involved in the licensing. I think we should be just a factfinding enforcement agency.

Senator NUNN. I think Mr. Von Raab, you mentioned in your statement that or in answer to the question that you didn't believe the Commerce Department couldn't really do the job with the number of people they have there now?

Mr. VON RAAB. The point I am trying to get across is I am not sure that to deprive Commerce, the ability to do any enforcement in this area is a good idea.

I say that only because we live with a similar problem with respect to drug investigations in which we are deprived by the Reorganization Act of 1972 from conducting drug investigations. DEA has that responsibility.

Senator NUNN. What I am puzzled about, I have been through all of that——

Mr. VON RAAB. Therefore I think it is a mistake to prohibit a department from conducting certain activities which are very closely related to other matters that it deals with. I am not suggesting in any way that Customs should not, in effect it is, but should not remain and grow as the primary if not almost total enforcement arm.

It makes me nervous to remove any enforcement authority from the Commerce Department. That is my concern.

Senator NUNN. But if you just remove the people, left the authority there, that would solve it, wouldn't it?

Mr. VON RAAB. You will get to it one way or the other.

Senator NUNN. What I am puzzled about is you don't believe they could properly enforce——

Mr. VON RAAB. Certainly not with that number of people.

Senator NUNN. But then you added you don't think they should increase the number of people.

Mr. VON RAAB. I don't think they need a large enforcement effort. I just think it is probably important for them——

Senator NUNN. What you are basically saying is we should leave some authority and maybe a few people in the Commerce Department for sensitivity and prestige purposes and then shift the main responsibility to the Customs Service?

Mr. VON RAAB. That is probably true.

Senator NUNN. I want to thank all of you for appearing, not only appearing here today, but also cooperating with us so well here in this whole investigation.

The staff has informed me of your excellent cooperation. We appreciate it. Mr. Von Raab, if you could reduce those charts to be this size so we could put them in the record, we would appreciate it.

Mr. VON RAAB. We have a few sets. We will send them up.

[The charts referred to follows:]

OPERATION EXODUS

TREASURY
U.S. CUSTOMS SERVICE

PROBLEM: FOREIGN ACQUISITIONS

- Critical Technology
- High Technology
- Other Commodities

OPERATION EXODUS

SOLUTION: OPERATION EXODUS

EXODUS Command Center

- Intelligence
- Inspections
- Investigations

INSPECTIONS

- Fraudulent Exports
- Smuggling
- Diversion

OPERATION EXODUS

INTELLIGENCE

- Manufacturers/Exporters
- Shippers/Brokers/Forwarders
- Foreign Customs Services
- Commerce/State
- U.S. Intelligence Services

OPERATION EXODUS

INVESTIGATIONS

- Criminal prosecutions
- Techniques – smuggling/fraud
  - Sources
  - Surveillances
  - Data base analyses
  - Foreign investigations

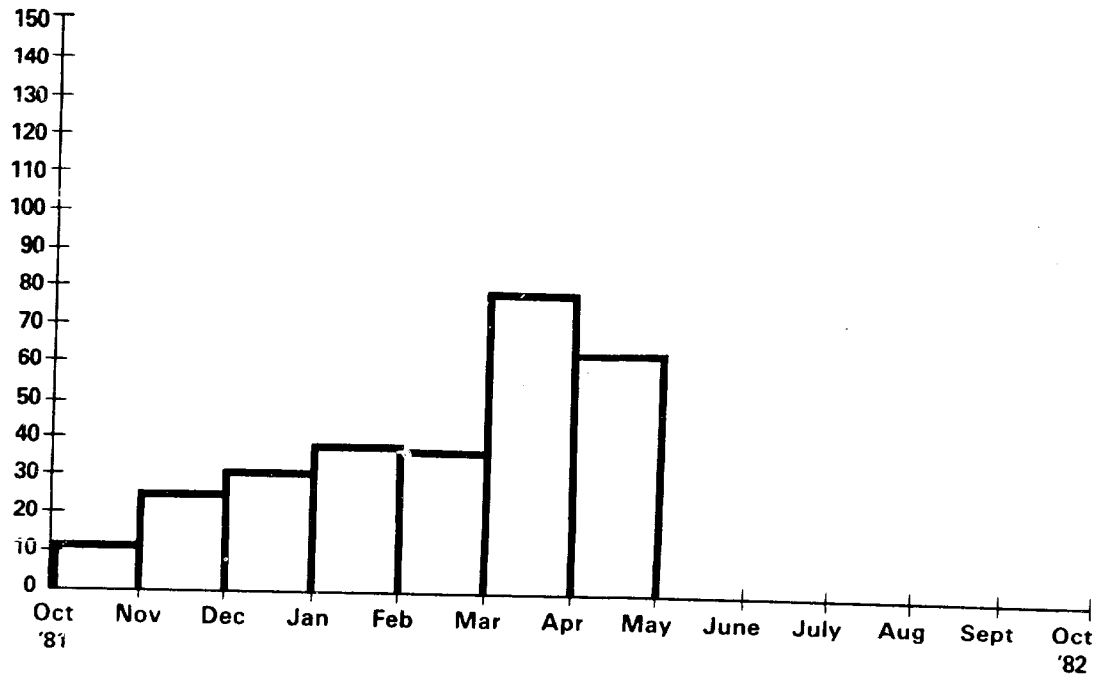
OPERATION EXODUS

CONCLUSION

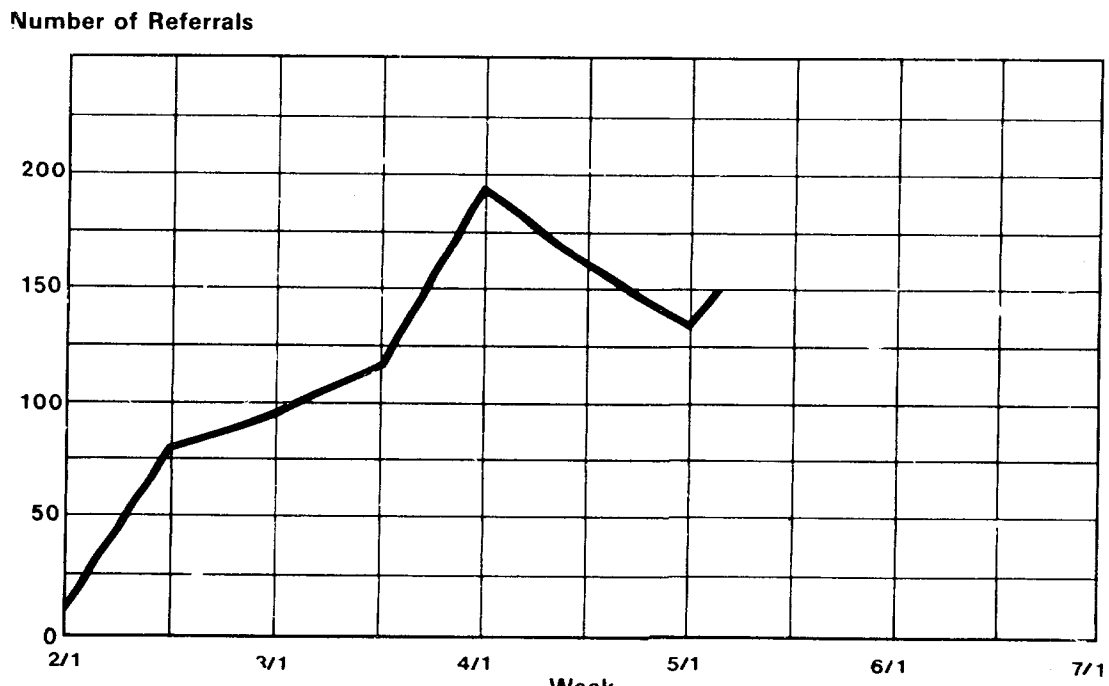
- Disrupt flow of critical tech
- Impede military buildup
- Burden military economy
- Enforce sanctions
- Deterrent/compliance

OPERATION [redacted] EXODUS

Number of Export Seizures
FY '82



Referrals to Exodus Command Center



Senator NUNN. Thank you, very much. The subcommittee will be back here at 9 o'clock Tuesday, at which time we will hear from Adm. Bobby R. Inman, Mr. Lorenzo, Deputy Under Secretary of Defense, and Mr. Bryen, Deputy Assistant Secretary of Defense, as well as Mr. Lecht, former chairman, president of the board, of Advanced Computer Techniques Corp.

[Member present at the time of recess: Senator Nunn.]

[Whereupon at 12:30 p.m., the subcommittee recessed, to reconvene 9:08 a.m., Tuesday, May 11, 1982.]

INTENTIONAL
BLANK

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

TUESDAY, MAY 11, 1982

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met at 9:08 a.m., in room 3302, Dirksen Senate Office Building, under authority of Senate Resolution 361, dated March 5, 1980, Hon. Sam Nunn presiding.

Members of the subcommittee present: Senator William V. Roth, Jr., Republican, Delaware; Senator Sam Nunn, Democrat, Georgia; and Senator Lawton Chiles, Democrat, Florida.

Members of the professional staff present: S. Cass Weiland, chief counsel; Michael C. Eberhardt, deputy chief counsel; Eleanore J. Hill, chief counsel to the minority; and Kathy Bidden, chief clerk; Gregory Baldwin, assistant counsel to minority; Jack Key, Glenn Fry, and Fred Asselin, staff investigators to the minority; and Kathleen Dias, executive secretary to the minority chief counsel.

[Members of the subcommittee present at convening: Senators Nunn and Chiles.]

Senator NUNN. The subcommittee will come to order.

Senator Roth is coming in a few minutes but has asked me to begin in his absence.

Our first witness this morning is Michael Lorenzo, Deputy Under Secretary of Defense, International Programs and Technology, Department of Defense.

Mr. Lorenzo, do you have some associates with you? If they are going to testify, I will ask all of you to take the oath.

Mr. LORENZO. I have a lot of supporters, Mr. Chairman.

Do you want them to take the oath? I don't know if I will call on them or not.

Senator NUNN. We can have them come up later, if you need them.

Do you swear the testimony you give before the subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. LORENZO. I do.

Senator NUNN. Mr. Lorenzo, we appreciate you being here this morning. We appreciate your cooperation with the subcommittee. You can introduce your associates and I will ask if either of you are going to testify, you go ahead and take the oath now.

Do you swear the testimony you give before the subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Dr. KAPPER. I do.

Dr. LOMACKY. I do.

Senator NUNN. We swear all our witnesses before the subcommittee without exceptions. It is a long tradition.

Mr. LORENZO. Nothing like starting with a common base line, Mr. Chairman.

Senator NUNN. That's right.

Mr. LORENZO. It is indeed a pleasure, Senator Nunn. I guess I have the go ahead, do I not?

Senator NUNN. Yes, sir, you go right ahead.

STATEMENT OF MICHAEL LORENZO, DEPUTY UNDER SECRETARY OF DEFENSE, INTERNATIONAL PROGRAMS AND TECHNOLOGY, DEPARTMENT OF DEFENSE, ACCOMPANIED BY DR. FRANK KAPPER, DIRECTOR OF MILITARY TECHNOLOGY SHARING AND DR. OLES LOMACKY, DIRECTOR OF THE OFFICE OF TECHNOLOGY TRADE

Mr. LORENZO. Mr. Chairman, in the interest of time, and I might say the thorough work we have done with your wonderful staff, Glenn Fry and others, and going over the issues, the substance, I would like to submit my prepared statement for the record as if I read it and make a brief opening statement to summarize the statement, and I would like to hit a few highlights and be prepared, perhaps, for some questions you may have.[1]

Senator NUNN. That will be fine.

Mr. LORENZO. I mentioned earlier, I have Dr. Frank Kapper here on my left. He is the Director of Military Technology. He handles munitions cases, FMS cases, MOU's, national disclosure policy, mainly what is known in the vernacular as West to West trade.

On my right is Dr. Lomacky. As you know, he has the very difficult and unpopular job of being in charge of dual-use technology transfer, which comes under the Export Administration Act of 1979 and which is the primary thrust of the hearings today, commonly known as East-West trade, which I think is a misnomer.

It is really West to East trade we are concerned about.

The statement goes into the defense roles and responsibilities, and accomplishments to date, of which there have been some. We would like more and are working hard with some of our concerns related to export control.

Limited by an unclassified hearing you have here, of course, we stand prepared to go into closed session in subsequent hearings, if you so desire, and, of course, classified sessions which you may desire to do to get down to a lot of the nitty gritty, et cetera.

I looked over and I have read the statements of a lot of my colleagues who have already testified before this subcommittee and some of them to follow.

Senator NUNN. Mr. Lorenzo, if you prefer to go through your whole statement, we would be delighted. It is not that long. I am sure that might be more comfortable for you. We have time this morning.

We will be delighted to hear all of it.

---

[1] See p. 552 for the prepared statement of Michael Lorenzo.

Mr. LORENZO. Rather than read word for word, I was going to hit the hightlights.

Senator NUNN. Whatever you prefer.

Mr. LORENZO. Really, we do two functions for the Under Secretary of Defense Research and Engineering, Dr. DeLauer.

One is the technical policy and the other one is technical assessment. This combined with strategic policy that is going to be covered by my successor, Dr. Bryen, generally constitutes the DOD decision or position that we go back to Commerce as our response to anybody's request for technology transfer.

Technical policy becomes very difficult, like policy in general, to define. We define it as pertinent to technical performance, operational parameters and the acquisitional aspects of technology transfer. Dr. DeLauer himself has established a new technical policy. Since we are both rather fresh and recent from the private sector, it goes like this. We have discovered and observed that on a case-by-case review basis, we do an excellent and outstanding job in turning down cases.

However, it is our opinion that we do not do a job commensurate with telling industry what they can do and can sell. We are working on that and will give you some examples later, if you so desire.

There are many, many cases.

Let me take one now. A CAT scanner which is headed for a hospital. Everybody wants to help a hospital. I think maybe Larry Brady uses this example, too.

I have a little different rationale than he does, but that is all right. The CAT scanner is going to be roughly a million-dollar piece of equipment. So that means a lot to the people manufacturing and selling. However, in that CAT scanner is imbedded a general purpose computer, an array processor, display and signal processing equipments both in hardware and software.

Obviously, the imbedded equipments only amount to around $35,000 to $40,000. However, they are accessible and normally through engineering practices they are readily accessible, to be used off-line for other things that we don't want them used for.

They are high powered computers. Well, first, the usual harangue and argumentation goes on. The case of course should be considered on its pure merits, that is whether it could contribute a significant enhancement to the military capability of a potential adversary, either the country receiving it or another country who gets it on a third party transfer.

In looking at this very deeply, we find out that we have not and really should use technology to help solve technology transfer leakage, or so-called hemorrhaging.

This we can do, and I am glad to report to you though with a humble and rather primitive beginning, that efforts are underway, because we do want to protect the trade, the economy of our country which, of course, we all know needs help now more than any other time and sell, but protect the critical technology so it cannot be used for off-line uses. And this we can do by changing the engineering design to make the software, you might say, difficult to reverse engineer, change the writing and change the mechanical accessibility. And so we would like to work with you in the months to come and

95-929 O - 82 - 15

I think we can make great strides in letting a lot of our advanced technology go out but it will not—in unmodified form—let's say modified form, I am sorry, be a contributor to the military enhancement of a potential adversary.

That, as you heard, is costing us a lot of money in defense today. The Soviets obviously have built up tremendously over the last 15 years with a lot of technology from our side and they depend on Western technology.

I think with approaches like this, as an example, we can at least make it very difficult for them and hopefully keep down the amount of defense money expended in countering their threat which is being built on Western technology to a great extent.

I might say in passing a very important message, I would like to leave with the subcommittee is that we are getting great cooperation from American industry. It is a good thing.

I will cite two examples. You take John Young, chief executive officer of Hewitt-Packard. We sat down with them in detail, also with Dr. Matt Sutton, Minneapolis Honeywell. They do not want to transfer their advanced critical technology to do anything conflicting with defense desires. We have to tell them what it is we want them to do and what they can do, instead of all this back and forth work we are going through now.

Of course, we are in the learning period of controlling critical technology and we will get there, I am sure.

Senator NUNN. Do you have a group of people under your jurisdiction who really sit down and conceptually with their scientific background and knowledge try to come up with a list of what the Soviets really need, what is critical to them in the defense arena, what kind of dual use technology they could employ in their defense efforts?

Mr. LORENZO. I think the answer to your question, Mr. Chairman, is essentially yes. A military critical technology list, which was called for in the Export Act, is a step in that direction. We have revised it twice and it is being revised again.

The first time it was aimed for products predominantly. As you know, the first submission was October 1, 1980, in accordance with the act.

The second round, we infused in that revision, you might say a Bucy report type of description. The end products themselves are not too bad because we give it to somebody who has to reverse engineer and that takes time.

However, in the Bucy report, and he was 10 years ahead of his time, he dealt with Keystone equipment, in other words, something that could be done to the design, production, and manufacturing process. Those are the kinds of technology that would hurt us most if it falls in the hands of an adversary.

I would say the military critical technology list is one step in that direction.

Senator NUNN. Does it cover dual use technology and commercial applications?

Mr. LORENZO. Primarily that is what it covers right now, dual use technology. As everybody knows on this subcommittee, that is technology and products predominately made for the civilian market, but

which have critical military applications. The majority examples are computers, including the software and that kind of product.

Senator NUNN. Do you ever get the feeling we are trying to control too much and by trying to control too much we aren't able to do a good job with controlling anything?

Mr. LORENZO. Personally, I think the answer to your question is yes. When I came from the private sector 7 months ago, I had the feeling we were unnecessarily controlling too much, like the CAT scanner I mentioned.

We get in an argument and say, yes, that imbedded computer is critical and could help, but let me go off on a little philosophy, and I am going to leave another paper and introduce it for the record which you can keep.[1]

Technology really is an international language. When you get all done, the physical scientific laws of nature were imbedded in all people, with all ethnic backgrounds, almost from the beginning of the Earth. Everybody knows what they are in every language. I go around the world, I talk to the Turks, I talk to the Japanese and when you start talking about such things as Carnot's laws of thermodynamics law, they all know what you are talking about "in English."

You do not, as you know, need an interpreter. Being a research technologist and working at the graduate level, I have no difficulty communicating. We have to understand that they all know the physical scientific laws of nature very well in every language and they know what the parameters are for key payoffs. What we fail to realize in this country is that if we can control and classify things to the ultimate, we can impede progress, but they will eventually know what we do. The classical example of that is nuclear energy.

That is enough motivation for them to know where to put their resources.

Yes, we can control critical technology, and I think we can identify such fairly well. However, the best control in the world is short-lived at best so we shouldn't use a lot of discretion on what we control because it goes contra to our economic development, open society, free trade understanding with foreign nations and also building up mutual respect with foreign nations to meet your military obligations.

The bottom line is this: If you buy everything said, and I think you do, I think you will also buy that the physical scientific laws of nature are in the hands of everybody and always will be. Of course, we being an open society, just by definition, our findings get in our research and development findings, particularly at universities where we share knowledge to help out the whole world. But we have bad people in the world here and there who use it for other things. We can and will control critical technology.

Let me come to the bottom line. There are two things we can do: One, we can be smarter as in the example of the CAT scanner I talked about—another is keeping our technology base out in front and ahead of everybody else and I think we are doing that very well in this country and spending approximately $20 billion in fiscal year 1982 R. & D. dollars—I won't get into exact numbers—just for other than research and development, or let's just say the technology base in DOD.

---

[1] See p. 562 for the material referred to by Mr. Lorenzo.

Being smarter, I think, is where we as a nation have failed in technology transfer, not doing things like I described, as in the CAT scanner.

Let's back off, and I am answering your question in the affirmative, yes, I think we sometimes, and this is a personal professional opinion of my own, are controlling things maybe too much. If we modify them slightly and make them inaccessible for uses we don't desire, I think we will go a lot further in obtaining our national goals and objectives.

I am sorry to give you such a long answer.

Senator NUNN. Is DOD the proper place to do that? Without any doubt, DOD ought to have a major input and, of course, I joined Senator Jackson in his efforts to give DOD much more input than they had formerly. But is DOD the place where you should get an objective technical analysis, let's call it a Soviet wish list, a list that we compose of what the Soviet Union really needs? Certainly DOD should have an input, but I wonder if DOD or State or Commerce, each with their own perspective, is the proper place for that kind of list to be found.

Mr. LORENZO. You pretty well answered all your questions, Mr. Chairman. DOD can give you the major, critical inputs for what the critical technologies are, what the Soviet Union needs for military use. But you have to remember of the total electronic capability in this country, DOD uses less than 5 percent.

So you will need somebody, some organization with a scope bigger than DOD to handle the total problem. I think you pretty well answered your own question by the way you stated it. I am in agreement.

Senator NUNN. Theoretically the final decision will be made at the White House on any dispute, but as a practical matter dealing with thousands of different items, where should the technical part of the equation and policy part come together for a final decision after receiving the input from the various agencies?

Mr. LORENZO. That is a very difficult question for me as an individual to answer. I will answer you very truthfully and honestly, I don't know where it is. I don't think you have it.

Does that answer your question?

Senator NUNN. Not any single place.

Mr. LORENZO. That is correct. I don't think DOD should be the total picture, but I think DOD is very critical and a very major contributor. When I say DOD, I say all of its intelligence agencies and all the intelligence agencies we work so well with, like the CIA, DIA, so forth.

That working relationship is very good, very critical and very vital.

Senator NUNN. Go ahead.

Thank you.

Mr. LORENZO. I would like to just cover one more thing here. There is a trend, and this goes back to what I said earlier, Mr. Chairman, we are turning down more cases or rejecting more requests for technology transfer.

For example, just to give you and the subcommittee a feel, for the munitions cases or West-West trade, let's say, in the 1981 calendar year, we handled or processed about 8,000 cases in our office in DOD. That was just a part of the 28,000 we delegated, you might say, by

mutual agreement, that Bill Robinson and the Munitions Board handles and that working relationship with the Munitions Board in State and Defense is outstanding.

It has been very good for years. We do get together and solve our problems very well, but let's just say this: Less than a couple years ago, the turndown rate was less than 1 percent. In 1981, the turndown rate was 5 percent, but that is sort of misleading. It's apples and oranges a little bit. Well, the turndown rate was 5 percent on the 8,000 cases we said we wanted to see as examples, you might say to set technical policies with the Munitions Board.

On a lot of the approvals we gave, on the 95-percent approvals, a lot of them have "fences" and "gates" and no no's here and there, or modifications to make things inaccessible or parts of it.

I don't like to see that high turndown rate increasing because that implies we have gone back to the other points I have made. We are not communicating too well with our friends in private industry. We are spending a lot of money. But we do offer and have offered more advice through what we call a defense advisory service.

The State Department works with us very closely. Instead of a contractor or an applicant submitting a total case, he submits just a draft. We give an advisory, sit down and talk it over with them and back they go. We don't waste a lot of time and create a lot of friction and irritation. Technology transfer, by and large, in our open society, I think is communications, making it known to all sectors that are involved an awareness of the impact of certain critical technologies. If we do that, and I am talking about university research which we are working very closely with, a lot of studies, National Academy of Science and all around the country, I think we will get there better in our open society.

As Dr. Guy Steven recently said, we get confused in this country of having too much of a matrix organization where we hear everybody from all sides. It is known to the Soviets and we have been accused by them in international fora having an "ad hoc" form of government.

Everybody speaks and everybody does everything, but by and large, I think if we keep on that approach, and we have no other choice than to do that, that is our way of life.

I think once we get there, we are going to be in better shape than our potential adversaries.

On dual use technology, which this committee is primarily interested in today, working with Commerce and looking over the numbers, it seems like we had a rejection rate of less than 2 percent on the defense process cases and that was, about 2 years ago. And this past 1981 calendar year, that reject rate was up to 15 percent. There the job is very, very difficult because you are dealing with people who have made a product primarily for the civilian market and it does have defense application.

Of course, that was a sample of 3,500 cases we did, taken from the commodity control in Commerce which approximated something like 77,000 cases in 1981.

So I have covered here just the highlights, the MCTL. We are improving it. And I might just say, with a very small staff we do interface with a lot of people. There are over 300 key technically qualified people

we interface with in the rest of the Department of Defense, such as all the military agencies, predominantly the research and acquisition people, counterparts and all the intelligence agencies and many, many, thousands in the private industry.

To give you an example of private industry and our interfaces with it, MAPAG alone, a multiassociation reviewing our MCTL right now, has over 80 company members, but a staff person gave me an estimate of over 90,000 people in American industry.

So we have underway, have done and have a tremendous educational process for technology transfer.

I might go a bit further, Senator Nunn, and I know you are well aware of our four power meetings where we meet with Germany, France, and England twice a year. Dr. DeLauer is the principal representative for the United States and I am the alternate.

We also meet with CNAD, the Conference of National Armament Directors, of 15 nations in Brussels, Belgium, twice a year, and since I have been aboard, I may not have become unpopular but I have introduced on the agenda or at least I have helped introduce it. It has also been introduced in the NATO technology transfer study and others, which is a very good thing, and Dr. Bryen's statement is going to uncover that very important study, underscoring to the allies: "Hey, you are very nice people, we need you; we need a mutual military capability but we want to help you close your doors on letting dual use critical technology out to potential adversaries or places where they can do harm."

And this is very, very effective. The bottom line on the NATO technology transfer study, in my opinion, is to get the respective Minister of Defense, counterpart to our Secretary of Defense, involved in their government infrastructure on all technology transfer, particularly dual use, going from their civilian contractors into the East-West bloc.

And a lot of progress has been made and I don't want to steal the thunder of my colleague, Steven Bryen. He is probably going to talk about France. France has a new law where the MOD gets into this process and the law went into effect October 9 but it is on the agenda now and all of these international fora are getting attention.

They know and I give credit to our intelligence community networks, that we have good networks. They also have a lot of good networks, not comparable to ours. They are asking us now in meetings, and they bring the subject up themselves. They say if we get something leaked, let us know. So I think our savior with our allies is their MODS and I say they are working the problem and they have a long way to go and I will defer the rest to Dr. Bryen to get into that area.

I am pretty much through with my statement, Mr. Chairman.

You can go ahead and shoot questions. We do have the DOD technical data base we outlined. The foreign disclosure technological information system is a massive effort. Just the supporting documentation is over 10,000 pages.

On foreign availability, which you sort of alluded to in your question. Let me say this. True, DOD may not be the agency to put it all together, but certainly with the intelligence agencies, I think we can make a significant contribution. If for military enhancement of a

potential adversary, I think DOD is definitely the main arm and also should play a major part but I cannot answer your question, who is that total agency.

May I suggest you go talk to Senator Garn, he may have some ideas on that point.

Senator NUNN. Thank you very much. When you make up the militarily critical technology list, the MCTL, does that in effect determine it for even availability of technology?

Is that a key part of the process?

Mr. LORENZO. The MCTL is concerned with availability in the adversary countries. If they already have something in great bunches, or certain technologies, it is pretty hard for us to say to our allies that we have to control it. There is definitely a corollary or strong relationship.

Senator NUNN. We have heard in previous testimony that diversions of U.S. technology occur through free world nations. In light of this, do you think D.R. & E. reviews an adequate number of free world export licensing cases?

Mr. LORENZO. We need to do more in the free world area. Since this is an unclassified session, I won't cite the countries that cases are going to. We are on record now in daily dialog, you might call it, in an argument with the Department of Commerce. We do want more cases.

The answer to your question is, no; I don't think we are doing enough cases to the free world because technology goes into the free world. There are all kinds of international trade houses, all kinds of multinational hookups. all kinds of companies that are multinational; some are part or totally owned by the Communist bloc—yes; to answer your question, we should look at more free world cases and I think when the act, the Export Administration Act of 1979 is readdressed, when it comes up in 1983, that should be incorporated in the revision, or updating of the new act. We will be glad to make recommendations for you at that time.

Senator NUNN. Thank you very much. Does Defense Research and Engineering have a presence in the enforcement activities or do you strictly have the input in the policy level licensing or does DOD in any way enter into the enforcement?

Mr. LORENZO. We don't have I guess you would call a direct or substantive impact on enforcement, but we are consulted at all times. We are now preparing in connection with our colleagues on the policy side of Defense, Dr. Bryen, the "Mushroom Book," in other words, a book Dr. Lomacky on my right and I are preparing to help Customs identify high technology.

In other words, when they are out checking shipments and so forth, what is it they are looking for, how should they look for it? We should be more involved and we have been talking informally with both State and Commerce and they have expressed a desire for us to be more involved. We just have to develop the people and I foresee where we are going to have to provide people probably onsite to help out as this enforcement activity grows. This is something that has come up in the last 6 months or a year. Customs has put more people on.

Project Exodus is underway and they are revealing more. Yes; we

have to get with it. I think we have to provide more input and definitely we can help them in the technological and engineering aspects and particularly in training of their agents on what to look for, what it is when they have it, and how to handle it, and what to do about it.

Senator NUNN. We heard testimony from Dr. Lara Baker of the idea to establish a technical expert group somewhere away from Washington divorced from policy to function as a technical evaluation center, not that all the people would be housed there, only a small group, but that the technical information would be cleared through there. Would this be an advantage or do you see it as just adding one more layer in the process?

Mr. LORENZO. If I said yes, I would be shooting myself in the foot, Mr. Chairman. Dr. Baker is doing a very good job for us right now. He has a lot of good people and they contribute tremendously from their background in nuclear weapons development in that the major technology used is you might say supercomputers. He is doing a very good job. So from a selfish point of view, I would say no. I don't want him to do that, I would want him to do what he is doing right now, but if he decides to do it, of course that is his business in our free society.

I would like, if a group was going to start like that. and we essentially have parts of that right here; to see it in Washington. We are looking at—my bosses and I are right now permanentizing my staff, making it more professional, making it more career oriented and perhaps we are looking at alternatives, to set up you might say situations he has. His idea is good. But from the selfish point of view I am not going to shoot myself in the foot and bless him to do it in Albuquerque. I want him to work right now for me, which he is, and he is doing one mighty fine job.

Senator NUNN. How many people in your office are actually dedicated to what you call West-East trade functions? What is the staffing you have dedicated to that purpose?

Mr. LORENZO. I took a count very recently, as a matter of fact last night.

I have taken many counts since I have been on board. We have a total, you might say, on East-West trade which I think is a misnomer because we are talking from West-to-East trade, of 12 professionals and 4 secretarial. But of those 12 professionals we only have really 4 that you might say are deeply highly technically qualified people and 1 administrator. Then I have more technically qualified. I am sorry, I should have said 4, of a permanent nature and I am fighting for more and have gone down to my bosses for more and I am promised that I am going to get more permanent because this cadre of 11 people—we have 1 schedule C temporary, trainee, involves a lot of trainees coming and going. They are very good. That is part of the educational process.

We consider and I have gone to the mat on this, 11 truly technically qualified people to form a minimum critical mass in a centralized location because we are dealing, as I have mentioned before, with 300 highly qualified technical people in the rest of defense, and intelligence agencies, 90,000 in industry, and also you might say 5,000 in foreign governments.

I have never counted the number of R. & D. people we are dealing with in foreign governments. So I have drawn the line you might say. I don't think we could be any smaller and having gone through many recent exercises in the last 2 months, you cannot delegate any more of the responsibilities to the military services. We need a minimum critical mass just like an atomic weapon. You cannot get anywhere unless you have a certain minimum critical mass and from a management point of view I think that is a very logical point.

I would like to enhance them, make them career oriented, get rid of the temporary label. Qualified people are very important, but you have got to automate the data and use other management techniques that we are doing very fast, such as entering our [illegible] into FORTDIS. I think that pretty well answers your question. [illegible] are small. I think as the job gets bigger we have to get smarter with more automation or have more permanent people, and we are using a lot of contract help, too.

I might mention the Institute for Defense Analysis, headed up by Dr. Alex Flax. They have been supporting us particularly on the MCTL, and many other things and are doing a very outstanding job.

Senator NUNN. Do you or either of your associates have any recommendations about changes in the law that we should consider?

Mr. LORENZO. We have several recommendations. They are kind of detailed. We would like to document them for you and submit them for the record at a later date.

Senator NUNN. All right. Are those recommendations in the form of administration proposals or just DOD proposals at this stage?

Mr. LORENZO. The majority of them will be from the DOD perspective. But we will give you recommendations on the overview when the act is to be revised in 1983.

Senator NUNN. I also have a number of proposals I am going to probably make at the close of the hearings that I would like for you to review and what I will be doing is making recommendations to the subcommittee. There may be several of us individually, Senator Chiles, Senator Roth, and others, that would like to make recommendations to the subcommittee. But that is not an official final view of the subcommittee. We would like your input about those recommendations.

Mr. LORENZO. We will be very happy to participate, Senator Nunn. We have in the past. I have looked over the record. I want to congratulate you on the Culver-Nunn RSI law as well as other things. I think you are very internationally oriented. You are looking at the total picture.

I think technology transfer is a very difficult problem. We would be glad to work with you.

Senator NUNN. It is certainly not simple.

Mr. LORENZO. It is a very tough job—technology transfer—you are going against the tide, you don't have the big dollars a lot of the other programs have like a lot of the strategic and tactical programs. You are taking things away from people. You have got to know all the technologies. You have got to have highly qualified people. You have to tell people no. On top of it all, it is the most thankless job probably in the Department of Defense today.

Senator NUNN. Of course, we operate in an alliance also and if we do not coordinate in the alliance, if we don't have commonality, standard-

ization, interoperability, those things in the alliance, we deplete our resources to the point we can't defend against the Soviet Union.

The only way you get those things is to cooperate more at the R. & D. stage, at every stage which means you have got to have probably more technology transfer at least within the alliance. So this is not exclusively an American problem. America can't solve it. It has got to be an international approach as you have already said.

Mr. LORENZO. You are so correct. It has to be multilateral. You can't go unilateral on the controls. You are so correct. You have said it so well. I called it the "delicate balance" of giving friends—allies—technology and controlling critical technology that might leak to the adversaries' atmosphere.

Senator NUNN. The key to it is to get that list of the things you are going to control down to a manageable level and not having it so broad and so long that in an effort to control everything you don't control anything.

It is like classification, too. If your classification gets so broad, if everything is classified, in an effort to protect everything, you end up causing such disrespect for the system you don't protect anything and then you leak out information every day that is very, very important. So I think here the answer administratively is illusive, but at least in concept we have got to find a way to hone down what it is we control as the most important element and do a darned good job of that as I see it.

Mr. LORENZO. You are so right.

Senator NUNN. The challenge is how do you do that. We have got a lot of agencies involved. There is certainly no simple answer to it. But I appreciate very much your testimony. Do either one of your associates want to add anything at this point? We would be delighted to hear from them? Any suggestions, recommendations?

Mr. LORENZO. Fire their boss.

Senator NUNN. Do either one of you want to make any statement at this point?

Mr. LOMACKY. Senator Nunn, I think Mr. Lorenzo has outlined very well the kind of work that we do and the difficulties that we face. One of the major efforts that we have underway now is to achieve precisely what he alluded to; namely, to get our allies to cooperate with us in technology and export control. But we have a very intensive effort underway in Cocom. We have taken the critical technologies list and we are making very good progress and getting that list accepted in the negotiations on the Cocom list.

I am very encouraged by the attitude of our allies in that we were told over the years, no, they cannot control technology, this is strictly a U.S. kind of thing. I am very pleased that we have made some very important progress in that area. I might also add that as in the past so it is today they are extremely careful to demand and rightly so the kind of precision which you have alluded to; namely, they want to make sure that we have made a good intelligence assessment of the other side. They want to make sure that what we want to control is described in such a way that it has a minimum unnecessary impact on commercial trade.

I think with these criteria is they are presented to them properly I think the chances are that they will accept our proposals. If we do

not follow these rules I think we will have a very difficult time. Thank you.

Senator NUNN. Thank you.

Thank you very much, Mr. Lorenzo. We appreciate all of your cooperation, you and your associates. We know you have a tough job. We look forward to your giving us your reaction to the recommendations we will be making next week.

Mr. LORENZO. It is a tough job and it is a challenge. But with people like you on our side we will get there.

Senator NUNN. Thank you very much.

Our next witness, Admiral Inman, is coming in just a few minutes. I believe Mr. Charles Lecht is here. If you would kindly take the chair we will go ahead and hear from you and then we will hear from Admiral Inman. I think it is really fortunate we are going to hear from you first in a way because I have read your statement and find some very interesting points there that I think could be addressed later with questions from other witnesses.

We swear in all witnesses before this subcommittee. It is a matter of practice before the Investigations Subcommittee. So before you start your testimony, if you will stand and take the oath.

Do you swear the testimony you will give will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. LECHT. I do.

Senator NUNN. Thank you very much. We appreciate your cooperation with the subcommittee. We appreciate your meeting with the staff and discussing these areas. We know you are highly qualified in this whole area of technology. We look forward to having your statement.

TESTIMONY OF CHARLES LECHT, FORMER PRESIDENT AND CHAIRMAN OF THE BOARD, ADVANCED COMPUTER TECHNIQUES CORP.

Mr. LECHT. Thank you very much, Senator Nunn.

I have my prepared statement which I submitted to the subcommittee. I will summarize it if you would like.[1]

Senator NUNN. Your statement is not too long. We would be delighted to hear it, whatever you prefer to do. I might add, Mr. Lecht is the former president of the Advanced Computer Techniques Corp. in New York.

Mr. LECHT. Yes, sir.

Senator NUNN. Whatever you desire.

Mr. LECHT. I agreed to testify to this subcommittee on the issue of international trade of computer technology because I believe the goals to which this subcommittee is directed are correct ones and important ones for the national defense and security of this country.

I have spent many days abroad for the last 15 to 20 years and I have had occasion to work with both Socialist and Western countries. I have some different conclusions regarding Soviet or should I say Soviet bloc attempts to acquire a U.S. technology. I have reached conclusions as to why this is going on which differ from those which I have previously read about or heard about in the media or in Washington.

---

[1] See p. 570 for the prepared statement of Charles P. Lecht.

Primarily I have come to the conclusion that the concept that the Soviets want U.S. technology because they can't make it themselves or they can't buy it themselves is a fallacious one. I have concluded that the Soviet technology establishment—in the country which produces more scientific literature than any other country in the world—is capable of producing what it wants. I have thus concluded that the Soviets have been looking for U.S. technology primarily because they want to find out how our military materiel work, our missiles, our aircraft, our radar, our sonar, and the like. Since most highly advanced military technology is driven by dual use embedded computer systems to be found in both the private as well as the Defense sectors, the acquisition of these systems by the Soviets reveals information on how to jam our technology-driven military devices—how they operate or what their shortcomings are.

My prepared statement supports this thesis.

Furthermore, my experience abroad in dealing with a variety of companies, both American and foreign, has led me into direct contact with Soviet military on one occasion—I have been called at my hotel room by a Soviet general asking me to come have a drink with him, an event which I refused to do for my health and welfare, and loyalty to this country.

I have found that the notion of creating lists of items to guide what may be traded and what may not be traded and which can be used by persons at the borders of our country won't work in the high tech area, especially around computer systems technology. Much of this high tech stuff has elements which vanish into the microscopic world, has no metal thus are not detectable by machinery. For example, computers for the future are being experimented with as creatable in test tubes—protein based devices which are at the forefront of the technology. But, even today's metallurgical, chemical, and electronic-based devices which are at the developmental forefront, allow for the creation of systems which are extremely powerful and extremely small and almost nondetectable. These are the devices being used in our embedded weaponry.

I thought I would call this to the subcommittee's attention to indicate that I really believe the concept of border policing and lists which may be looked at by, say, border patrolmen or the like is an untenable one in this age of high science in and about computer and communication systems technologies.

Senator NUNN. You are saying the advanced technologies are so sophisticated, so small and involve know-how in many cases and that border control is not the answer to controlling that kind of high technology?

Mr. LECHT. For the most part I don't see how it could be controlled that way at all. But I also don't believe that the capacity to create these is the privileged commodity of the U.S. scientific community. I think the chairman of Control Data Corp. and others have testified in the past that U.S. dominance in the high tech area is no longer a reality. Japan, countries like France, England, Russia, and even Soviet bloc countries have the capacity to make exactly what we are making now.

So I wonder about the Cocom lists and our ability to police these lists and whether this preoccupation was not causing us to focus in the

wrong direction, so that we cannot see that the Soviet desire to acquire our technology has more military meaning than anything else.

Senator NUNN. What do you think we ought to be doing? You acknowledge it is a serious problem, I think. You would narrow it down more to the pure military analysis part of it. You are saying border control in this sophisticated age is not adequate, maybe not even relevant. What is it that we should be doing in this country in your view to begin to address the problem as you see it?

Mr. LECHT. First of all, I believe the establishment of a subcommittee like this one to identify the problem is very relevant and extremely important because up until this point I am not sure that we have identified the problem in the United States. Certainly cooperation at the source of these high technologies is probably the beginning point. I have here a list of the American microprocessor companies and their foreign involvements and it is quite astounding. You've got companies for example, like American Microsystems, Inc. It is a Gould Co. It is a U.S. owned company recently bought back from a West German company which has involvements in Austria. We know that Austria has been a center of technology transfer in trade for many years now. If you go through this list, and you see companies like Fairchild Camera, Analog Devices, you see Motorola, Nixdorf, Solid State Scientific, all with foreign involvements, with foreign staff on site at plants abroad. Even if these are U.S. companies they are worked in by foreign people in various locations around the globe.

Some of the devices that they are working on are so small that you can carry 1,000 of them out in your pocket and still not be detected.

Senator NUNN. When you say controlled at the source, do you mean much more governmental business involvement and coordination? Is that what you mean?

Mr. LECHT. Yes, but better focused. As I said earlier, if you buy the idea that we are no longer the country which has a privileged position in solid state large-scale integrated circuit technologies. Then we don't have as our primary worry controlling trade in those technologies. They can be bought elsewhere. We have to control those particular technologies that relate to our national defense—the plants that make these technologies, the data describing them and the way they are employed.

Senator NUNN. We go a step further. How do you go about doing that? What do you do that we don't do now? I think you have made it plain that some of the things we do now you don't believe are relevant, but when you really hone it down, trying to control the defense technologies and as you have described it, what steps do you think could be taken that are not now being taken?

Mr. LECHT. It should start with an education program that delineates between those items which are peculiar to our national defense and those items which are not. We do not need a blanket embargo on all high tech going abroad. Such an embargo doesn't have any meaning. We do need better identification by the Defense Department of those technologies which are key to our national defense and then a campaign to educate source management who are creating these technologies.

Senator NUNN. Both in this country and in our allied countries?

Mr. LECHT. Yes, sir.

[At this point, Senator Chiles withdrew from the hearing room.]

[The letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive hearings without a quorum of two members for the administration of oaths and taking testimony in connection with hearings on the Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations, to be held May 4, 5, 6, 11 and 12, 1982.

WILLIAM V. ROTH, JR.,
Chairman.

SAM NUNN,
Ranking Minority Member.

Senator NUNN. You believe that if the list is properly made up and kept current and changed with the state of the art, that that kind of education campaign between the Department of Defense and the other departments and high technology industry would be more meaningful than all the law enforcement we could muster?

Mr. LECHT. Yes, I believe it would be a good start. Certainly in the United States you have a lot of sympathy for Defense requirements and the requirements for maintaining secrecy around high technology affecting that defense. But abroad, I am afraid our partners don't have the same sense of urgency with regard to the handling of our high tech products. For example, I have seen Russian computers sitting alongside American computers running the same software in some of our allied countries. I have concluded that in other country locations of our plants producing high tech there really isn't a lot of sympathy for our secrecy needs.

I have seen Communists working in American plants in high tech in northern Italy for example.

Senator NUNN. Communists actually working in the plant?

Mr. LECHT. Yes; card-carrying Communists and proud of it, encouraging others to attend their meetings in the evening.

Senator NUNN. Are these American companies operating abroad?

Mr. LECHT. Yes.

Senator NUNN. Dealing in high tech?

Mr. LECHT. Yes.

Senator NUNN. Dealing in items that you think might be crucial to the national security?

Mr. LECHT. No question about it, sir.

Senator NUNN. You travel quite a bit. Does your company do business in several foreign countries?

Mr. LECHT. We have just about worked in every Western country, in the Far East, Australia, Japan, South Africa, and black African countries. We have also worked in Yugoslavia and in the Soviet Union, in Hungary, Czechoslovakia, and the like.

Senator NUNN. What is the general attitude of American businesses toward this problem? Do you find them generally anxious to cooperate or are they very skeptical about governmental efforts?

Mr. LECHT. No; I think that any serious businessman in this country is compelled to cooperate with the Government's requirements on the transfer of technology abroad. I think that they generally are sympathetic. The problem is it has been so overstated in the past that at times they become suspicious that it is going to in some way impact their capacity to trade anything.

Senator NUNN. In other words, by overstating the problem if the Government does that, and by having too many items on the list that perhaps do not have the significance that you have described, you create skepticism among businesses and less cooperation rather than more?

Mr. LECHT. Yes, the American businessmen who are going abroad and who see large-scale integrated chips of the most modern variety coming out of the Soviet Union, wonder what the flak is about in the newspaper which says we shouldn't trade with them.

Senator NUNN. You mention in your statement that the General Electric Co. trains Soviet personnel in computers in Milan. Would you tell us a little more about that?

Mr. LECHT. I mentioned that they trained them in the latter sixties. The General Electric Co., as well as IBM and all the other manufacturers, have been selling high technology to the Soviet Union of one kind or another, I should say, over the past 20 years off and on with various periods of time where restrictions prohibited this.

And with the sale of computers, frequently there is training as part of the package of the sale of these devices. This involves taking the client's staff into a classroom to train them on how to operate, program, and, in general, how to use the machines.

Well, if you sell to the Soviet Union, they need the training also. I have seen Soviet staff in classrooms in Italy being trained by computer manufacturers' representatives from the United States of America.

Senator NUNN. When you actually sell the computers, the training goes with it, though; doesn't it?

Mr. LECHT. Frequently it does, sometimes they will buy it.

Senator NUNN. The critical decision is whether they sell the computers at all.

Mr. LECHT. I don't think that stopping the sale of computers will benefit anything though. They hardly buy anything from us anyway in the computer area in the Soviet Union. The demand statistics don't seem to justify the concern so often expressed that they cannot manufacture or obtain high tech without U.S. involvement. What they are more concerned with in my opinion is high tech that finds its way into the nose cone of a missile.

Senator NUNN. So you are saying the kind of computers that have been sold you don't think are damaging?

Mr. LECHT. Most of the computer technology the United States has sold to the Soviet Union could have been bought anywhere else or made themselves. It is the stuff they stole, sir.

Senator NUNN. There are export control lists that our Government has. Are these widely distributed in industry, in your view? Does industry appear to be cognizant of what the Government believes is critical?

Mr. LECHT. These export control lists, I think, spend more time in the Government files than they do in the hands of people doing international commerce. I have never seen a recent export control list until your subcommittee started. I should say, I haven't seen one in years. I had seen one earlier. I don't think the past or current export control lists portray a deep knowledge in current high tech by those who prepared these.

Senator NUNN. Could American private businesses and people in the high tech area play a role as an advisory kind of committee in this area and be helpful or would there be such inherent conflict of interest that it would not be feasible?

Mr. LECHT. You have to start somewhere. I think bringing some high tech advisers into the Government to better help define the problem and better help create the guidelines is absolutely mandatory at this point in time.

For example, some of the lists at the present time are influenced by the notion of size of the machines. Well, size today means old, not new. The bigger they are the older they are, the newer they are, the littler they are. So on occasion we hear that we can't sell big machines but we can sell small ones. It frequently turns out that the smaller machine the more powerful it is, the larger, the less powerful. Thus, there are a lot of conceptual revisions needed and I think the scientific community ought to be brought in on these revisions.

Senator NUNN. Have you had any dealings with the Department of Commerce in enforcing American technology transfer?

Mr. LECHT. Well, the Department of Commerce once helped me transfer some of my technology over to Italy to demonstrate it at an Italian fair, but other than that dealing, I have had none.

Senator NUNN. Have you seen them create much of a dialog with industry about what should and should not be on the list? Is there any kind of educational effort going on from the Commerce Department that you have personally seen?

Mr. LECHT. No, sir, I haven't.

Senator NUNN. We appreciate very much your being here, Mr. Lecht. Your testimony has been very helpful and very heartening and we thank you for your cooperation with the subcommittee.

Mr. LECHT. Well, I was heartened to see this subcommittee formed, Senator Nunn. I wish you good luck and great success.

Senator NUNN. We hope to continue to bounce ideas off of you.

Mr. LECHT. It will be a pleasure, sir.

Senator NUNN. Thank you.

At this point, Admiral Inman is our next witness and we will take about a 5-minute break while we wait on him to arrive.

[Member present at the time of recess: Senator Nunn.]

[Brief recess.]

[Members present after the taking of a brief recess: Senators Roth, Nunn, and Chiles.]

Senator NUNN. Our next witness is Adm. Bobby Inman. Admiral Inman, we appreciate the excellent job you have done for your country in every area and I particularly appreciate the interest you have displayed in the technology transfer area. I don't know of anybody in government that has concentrated on it more and given it more em-

phasis in the last couple of years than you have. I also appreciate your cooperation with our staff in preparing for these hearings.

We are delighted you are here. We swear in all the witnesses before the subcommittee so if you would take the oath we will be glad to get your statement.

Do you swear the testimony you give before the subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

Admiral INMAN. I do.

Senator NUNN. Thank you.

Why don't you go ahead and proceed and then we will have questions.

TESTIMONY OF ADM. BOBBY R. INMAN, DEPUTY DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Admiral INMAN. Thank you, Mr. Chairman. I have a statement that I will submit for the record, if I may, including as a part of it the unclassified version of the intelligence community's look at Soviet acquisition of Western technology.

Senator NUNN. That will be admitted, without objection.[1]

Admiral INMAN. The origin of that study really begins with this subcommittee and its staff, as you will well recall, from dialogs that go back a year and a half, the questions asked about the general status of Soviet technology transfer and inadequacy of the answers we had——

Senator NUNN. If you could pull that mike up a little closer.

Admiral INMAN. How is that?

Senator NUNN. That's good.

Admiral INMAN [continuing]. And the inadequacy of the answers we had available. The whole question of technology transfer had not been a priority topic. Out of the dialog between this subcommittee, its staff, and the Senate Select Committee on Intelligence, we were asked in March 1981 to do an interagency study to pull together all we knew about the Soviets success in acquiring Western technology and their use of it in their military buildup.

A 6-month effort was undertaken. The results were startling to those of us inside the intelligence community as well as to the users. It was clear that we had a great deal of information about the nature of the Soviet efforts, their use of their Eastern European allies to support it and the general outcome. We provided that study in its full classification level to the Senate Select Committee last October, and then we proceeded in the ongoing dialogs within the administration and with the staff both of this subcommittee and of the Senate Select Committee to try to refine what we knew to improve our capabilities to track the problem better in the years out ahead but most of all to try to help assess the impact of the damage and what might be done in response.

I would point out two or three highlights from that knowledge for our discussion today. First, is we look at the militarily useful, mili-

[1] See p. 577 for the prepared statement of Adm. Bobby R. Inman.

95-929 O - 82 - 16

tarily related technology that the Soviets have acquired from the West, about 70 percent of it has been accomplished by the Soviets and the East European intelligence services. They have used clandestine, technical, and overt collection techniques in the process. They are trying to get technologies of proven Western weapons and component designs that can be applied directly to Soviet weapons research and development, and industrial needs.

They concentrate their efforts through open purchases, legally accomplished where that is possible and where it is not successful, through illegal purchase and when that is not successful, through use of espionage.

The sources of the technology may be Government classified or unclassified reports, private company's proprietary reports, open source technical documents from companies and Government organizations—much of the embargoed equipment falls in this category as well. The Soviets have undertaken a thorough vacuum cleaning of everything in the public sector which will let them better target their espionage activities. Of the remaining 20 to 30 percent of the acquisitions of information of potential military value to the Soviets, most comes through legal purchases and open source publications acquired by other Soviet organizations, such as the Ministry of Trade and related international bodies.

A very small percentage of it comes from direct technical exchanges conducted by scientists and students.

As we look out into the later 1980's, we believe that future Soviet and Warsaw Pact acquisition efforts are likely to concentrate on the sources of such components and manufacturing technologies, such as defense contractors in the United States, Western Europe, and Japan who are responsible for military technologies, general producers of military related auxiliary manufacturing equipment, again, in the United States, Western Europe and Japan, and small- and medium-sized firms and research centers that develop advance component technology and designs, including advance civil technologies with future military applications.

Since the early seventies, and Soviets and their surrogates have increasingly used their national intelligence services to acquire Western civilian technologies, for example, automobile, energy, chemicals, and even consumer electronics. Since the midseventies, the Soviet's European intelligence services have been emphasizing collection of manufacturing-related technology in addition to weapons technology.

And since the late seventies, there has been an increased emphasis by these intelligence services on the acquisition of new Western technologies emerging from universities and research centers.

I can only conclude from all of these efforts that the Western security services will be severely tested by the Soviet intelligence services and their surrogates during the eighties.

I am pleased to say that coordination within the intelligence community and intelligence support for the executive branch, the various departments and agencies which have responsibilities in this area, is substantially better than it was a year ago. In the wake of the study document, the DCI has established a Technology Transfer Intelligence Committee along with a dedication of analytical resources which had

not previously been committed to the problem and new mechanisms to coordinate how the intelligence community pursues intelligence collection, analysis, and reporting, and new subcommittees to support the activities of the other departments as they try to bring better coordination and better formulation of policy.

There is still a great deal of work to be done.

Mr. Chairman, rather than proceeding further with the formal statement, I think it would be better to use the time to try to field questions of members of the subcommittee.

Senator NUNN. Thank you very much, Admiral Inman.

I will take just a few minutes and, Senator Roth, I defer to you and Senator Chiles.

We just heard testimony from Mr. Lecht who is in the software side of the high technology business. His statement, if I could paraphrase it without trying to quote it, is essentially that the high technology critical lists that he has seen are very broad and tend to be very severely outdated and do not aim themselves toward state-of-the-art technology, small computers, and that sort of thing. I understand from other witnesses, too, that there seems to be a consensus that we ought to really make an all-out effort to narrow the list and to try to find the areas that are critical to the Soviets rather than trying to do a job of controlling more and more, poorer and poorer.

Do you generally share that sentiment or do you disagree?

Admiral INMAN. I do not sign up to it entirely, Senator. I think we have to stay focused on the larger problem of trying to do the best job across the broadest range of technologies. I agree one ought to prioritize the activity. Clearly the critical technologies ought to get the immediate priority attention. But what I worry about in that formulation is that one would then conclude that is the end of the problem and that one does not need to pursue the whole broad range of activities.

There is no doubt in my mind that the highest priority ought to go to the direct weapons-related technology, the ones where we have classified research underway.

The mechanisms may not have worked well in the past, both to update those lists and to have the kind of dialog with industry that lets you know what is coming along as the newest area of technology. I suspect improvements are doable and prioritizing ought to be undertaken regularly, but as a broad general national problem, we ought to look to try to preclude the broadest range of acquisition by the Soviets of Western technology which feeds that continuing military buildup.

It is from looking at the scope of that buildup across the whole range of strategic conventional forces, manufacturing capabilities, that I am persuaded this is a challenge that is going to be with us for another decade.

Senator NUNN. When you look back—you have been involved in the intelligence area for some time now without regard to any administration, Democratic or Republican, but if you look back at the last decade, how would you rate our greatest failings in the technology transfer area?

Admiral INMAN. I have to conclude from simply the accumulation of evidence and Soviet success that our performance has been very

poor, indeed, in the whole area of limiting technology transfer, but I think, Senator Nunn, that you really have to look at that and in the climate of times. For a decade, the country at large, as well as the Government, put its faith in total broad terms in détente as an approach that was going to bring us peace, that was somehow going to slow down the military threat we were going to have to face—a general optimism that all exchanges were inherently good, that whether they were scientific or technical or simply economic, business, that that would produce from our principal adversaries a greater willingness to work with us rather than to feed the military threat that we are going to have to face.

That was also a climate when we were pulling down our whole national security apparatus with the basic question of what can we do without? That impacted heavily on the intelligence community where we lost a great deal of manpower to pay for new technological collection opportunities. As we gave up what we could do without, one of the many things we gave up was any kind of coordinated collection or reporting efforts against the Soviet acquisition of technology in this country.

It had its own impact in trying to assess the success of the Soviets R. & D. efforts. One of the small side benefits of this latest study is that we now recognize the Soviets did not embark, as some had feared, on the major investment in R. & D. to find breakthroughs in areas that we were ignoring. Rather they used the clear technique of taking whatever the West was developing, adapting it to their own needs and getting it into production in very impressive timeframes.

When one looks back, what you get is a reflection of activity all across the Government and the general attitude of the country not to worry about the loss of outflow, it is kind of a security blanket comfort that any kind of trade or exchange was inherently going to be favorable for us. When one looks at the results 10 years later and looks at Soviet activity, I think it would be very hard to come to those same conclusions at this point in time.

Senator NUNN. If you had to rate our problems now addressing the most critical for the next decade in this area, how would you rate the major challenges?

Admiral INMAN. I have read a lot of writings, I have listened to a lot of speeches, both inside the Government and in the private sector over the last decade in describing Soviet economic problems. I can remember 10 years ago listening to a learned authority tell those of us who were in his audience that within 5 years, the state of the Soviet economy would be so bad and the problems with the minorities would be so difficult that we didn't really need to worry about the Soviet military buildup. They would be turned inward to deal with their problems and they would not be a challenge.

I have heard the same authority say almost exactly the same thing last spring, almost 10 years later. But, in fact, I am still looking for that change. The economy is in bad shape, cost of the empire is high, but they have continued to protect a steadily increasing investment across their whole military structure for the last 17 years. The result is that we now face a qualitative challenge as well as a quantitative one.

The qualitative one that we didn't face at all 11 years ago, an ability to stay and fight, with a whole range of weapons systems which have very impressive standoff capabilities.

Much of that growth in the Soviet side, in manufacturing techniques, in weapons systems, in design, has come about from their acquisition here. As I look out for the next 10 years I don't see anything on the horizon that is going to change those priorities on the part of the Soviets. I think they are going to continue to have economic problems.

The major pressure on them right now is the agricultural failure and the hard currency they have to spend to buy grain. But they have continued to protect the investment in the military sector and I think they will continue to do so. Therefore we must pay very high propriety, I believe, to outflow of technology which will let them quickly adapt and bring into use of more sophisticated weapons systems, standoff, longer range, better guidance systems—accuracy is going to be increasingly a problem we have to deal with in their strategic weapons as well as their conventional weapons and, again, a good deal of the technology for that has come out of the West.

So I would rank efforts to preclude Soviet access to high technology, to things that would improve the firepower, the acquisition, reconnaissance capabilities very high in our own national priority interest. We have got a very long way to go in our own rebuilding program.

Senator NUNN. In that rebuilding program, what are your priorities?

Admiral INMAN. Let me split that into two categories. I can speak pretty easily about the priorities in the intelligence community side. There I believe the challenge that we are going to face in the decade ahead is going to find its greatest prominence in challenges all over the Third World, competition for raw materials, natural resources, problems with access to markets, and countries with political instability. A great change that faces us is Soviet mobility, mobility of the Soviet power to the degree that we have never had to worry about in the past.

Thirty years ago, when we looked at the Soviet Union as an adversary, their forces were primarily designed for use perhaps 200 miles from the periphery of the Soviet Union. By the mid 1950's, it was a 600-mile line. By the early 1960's, and the exercises, it was a 1,500-mile line. But was still largely in their own discussion a defensive position and a defensive structure.

By 1975, that had changed abruptly. Theer was no longer a 1,500-mile line. They looked to use their forces wherever they saw the interest of the State involved. But they were still cautious and therefore in the late 1975 time frame, in the move to Angola, they used Cuban troops—not their own—with Soviet airlift and Soviet equipment. In Ethiopia in 1977, the same pattern evolved. It was Vietnam's manpower, Soviet equipment, that moved into Kampuchea in 1978. The watershed came in 1979 with the Soviets willingness to use their own forces in Afghanistan.

We had watched a massive airlift exercise into Mongolia in April of 1979. And that turned out to be a precursor for a massive movement of force into Afghanistan on the Christmas date of 1979.

When one thinks out to the next decade, with a new generation of leaders who may not be as cautious as these old Bolsheviks that we have

dealt with for the last 17 years, I believe one has to worry a great deal about whether those new leaders will be as reluctant to use Soviet military capabilities beyond their own shores.

It is not beyond the realm of possibility that we will find a decade out, or sooner, an unstable situation and sudden quick movement of Soviet military forces into the arena and we are then confronted as the British are now confronted in the Falklands with the fact of military presence and trying to contemplate what to do about it. But it is going to be vastly different than dealing with Third World nations using borrowed military equipment, with sophisticated capabilities, with the ability to use that high technology at very substantial distance.

The country has to contemplate whether we have the mobility, the range of conventional forces that can deal with that kind of challenge.

It is a very long winded answer to what are the priorities for the future, but we are going to need to know a great deal about countries all over the world, to try to anticipate in advance where the instabilities are developing that might offer the opportunity for our adversaries to take advantage of the opportunity.

We are certainly not going to be able to do less in following the threat in the Soviet Union itself, to the peripheral nations, particularly in Eastern Europe and across the central European plain.

Senator NUNN. Getting it down to the high technology area, what is it that we should do better than we are doing now? What should be our emphasis in high technology?

We have heard a good many suggestions over the last 4 days of hearings and we are really searching for priorities. If you had to name the priorities of ways which can improve, what would you list?

Admiral INMAN. Senator Nunn, I am not the best witness to answer that, since I have spent most of these last 30 years looking out at what others do, not at what is happening in the United States.

Senator NUNN. Let's look at the intelligence area then.

Admiral INMAN. In the intelligence area, we clearly need more analytical personnel, dedicated to a range of problems, particularly to problems like technology transfer. I am less certain what we need in the counterintelligence area. I am less certain because we have had a long time, a number of delays in getting underway with the kind of detailed examination of our long-range needs in that area that has already been completed in the foreign intelligence area.

True, there is a major component in technology transfer avoidance that falls to the FBI, to the other organizations that operate in the United States. There is a study now underway which should be finished by July which will define with a great deal more clarity, both the threat that is faced, the methodology being used by various foreign intelligence services to extract information from this country and the kinds of resources that are necessary to deal with it. So, you will get a much better answer on this question along about late August 8 or early September.

My guess to you is that the first priority is a pretty substantial input of manpower into the Federal Bureau of Investigation. Also less expensive and easier to do these days are going to be some additional steps to automate files available to Customs, Immigration, to increase the speed with which they can correlate information available to them, and make it available to the enforcement agencies.

From my own cursory examination, and your detailed one in these last days probably now already exceeded my knowledge, most of these agencies have had very little help in the last year or so, either in the way of manpower to deal with the increasing foreign presence in this country——

Senator NUNN. The FBI has had a real cutback in this area.

In the last 6 years they have had substantial cutbacks.

Admiral INMAN. It is an area that I don't believe there is a substitute for manpower to deal with the problem.

Senator NUNN. Senator Roth?

Chairman ROTH. First, let me publicly say what a splendid public servant I think you have been, Admiral Inman, and as a member of the intelligence committee I regret very much your decision to depart.

I think these hearings initiated by Senator Nunn are extremely valuable and ones that are at least to me very complex and troubling.

If I understand your answer to an earlier question of Senator Nunn, you disagreed with the idea that we should concentrate on select areas to prevent the transfer of high technology but instead, have a broader approach.

Admiral INMAN. I disagree, Senator Roth, only if that means you are simply going to concentrate in the high technology area and then give up the efforts on the other areas.

I have no difficulty at all with the prescription that would say the highest priority, the maximum concentration of effort in the intervening months should be to try to stop the outflow in the highest technology area. And we should be able to rapidly define that from inside the Government and we ought to get the new mechanisms established very quickly that let Defense stay right at the front edge of what is coming along in industry. Most of it, I believe, will be coming out of advanced research in any case. So it ought to be feasible to have a very rapid updating and change of focus of where your highest priority is, but I believe we should never lose sight of the breadth of the Soviet efforts and I take the view that it is in our long-term national interest to impede as much of that as it is feasible to do.

Chairman ROTH. That is the point I would like to get at. To me it is troubling because looking at it from the one perspective I agree with you. But at the same time, as a democracy we take great pride in having an open and free community, so that once we start talking about preventing the transfer very broadly, you come in to conflict with other goals of this county.

I have been told that particularly in the area of research and development, the free flow of information among the scientists is fundamental and that one of the reasons for our success is that you do have this free discourse between the universities, Government and the private sector, all which makes it seem to me extraordinarily difficult to have very effective controls in a broad sense of the word unless we make some sweeping changes.

Then there is the other aspect of the problem and that, of course, is trade which is important to this country and on which our future prosperity and strong economy depends.

Often one hears that if one shuts off this technology we are shutting off sales and that means that we cannot compete not only with those behind the Iron Curtain, but other democracies.

So that I wonder if we can realistically shut off all technology without impeding some of these other efforts. Would it make sense that we should export no technology, not only from the military point of view, but from the competitive point of view?

Would that be a practical approach to try to shut off the transfer of all technology?

Admiral INMAN. Senator, I don't think it even feasible to consider shutting off all of it. I have been spending a lot of time tugging at this problem since the committee first started asking me questions about it 2 years ago.

I have a perception that the leakage from basic research is minimal. There is a little. But that the Soviets themselves have difficulty in applying that. That burns up time; that it is in applied technology where the gains are quickest; where the applications are fastest, where one can also make sure judgments about the impact on our own case if we make an effort to impose additional restrictions.

I would set out for your several basic ground rules with the ease of one who is departing that is not going to be responsible for a great deal of it.

First, that before one enacts additional legislation or establishes new controls the first emphasis ought to go on insuring that the ones we have now work well. I think we will clearly document in the next several months that in dealing with the espionage problem we have simply provided far too few people with too little support here in this country, to let the job be done the way it needs to be done.

I suspect when one examines closely the implementation of the Commerce export controls, the efforts by the State Department in the international trafficking and arms regulations, and looks at the Defense critical technologies list, you are going to find several things.

You will find a measure of protection of bureaucratic turf. That always happens when organizations are being pulled down in size. The first priority becomes protecting turf. I think you will find probably some shortfalls in manpower and in automation and perhaps not as close working relationships among the various organizations as really ought to occur.

I would put first priority on trying to improve the performance of the existing mechanisms.

There may be a need for some additional legislation. I would go very slowly in that category where one is dealing with the open publication of basic research. There I have been trying since last January to spur the academics into addressing that problem themselves. I have a basic faith that if they put some effort on the problem, they are probably far more likely than those of us in Government to come up with some thoughtful ideas on how one impedes the outflow and I choose that word very carefully.

I don't believe the idea of a total cutoff of outflow is achievable and I am not sure it is even a useful goal. But I think one ought to consciously look at the whole range beginning with advanced technology as the area where the highest payoff is likely to occur and look at all the measures that one can undertake to impede Soviet access to technology which they can use for production of military hardware.

Chairman ROTH. Admiral, to what extent has the Soviet Union been successful in securing this technical information from our allies and partners?

Have they been better, about the same, or less effective than we have in protecting the technology of national security?

It seems to me this is important from a number of standpoints, first of all, to what extent we are going to exchange technology; second, many of us think that it is important that because of the increasing costs of weapons that they should begin to purchase agreed-upon weapons on an alliancewide basis.

It would be increasingly difficult if we couldn't share technology because one or the other of us were less reliable.

Would you care to comment on that?

Admiral INMAN. We are too far down the path to try to walk back from sharing technology with our allies. I would not want to walk it back because I think commonality of weapons systems and capabilities over the long term is going to be a greater plus than the potential drainage. But in any case, we are too far down that path. But there are components that are not subject to immediate Government control in any case. With the growth of the multinational corporation, there are many subsidiaries that are not only manufacturing, but file for patents back in this country from foreign subsidiaries. And we sat about consciously to help our former enemies as well as our former allies rebuild their economic health.

We have been successful beyond our wildest dreams and now some of that competition is very intensive. One cannot seriously talk about being completely successful in denying Western technology to the Soviets without including our allies as close partners. That means it is a much more complex problem. Where we can impact is on the direct access for equipment, hardware that is being developed; particularly in the military sphere where clearly we are the leaders still.

In response to part of your question about how much do the Soviets acquire from the various components, I don't have a certain figure on the percentage of the success that has come out of Western Europe or out of Japan. I do know that they have intense efforts in those areas just as they have here. We have had some particularly good reporting in the last year from a defector in the Far East who documented very substantial efforts the Soviets made in Japan to acquire technology.

Again, in Western Europe and Japan, as here, they have been successful in buying a good deal of it. They haven't had to steal it. What is clear is that the Soviets to this point in time are very dependent on the totality of that vacuum cleaning and purchasing for this massive military buildup that we have watched occur.

Chairman ROTH. My last question, Senator Nunn, you said in answer to a question that the Russians, the Soviets, have not tried to implement or fill out those areas that we have not provided to do work ourselves. There was a recent editorial in the New York Times commenting on technology transfers to the Soviet Union in which it expressed the opinion that lowering the barriers to the flow of technology to the U.S.S.R. is not necessarily a bad thing.

It editorialized that "a more relaxed policy would serve the West's best interests because a steady supply of foreign technology taxes the Soviet Union's incentive to develop its own, better to have the Soviets stealing and copying, following a few steps behind than working independently and becoming able to deliver a technological surprise."

What would be your response?

Admiral INMAN. It will not surprise you that I do not agree. It is wishful dreaming. To say that it has sapped the Soviet efforts, I am afraid portrays a lack of understanding of the state of the Soviets and how far they have come in building up an R. & D. structure.

You worry me a little in the first part of the question. I hope I did not mislead the committee in my wandering answer. We have not found evidence thus far of a Soviet breakthrough in a critical technology area that they have pursued on their own or indeed that we have ignored.

There clearly is apprehension in fields like charged particle beams and lasers, where they were clearly investing large sums of money in research and development and test facilities that they might in fact have that prospective breakthrough.

We have not seen evidence that they have achieved any. But what is clear at this point is that the primary path the Soviets took was to acquire what was obviously easily acquirable, technology from the West and to adept that to their needs.

They have done that ranging all the way from manufacturing techniques or technology to the guidance systems, to improve the accuracy of ICBM's and SLBM's and cruise missiles.

Chairman ROTH. Thank you.

Senator NUNN. Senator Chiles?

Senator CHILES. Admiral, I want to add my voice publicly to thank you for your outstanding service and to say that I hope your leave is going to be temporary, and that you will be back giving us your services.

You mentioned that the Soviets had a problem in agriculture and that they have had to expend their hard currency to obtain grain and food.

Argentina has been the principal supplier to the Soviet Union of grain. For that, the Soviets have paid hard currency.

Given the present situation in the Falklands, do you see the Soviets getting the possibility of not having to use hard currency, but being able to trade off weapons, which they seem to have a large capacity to manufacture, for grain?

Admiral INMAN. Over the past decade, the Argentines have turned largely to Western Europe as a source for their military hardware. That is expensive. They have not previously indicated any interest in procuring Soviet hardware, even though Peru was acquiring a great deal of it. But you have fingered a very major worry that I have, that the outcome of this crisis will be a decision on the part of the Argentine Government to embark on a substantial program of acquiring new military hardware from the Soviet Union.

I think you will find the Soviets very eager to sell at a bargain price and particularly if that means they can lower the amount of hard currency they have to spend to get access to get wheat and beef.

It is a major cause for worry in the months ahead.

The only thing that stood between that to this point has been lack of Argentine interest in turning to them as a major military supplier.

Senator CHILES. Of course with those weapons could also go the advisers, spare parts and all of the——

Admiral INMAN. Dependence.

Senator CHILES. Yes, dependence will go at the same time.

I would like ask you another followup question on an issue that greatly concerns me and a number of my colleagues in the Senate, the Soviet threat. We even had a closed session of the Senate to go into the Soviet threat. There had been a briefing by the intelligence community for many of us prior to that, but the feeling was that, because only 25 or 30 had availed themselves of that briefing, all of the Senate should have that opportunity.

For that reason we went into a closed session. That is not done very often in the Senate.

I and many of my colleagues feel that that briefing we received was so sobering. It was alarming to see the tremendous buildup, and to compare what actually happened every 5 years with what we thought would happen. We now see the Soviets achieving a momentum that would be very, very difficult for them to stop and reverse. A large portion of their GNP now is going into the war machine; it has got to make up so much of their employment. I feel that is something that should be more available to the U.S. public. There is no perception on the part of the public as to actually what that buildup is.

We are continually told that all of this is classified. My concern is: Are we going so far as to classification of this information that we are prohibiting the ability of really forming a public understanding in this country that is necessary to do something about this Soviet weapons buildup?

I wonder the way that we collect some of this information is classified. How much about those methods do the Soviets really care about now?

The information we collected is something that is available to the Soviets. But, ironically, the information is a secret from our people as opposed to being a secret from the Soviets. I understand that how we collect some of this information is classified. However, from your perspective, how are we going to be able to show this alarming buildup to the American people in sufficient detail to convince them that this is not rhetoric, that this is not one of those statements that will be discounted later? How can be made the public understand this threat?

Admiral INMAN. Senator Chiles, let me try to stumble my way through a response to that in an open, unclassified session.

Senator CHILES. I understand this.

Admiral INMAN. I happen to be a great admirer of John Hughes and of the presentation of the Soviet buildup which would help a lot of people. It was put together a number of years ago and I have watched the impact on Republican and Democratic Congressmen, Republican and Democratic administrations, and our foreign allies. It has in every instance been a very sobering presentation because of the accumulation of data before your eyes on the full scope of the buildup, the infrastructure, the building of shipyards, the building of airplane factories, the building of tank plants, the clear fact that they are using those facilities substantially less than their capacity at this point in time even when we have worried in our own defense buildup of whether we have the industrial capacity to do the job that needs to be done.

The complications in releasing that information, or in declassifying it are substantial. One is the question of the impact of the Freedom of

Information Act. If you declassify satellite information to use for that specific purpose, is all of it, thereby, open and accessible and thereby knowledge of what you targeted, how frequently you acquired it, available under the existing terms of the Freedom of Information Act.

There are considerations one must carefully take into account on national technical means of verification of treaties and the whole arms control process and if one believes that we do need an arms control track as well as the rebuilding track for our defense capabilities, then you have to think very carefully about whether you endanger continued access.

The Soviets have an antisatellite capability now. Many of the systems which provide this information are very suspectible to its use. There is the question, when do you cross over the line between that which is accepted under treaty for national technical means and when is it a challenge to the secrecy in that closed society that they are not willing to accept. But I must admit those of us who have been inclined to support the use of the imagery had a real setback a couple of months ago when we did use imagery to describe the buildup in Nicaragua and the press coverage, at least some of it the next morning talked about the claimed, alleged, reported information and it was very clear that what to John Hughes and Bobby Inman was enormously persuasive information from photointerpretation, was instantly challenged. The average man in public is not a photointerpreter, able to make their own independent judgments. If the views of the professionals are not to be accepted as credible, then I have great reservations that, taking any risks about future access is worth the cost. Indeed, it has been the credibility that John and others of us have had with these committees which I think has been a central factor in the weight that that briefing has.

So we are on the edge here of some deeper and more complex problems of the general attitude that the media brings to the validity of information provided by the Government and specifically by the intelligence community on issues. If one doesn't want to believe that there is a Soviet buildup, you can find all kinds of questions to ask to divert attention.

I am grateful for the expressions of support that have come from the members here and I have enjoyed enormously my working relationships with you over the years. Rather than saying that this is a temporary departure I would rather phrase it a different way. As I go off to my second career, I hope I am still going to be able to help in addressing a great many of these issues from the private sector.

But even there, credibility, a willingness to accept the honesty and integrity of the professionals in providing information is absolutely key to building public understanding. A very good publication was put together with a lot of hard work last year called "Soviet Military Power." It does not have all the dramatic impact that you got, that many of your colleagues have gotten, as have I, from watching the full classified briefing, but all of the essence is there in that publication.

Senator NUNN. That publication was primarily done for NATO?

Admiral INMAN. Yes, sir.

Senator NUNN. An interesting thing about that publication if I can interrupt Senator Chiles for just a moment is the overall view

was it was enormously helpful in European circles. I was over there shortly after it was put out. But there were a substantial number of critics that kept talking about the fact this was simply expressed in gross terms, this is what the Soviets had, one, two, three, four with no effort to make a net assessment, with no effort to say what the American capability was, what the NATO capability was. Of course, when you get into net assessments you are getting into subjective judgments that would take 15 or 20 years for the Department of Defense to agree on, never mind the ones that go to the National Security Council.

I know the difficulty of putting out that kind of information. There is a totally different group of people dealing with it. That is where the skepticism goes. There is a great desire on the part of the people in the media and the public, I might add, to have someone digest the American-Soviet-NATO-Warsaw Pact balance in 30 seconds or less, in one page or less.

Tell us whether we are stronger or weaker, tell us who is superior and I think that is a very fallacious kind of approach but that is what you are dealing with and that is what, of course, we are all dealing with.

Admiral INMAN. I think we have gotten enchanted in this last 20 years, at least the public debate has gotten drawn too much to charts, graphs, trying to compare everything by numbers. The systems analysts love it. I am very skeptical about the ultimate value of making judgments about need in that way. I doubt if any systems analysts would have put the Falklands or the kinds of forces one needs to impact on the Falklands in the charts or in racking up the kind of capabilities one needs to deal with the troubled world of the decade ahead.

Senator CHILES. I am sure that is true. I would say one comment I have, I see the problem which you are raising. I have a feeling if you give the American people sufficient information and detail, they won't allow the media to interpret for them. They will make their own interpretation.

Admiral INMAN. I don't want to leave any doubt at all that I believe the Soviet buildup over these last 17 years has brought us to a perilous state. That there is now vastly greater military power in the hands of a very few leaders who certainly are not chosen by public mandate than have ever been in the hands of any of the czars in the time before.

There are several components. Ultimately whether those new leaders are willing to use those military powers in ways that are directly threatening to us or our interests will lie partly on our own military forces but partly on judgments about our national will. And clearly they will become very sophisticated at looking at public debate in the United States, but I am afraid sometimes they may conclude that there is less will to deal with problems than in fact I believe exists in the country at large.

Senator CHILES. I agree, that they could miscalculate.

Admiral INMAN. Yes, sir.

Senator CHILES. Thank you.

Senator NUNN. You made reference in the past and again this morning about scientific exchanges and your desire to stimulate the aca-

demic community and scientific community to take their own action. You are about to move into the private sector. We heard over and over again about how the Soviets send middle-aged scientists over as students, we send students of Soviet history over in an exchange program. One is after technology, the other is after some form of legitimate literary or historical endeavor.

[At this point, Senator Chiles withdrew from the hearing room.]

Senator NUNN. There is nothing wrong with the latter, but what is it you would like to see the scientific and intellectual community do in this regard and I stress voluntarily without Government dictating, I am sure that is what you mean?

Admiral INMAN. Happily what I wanted to see is now underway. In anticipation that the Government was going to eventually come to grips with the major technology outflow for which there are laws that ought to be effective and organizations that ought to be effective in at least making that very difficult, it was clear that there was a segment of this outflow that was not regulated, that was not controlled and in thinking ahead, I was trying to spur the scientists into giving attention to that area themselves and coming up with thoughts about what one could voluntarily do to deal with it.

That got interpreted as proposals for censorship, for threatening to put controls in places, to try and somehow turn the intelligence community loose on academicians and other things. They were just flatly false. What I hoped to get was an honest broker in the scientific community to put together a forum to discuss the problem and come up with recommendations. The National Academy of Sciences and National Academy of Engineering are now jointly sponsoring such an effort.

It is a study group that is going to take about 12 months to deliberate the problem very carefully. They were fortunate to have gotten the former president of Cornell University to head the group. They have had one meeting. They have another one coming up in a month. They need to be left alone. They don't need a lot of people peering over their shoulders either from the Government or from the media, but I have substantial optimism based on my earlier experience that they will define areas that are of concern where there are approaches that are entirely acceptable.

There will be some grumbling, but I believe it will be possible to determine what it really impacts on the free growth and exchange of science, and to recognize things that do not impact on that, that will nonetheless let us throw some barriers in the path of the Soviets to make their acquisition harder.

I would finally make a pitch that there are some exchanges that are clearly in our national interest. We are going to need in this decade out ahead scholars and students with genuine area study capability, with language skills who can watch the actions of our adversaries and give us sound advice, whether they are working in the intelligence community as analysts or whether they are working in the Foreign Service or other parts of the Government. And so we should be cautious as we go about assessing the value of exchanges that we don't underplay the value to this country of various area studies and language training as part of the exchange structure.

Senator NUNN. In other words, you are not here advocating a new law on scientific and technological exchanges?

Admiral INMAN. I am not. I think it would be an area well serviced to stay away from for a while and see what they can develop on their own.

Senator NUNN. Thank you very much. We appreciate your cooperation. We look forward to your views on some ideas we have in the next couple of days. What is your expected departure date?

Admiral INMAN. It depends on the confirmation of Mr. McMahon. I would hope that would go smoothly without difficulty and, therefore, in early June, he will be ready to take office and I will retire.

Senator NUNN. I hope you are accessible in the future to the Congress and to those of us who have come to respect you so much for your advice and wisdom and experience. We will certainly continue to call on you as if you had never left.

Admiral INMAN. Thank you very much.

Senator NUNN. Thank you.

Our next witness is Dr. Stephen Bryen, Deputy Assistant Secretary of Defense, International Economics, Trade, and Security Policy.

Dr. Bryen, if you have other people with you this morning, if you would introduce them, if any will be answering questions we direct to you, we can have them take the oath also. Would you raise your right hand.

Do you swear the testimony you give will be the truth, the whole truth, and nothing but the truth, so help you God.

Dr. BRYEN. I do.

TESTIMONY OF DR. STEPHEN D. BRYEN, DEPUTY ASSISTANT SECRETARY OF DEFENSE, INTERNATIONAL ECONOMICS, TRADE AND SECURITY POLICY, DEPARTMENT OF DEFENSE

Senator NUNN. Dr. Bryen, we appreciate your cooperation, your office's cooperation with this subcommittee and our staff as we have undertaken a rather lengthy, detailed examination in this technology area.

[At this point, Chairman Roth withdrew from the hearing room.]

Senator NUNN. We know you have prepared testimony today and will be glad to hear from you before we begin asking questions.

Dr. BRYEN. Thank you, Mr. Chairman. I will try and summarize my testimony a bit. Since you have the full text, it can be entered into the record.

Senator NUNN. Without objection your whole text will be entered.[1]

Dr. BRYEN. I welcome the opportunity to speak with you today concerning what we in the Department of Defense believe to be a most serious national problem, the control of technology which is being transferred to the Soviet Union and its allies. My discussion will focus on what we have achieved so far, what we have now in the works, what we have yet to do. Previous testimony has gone to considerable length to illustrate the scope of the problem. It would be very difficult to estimate the real damage done to American national security by the *Bell* case, which you have already looked at.

---

[1] See p. 583 for the prepared statement of Dr. Stephen D. Bryen.

That loss consists of both military damage in making those weapons systems vulnerable to countermeasures and the cost to the taxpayers to overcome the vulnerabilities that those compromises entail. But the same kind of damage is done in more subtle ways by a variety of mechanisms that are essentially directed by the Soviet Union to the detriment of the United States.

Undoubtedly you have heard or hear in the future of those who say only by constant investments in the technology base upon which our defense is founded can the United States hope to remain ahead of its strategic adversary.

Senator NUNN. Will you pull that mike up a little. Thank you.

Dr. BRYEN. Likewise, you will hear that it is impossible to constrain knowledge and to do so, in fact, is counter to the efforts to advance the onward progress of technology. We believe it would be imprudent in the extreme to shrink from the difficult task of devising and enforcing reasonable controls to preclude the use by the Soviets of the fruits of our technological genius to destroy the very system by which it is nourished.

It is our attempt to structure within the Department of Defense, reasonable controls over technology, controls which will effectively inhibit the flow of technology contributing to the growth in Soviet military capability.

Now it is a truism there is no substitute for case-by-case review of proposed exports, legal exports. Only by careful and objective assessment of the facts of each case can the operational, technical, and precedential impact of an export be properly assessed. We have no intention whatever of eliminating this vital element of our contribution to the Government's export control of technology. However, the case-by-case approach functions best within a framework of guidelines and criteria, proven standards by which judgments can be made.

In the past, our individual judgments were made in so flexible a fashion that we were overly subject to the vagaries of the moment. The effect has generally been to advance the margins of acceptability of exports through the gradual accretion of precedential approvals, by the way encouraged to some extent by the Export Administration Act without particular regard to the basic standards by which exports should be judged—the Nation's security.

Accordingly, we are engaged in a major effort to develop in a cogent fashion, a framework of policy within which the Department of Defense can provide its advice and counsel to the ultimate licensing authorities in our Government.

My office started with four people a year ago. We have expanded since then to a staff of 12. We have intensified our role in the export review process while at the same time undertaking a major effort to objectively develop policy. I would like to share with you some of the things we have done to date and I would like to solicit your suggestions for our future efforts.

First, an augmentation team composed of representatives of the military services has been assigned to my office and is preparing for the Secretary of Defense's signature a policy statement on control of technology transfer. This, we hope, will replace and improve a 1977 interim policy that is signed by Secretary of Defense Brown.

We hope that our new policy will reflect several changes that have occurred since 1977. One of the most important ones being the enactment of the 1979 Export Administration Act. This is the basic role under which we today operate.

In addition, this team is providing management assistance to my office in three basic forms.

The first of these is technical assistance to automate some of the routine administrative tasks involved in determining policy and processing cases. The second is to assist the integration of existing data bases used in routine case processing. And the third is the creation of a central library to provide the basic documents required for developing policy.

This subcommittee should know a year ago when I came on board, there were not available coherent records on past DOD determinations, or for that matter any determinations by previous administrations, nor was there any single source to appraise the result of past activity. And we are slowly correcting this deficiency. It takes time because we have to reconstruct records and try and determine exactly what has gone forward in the past and to base our new judgments on those records as best we can.

We are also working very hard to train our people, to develop rigorous standards and try to follow more disciplined procedures as possible.

In the long run, I think these efforts will pay off in that we will develop a solid core of professionals who will understand as best they can the problem and will work in a consistent and predictable way.

If we can do this in the Department of Defense, we have to do it in a broader way with the public, with the business community and with our allies and friends abroad and to further this effort, we have undertaken with our augmentation team the development of a white paper on this entire subject of technology transfer, which we hope will be published this summer.

The goals of the paper are to detail the importance of dual-use technology to our defense support industries, promote as much as we can a voluntary compliance with the export process and we hope to secure support for and assistance in developing methods which more closely review defense-related technology proposed for export.

The paper will attempt to present the roles and contributions of both our Department, State, Commerce, Treasury, and Justice, and the Bureau of Customs.

Another major effort is our attempt to work closely with both State and Commerce and seeking to strengthen strategic trade controls in Cocom, the coordinating committee, and thus to stem the flow of Western technology to the Soviet Union and its allies. As you know, Cocom is an informal nontreaty organization established in the early 1950's. It is comprised of the NATO countries, less Iceland, but it does include Japan, a very important member. It has, however, no formal link to NATO.

Senator NUNN. Is there a case to be made that there should be a more formal relationship with NATO or would that be a negative kind of development?

Dr. BRYEN. There is a good case to be made for it. I think the problem is a political problem in that Japan is a member of Cocom, of

95-929 O - 82 - 17

course does not view itself in the NATO system. Under those circumstances, those institutions will probably have to remain separate.

Senator NUNN. Does NATO have a way of getting its input in through the various Department of Defense inputs and the respective NATO countries?

Dr. BRYEN. You just put your finger on the very major issue and problem and one we have been working very hard on. If I can step away from my testimony, maybe I can try and elaborate on it a bit.

In the past, with the exception of the United States and to a lesser extent Great Britain, defense ministries, surprisingly played a very minor role in the technology control business. Surprisingly because the whole point of the effort is to deny strategic technology to our adversary. Our tradition was just very different from the tradition of our European colleagues and Japan as well.

What we have been trying to do is to turn that around and develop far more participation by defense ministries abroad in this entire process. We have gone to achieve this objective through two routes.

One is through Cocom. We have not achieved this yet but we have asked for a military subcommittee in Cocom to meet on a regular basis where military experts from different participating countries could get together, exchange information, evaluate proposals for export based on the strategic implications both for the individual countries and for the collective defense effort. As I said, we didn't get that. We did get agreement to expand use of Cocom to include military experts which we considered a step forward.

On a separate track, we have, and this is very much Mr. Weinberger's recommendation which was approved by NATO, undertaken a study within NATO of the whole impact of technology transfer on the NATO military missions. The purpose was twofold. First, we have tried often enough to relate the impact of technology transfer on America's national defense programs, but not so much how that cut into our allies programs. So it is a very ambitious effort and we have gone through the first 6 months of it now and quite successfully.

Second, it brings together defense ministry participants to consider the study of technology transfer and to take that information back home to their own governments.

The next point is, how do you get from NATO to Cocom?

Senator NUNN. So there is an effort to get NATO to begin considering this as a body.

Dr. BRYEN. Yes. It is more than an effort to begin. They are doing it. It will continue. I have learned that just today. We are very enthusiastic about it. We think it will be very helpful to all of us. It will create the kind of interrelationship and understanding that we need in other governments to get this job done.

Senator NUNN. Is that going to be a standing group in NATO?

Dr. BRYEN. We have asked that it be a standing group.

Senator NUNN. Of people that will be responsible for that and will get input from their own ministries.

Dr. BRYEN. That is how it has worked so far and that is how we want it to work in the future.

Senator NUNN. Then bring it up to the NATO representative level?

Dr. BRYEN. That is right. Again it was largely at the suggestion of

Secretary Weinberger that we undertook this effort. We supported it very fully. I must tell you that we had many barriers to cross to get the basic themes agreed on.

One of the aspects of this whole problem is that people didn't do this kind of analysis in the past, either here or anywhere else. When I came a year ago to this job and asked how technology transfer impacted military programs, there was very little available.

It wasn't that the evidence wasn't in the system. No one was putting it together and really attempting to evaluate it and do the right kind of impact study. We have done a good deal of that. We have got a lot more to do.

Senator NUNN. What are you going to call that standing group in NATO?

Dr. BRYEN. So far it has been called by the brilliant name AC 314 which means nothing at all, but it will be called the Technology Transfer Group as it has been known colloquially among those of us who have worked on the issue.

Senator NUNN. That sounds suspicious and covert enough to get it some attention.

Dr. BRYEN. We think it has already gotten some attention. It has been a process. We expect it to be a process. I must say that we have had excellent support among all our agencies who help us get the job done at NATO.

Senator NUNN. You were going to say that once NATO gets to be cognizant of the problem and a working group, what do they do to feed into Cocom?

Dr. BRYEN. Principally NATO will feed into the governments but what we want to see, obviously, is far more defense participation in the Cocom study as well and in each nation, a chance for the defense ministries to review proposals for export before they occur.

There has been one very positive development in that regard, if I can mention it today because I think it is an important contribution. This was the decision by the French Government to give its defense ministry a role quite similar to the one we play here.

We believe it has had a very positive result already and it has helped a great deal. We are very grateful for that step by the Mitterand government.

I was talking about Cocom and let me just elaborate one step further. This administration asked for it. It was actually the President last year at the Ottawa meeting who asked for a high level meeting of Cocom to see if we could strengthen the organization, to see if we could give it a new strategic purpose.

His request was accepted, a high level meeting occurred last January, and I think an important start was made in terms of reaching a concord with our allies on those items that we need to control and why we need to control them.

We are now in the process of following up that initial high level Cocom meeting—by the way, the first one in nearly 30 years, which gives you an idea of the problem right there. Now the issue is to get specific proposals adopted. In that connection we had a handful of very high priority, what we call quick fix, proposals which we will be presenting in June in Paris at the Cocom meeting.

We have every anticipation that these proposals will be accepted and we think they will go a long way to plugging some of the gaps and loopholes in the system that have persisted for some time.

Beyond that, we have a major list review coming up in the fall which will try to go even more broadly into areas where coverage by Cocom has been less than adequate.

I am skipping ahead because I have already covered the NATO and Cocom parts of the testimony.

I do want to mention, I think Mike Lorenzo this morning and Admiral Inman mentioned it, but a point that we feel very strongly about in the Defense Department, and which the administration feels very strongly about, and that is improving enforcement of both the legal and illegal transfers of technology.

There are two dynamics to the enforcement process, the domestic one and again the international one.

At the international level, one of the conclusions of the high level meeting was to explore how enforcement could be strengthened in Europe and in Japan.

We expect specific measures to be shortly negotiated at Cocom and we are looking forward to see the national implementation of that effort.

For our own part, Defense itself doesn't exactly participate directly in enforcement. We try to support our enforcement people with a number of efforts. One of them is to try to target and identify areas, sensitive areas where we think a special emphasis should be made by the enforcement people, whether it is the Customs people, Justice or people of Commerce.

A second one is to try to help our own Customs officials better identify materials and equipment that are embargoed. It is not a simple thing, not today, in the age of Atari and Pac-Man.

The Customs effort has been stepped up as you have already been told, I am sure. Behind that we are trying to provide the supporting assistance. We call it a "mushroom book." It is to give our Customs officials a fast and useful way to precisely identify the materials they are looking at.

Senator NUNN. Where did you get the name "mushroom book"?

Dr. BRYEN. I don't know, myself. I suspect it was in the discussions we had with the Customs people as we explored this idea in the initial phase. There was a suggestion made and we took it. Whether it applies to mushrooms hiding under, in a dark place, I suspect that is where it comes from. But once you adopt the term, well, it is somewhat like the plastic palace in the Senate.

Once the name is assigned, people forget why.

Let me deal with one final aspect, if I may, and then I will get to the questioning stage.

One of the things we can do in the Department of Defense, one of the efforts that I have taken a lot of responsibility for, because I think it is so important, is better management of our own technology.

The program that I started with and one that is very important to us in the future is the very-high-speed integrated circuit program. The VHSIC program has very great prominence for our military systems because it will enable us to improve existing systems and develop new ones with far greater capability.

The VHSIC product will be used in advanced-signal processing applications for weapons systems, electronic warfare, communications, radar, precisely guiding munitions.

It will enable us to do these things at a lower cost, we think; it will be smaller in size, with greater power than anything we currently possess.

Obviously, the protection of this technology is of highest priority. Congress, when it authorized the VHSIC program asked that we make efforts to protect VHSIC.

To date, a full system of controls has not been implemented and I think regrettably so. The task force I am heading now is designed to try to remedy this situation, to get this program under a system of control.

Part of it involves putting VHSIC under the ITAR, the international traffic and arms regulations, as the Congress intended. We are working with the State Department which has the authority and we believe we will soon accomplish this goal.

Our immediate task is to protect the technical data, the military hardware that is now being developed, before it is too late to prevent the dissemination of these technologies to our adversaries.

In addition to putting the VHSIC under the ITAR, we have to also deal with the problem of the wide amount of literature that has already been out on VHSIC, some of it covering the circuit design, some of it covering the hardware associated with the program, some of it covering the software.

Neither the ITAR nor the export regulations really will protect this kind of data from compromise. I don't need to tell you about the Freedom of Information Act.

Senator NUNN. Do you know of any reason why people other than American citizens or people who are legally in this country should be given access to the Freedom of Information Act?

Is there any reason why the Freedom of Information Act should be as broad as to allow foreign citizens to obtain information just as if they were American citizens?

Dr. BRYEN. That is a question you probably ought to ask the Justice Department specialists. I am not an attorney and I won't make any effort to explain it.

It occurs to me though that one of the things that we want, of course, when we are abroad is some reciprocal protection of rights. So one has to be a bit cautious in this area. But so long as we publish materials we have to expect, I think, that one way or another they are an open resource for anyone that wants to get their hands on it. We have proposed, as you know, special kinds of classification called restrictive.

Frankly, sir, I think the answer is a very careful attempt on our side to classify what we think really is important and what we are going through now, 2 years later, I am afraid to say, but we are still going through the process, is trying to find those forthcoming aspects of this program that, if we can protect, we can thereby protect the whole program.

We are making a major effort in that regard. We hope that this exercise in fact will be a prototype for control of other Department of Defense programs both in the emerging technologies field and to a

certain extent in more mature areas, where design, where circuit design, where specifications information, really tells the tale to the adversary.

It is a tough thing but it is one we regard as very important.

I think those are the main points I wanted to touch on this morning. I have some testimony about the Siberian pipeline. We have expressed concern and we continue to express concern about that because of the increment in hard currency earnings capability over a 25-year period at least that will accrue to the Soviet Union.

It will give them far more economic clout than they may now have. It will enable them, I am afraid, to have even greater access to the technology which we are trying to protect.

Admiral Inman did a superb job of describing the problem for you, both in the broad brush sense and in the narrow sense.

It is a terribly important issue. It is one that the administration is taking very seriously. It is one that we have to be successful in.

I cannot in confidence at this moment predict that we are going to be successful but I think what we need is a period of time to try out the effort on an organized basis.

I think we need 5 years minimum before we are going to see real impact of the mature technology effort. We need our allies to cooperate. We are working hard on that. We are going to need more resources to do the job. We have already put Congress on notice about that. We need to do some things in our own house to operate more effectively, to try to take those steps. We are to a certain extent feeling our way along.

Senator NUNN. Do you generally agree with the suggestion that has been made that the most effective way to control technology, know-how, small, very small sophisticated electronic computer equipment, and so forth, is to try to control it at the source with the Government-to-business education program rather than control it as it is going out of the country? I am not saying you don't try both, but I am saying which is the most efficient, which is the one that ought to be given the highest priority?

Dr. BRYEN. I guess it harkens back to the Bucy report, in respect that what you want to watch most of all is the manufacturing technology. That is the piece of it that hurts you the most. I put all of my—not all, but a great deal of my emphasis right there. I would be better off giving you an example rather than trying to speak generally.

In the microelectronics area, there is a small amount of very specialized equipment that enables you to make microelectronics.

A lot of that equipment is made in this country. Some of it is made under license abroad. Very little is entirely independent of what we develop ourselves. If we can control that manufacturing technology and the design technology that goes with it, we may have a good shot at certainly inhibiting very substantially Soviet efforts to acquire it. It is also one of the areas we simply failed to inhibit in the early phase. But we can do it. It is a last resort to track it on the way out but it has a very valuable impact.

Senator NUNN. You need to do all the ways but, it seems to me your most effective enforcement is through a dialog with industry.

Dr. BRYEN. We are doing that. In fact, we just had in representatives of the Semi-Conductor Industry Association.

One of the things we wanted to do was be as direct with them as we could. So we granted special clearances so there would be no holds barred. We got that done. We went through an entire briefing. Then we heard from them. They have some problems, too.

Senator NUNN. Do you do that on a one-on-one basis or do you do it in trade association seminars?

Dr. BRYEN. This was with a trade association, but it was one of the most senior representatives of the trade association. It was very much a prototype of a broader effort we want to undertake.

Senator NUNN. The FBI has a similar program and I am sure that theirs doesn't get into as much technicality as yours does in terms of details but they, I think, are going around alerting businesses to various covert and overt means of Soviet operations. Do you coordinate with the FBI?

Dr. BRYEN. We do.

Senator NUNN. Do you sit down and discuss it, talk about who is going to do what?

Dr. BRYEN. We have a group headed by Gus White at the White House that discusses all of these issues and we square off on these programs. But our effort was really designed to highlight for semiconductor industry people how they have, inadvertently, I might say, been contributing to Soviet military capability.

It was a very elaborate presentation, but I think a very sobering one. It is something we cannot do out in public. We felt we ought to experiment with this and see if it would help them to understand our problem, the national problem, and at the same time to develop some suggestions.

One of the things we would very much like to see security committees in our own sensitive industries, policed by the industry itself. Some of our industries are not known for their internal security.

Senator NUNN. You mentioned in your statement that you were replacing the 1977 interim policy of DOD for export control. What is the reason for replacing that?

Dr. BRYEN. We think, if you read the 1977 statement, I happen to have a copy with me, that it is basically an apple pie kind of description of what we should be doing. The problem is that it apparently had very little genuine effect either in the Department of Defense or in the interrelationship of the Department with other agencies.

It was too general. It needs more precision. We liked the part of that statement that keys on what is called the Bucy report, which I am sure you heard of already in discussions, the notion of aiming at the critical manufacturing technologies. But it doesn't get very far beyond that. It doesn't set out the marching orders in the Department clearly. So we are doing a front to back scrub of the whole thing. We hope to make it more precise so that it makes clear what ones' responsibilities, duties and roles are. That is the purpose.

Senator NUNN. What is our recourse if there is a controlled technology on the Cocom list and it is, let's say, transferred by one of the Cocom nations to the Eastern bloc. Do we have any recourse under Cocom or is it just a complaint mechanism?

Dr. BRYEN. Cocom is only a voluntary organization.

Senator NUNN. There are no sanctions involved?

Dr. BRYEN. There is no sanction in Cocom. But obviously we have to pace our cooperation with others on their overall performance, and technology transfer is an issue of significant enough importance to this administration that we are actually doing that.

It is a painful process. It is not one that I want to talk in open session about. But it is one we are very much engaged in and I think to the betterment of the whole effort.

Senator NUNN. You mentioned that certain technologies can only be adequately protected by national security classification. Are you saying there is nothing in between, either it is classified or not, if it is not classified, it is out there, available and that is it?

Dr. BRYEN. That is pretty much the case.

Senator NUNN. Would there be any need, desire or merit in trying to find something in between that would not be classified but would be labeled crucial technology or would that simply be too cumbersome to get involved in?

Dr. BRYEN. I think you put a big flag on it.

Senator NUNN. It ought to be classified or not classified?

Dr. BRYEN. Yes; I think parts of it have to be classified. It is a management thing as much as it is a security matter.

Senator NUNN. But can you classify dual use technology? Can defense classify technology——

Dr. BRYEN. We cannot classify what we don't know, but we own some things that we haven't classified.

What we need to do is look at our own house. That is what we are doing, and we say, are we being careful enough in protecting this program? That is the purpose of the VHSIC inquiry and I hope that we can expand that further in the future.

We are always accused of overclassifying things as a matter of course.

Believe it or not, there was not a great tradition in the Department of Defense to manage technology development programs from the point of view of security precautions. That is the thing we have to take a much more careful look at and we are.

Senator NUNN. In your statement you refer to the small industry that has risen in Washington composed of individuals who know how to play the system within the export control community. What do you mean by this?

Dr. BRYEN. What I mean by that are people who have become expert on the export control process, they know where the soft spots are, know how to characterize items in ways that make them sound perfectly nice and harmless and they are good at it.

I don't want to get into the moral issues about it. It is to be anticipated. It is an interesting point. On the whole we have little trade with the Soviet Union. When you take away grain, it is not all that much. Even our European partners don't do that much trade. Sometimes these issues are cast as if the economy is going to come to a halt if we stop the transfer of a certain item.

It is very rarely really the case. Of course, one of the things the Soviets have become quite good at is exploiting sick high-technology industries, industries that are cash short, need money, need R. & D. funds, whatever; they look for those companies because they are easy targets.

Senator NUNN. What specifically is your office doing to coordinate with the law enforcement community? You mentioned the mushroom book. Is that the main effort going on?

Dr. BRYEN. That is the main effort we have underway. The other way we coordinate—but what we try to do on a regular basis is to make known to, the State Department, that is where most of the action is, our concern about specific areas, so we can bring those to the attention of other foreign governments. We don't ourselves have a mandate for enforcement.

Senator NUNN. We have heard testimony the United States has indicted at least three West German nationals for violations of the Arms Export Control Act. These individuals are now fugitives and free men in West Germany, a Cocom nation. Is there any effort within the Government to make these offenses extraditable offenses?

Dr. BRYEN. I can't answer on the extraditable offenses. There is an effort to try and get our European allies to upgrade their entire legal structure. Here in the United States it is a felony to be involved in transferring the technology. In European countries, it is a misdemeanor at best. People calculate the cost. How much fine there is against the how much profit there is?

That is the wrong way to go about it. You need some positive disincentives and jail terms, or something severe like that. That is why we come back to your earlier question, that of customs catching these things and then making sure Commerce follows up. It is a very impressive way to get people to understand export controls.

Senator NUNN. We heard testimony from William Holden Bell, former Hughes Aircraft executive, who sold secret military information to Polish agents. He testified last week. How serious a security breach, in your opinion, was there in the *Bell* case?

Dr. BRYEN. I wouldn't comment on that except to say it was serious, but I wouldn't want to comment in open session. I think we can provide you in closed session with a real evaluation. That is not the kind of evaluation to make in public.

Senator NUNN. We may very well.

Dr. Bryen, you made reference in your testimony to the effort by the Soviets to build and equip a semiconductor plant using equivalent know-how from the United States.

Could the Soviets have built and equipped such a plant in the late 1970's and early 1980's without U.S. machinery, equipment and know how?

Dr. BRYEN. My answer is they could not. That doesn't mean that equipment necessarily came from this country. It could have been transferred from Europe or elsewhere. In fact, it could have been transferred from another country that bought that equipment—it could have been on the secondary market. There is a secondary market in this sort of machinery. These are terribly difficult things to trace.

What we know in the first instance is that a lot had to be U.S. equipment, that the system was full of holes, it was porous, it was easy for them to get it and they got it.

The microelectronics area has enabled the Soviets to upgrade their military equipment. Again, in my testimony, there is a kind of ques-

tion and commentary about where all this leads. I think where it leads is that we risk losing the quality edge on which our entire structure of national defense and alliance depends. I don't think we can afford to take that risk. I think there are things we can do to protect it.

This is why we are making this effort and we very much appreciate your support, the support of this subcommittee and the support of the Congress.

Senator NUNN. Thank you, very much. We look forward to bouncing some of our ideas off you and your people in the next week or so.

Thank you, very much.

Our final hearing on this subject in open session will be tomorrow morning at 10 o'clock in this room.

[Whereupon at 12:05 p.m., the subcommittee recessed, to reconvene at 10:05 a.m., Wednesday, May 12, 1982.]

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

WEDNESDAY, MAY 12, 1982

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met at 10:05 a.m., in room 3302, Dirksen Senate Office Building, under authority of Senate Resolution 361, dated March 5, 1980, Hon. Sam Nunn presiding.

Members of the subcommittee present: Senator William V. Roth, Jr., Republican, Delaware; Senator Sam Nunn, Democrat, Georgia; and Senator Warren B. Rudman, Republican, New Hampshire.

Members of the professional staff present: S. Cass Weiland, chief counsel; Michael C. Eberhardt, deputy chief counsel; Eleanore Hill, chief counsel to the minority; Kathy Bidden, chief clerk; Gregory Baldwin, assistant counsel to the minority; Jack Key, Glenn Fry, and Fred Asselin, staff investigators to the minority; and Kathleen Dias, executive secretary to the minority chief counsel.

[Senator present at time of convening: Senator Nunn.]

[The letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive hearings without a quorum of two members for the administration of oaths and taking testimony in connection with hearings on the Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations, to be held May 4, 5, 6, 11 and 12, 1982.

WILLIAM V. ROTH, JR.,
Chairman.

SAM NUNN,
Ranking Minority Member.

Senator NUNN. We have just seen a vote go up on the board. This matter has been debated for a couple of days. It makes more sense to have the votes. I will be back in 10 minutes.

Senator Roth is over there voting now. We will start the hearings in approximately 10 to 15 minutes.

[Brief recess.]

[Senator present at time of recess: Senator Nunn.]

[Senators present at time of reconvening: Senators Nunn and Rudman.]

Senator RUDMAN. The Permanent Subcommittee on Investigations is now in session.

The first witness in the continuation of these hearings on Transfer of U.S. Technology is Lawrence J. Brady, Assistant Secretary of Commerce for Trade Administration, U.S. Department of Commerce.

Mr. Brady, we welcome you here this morning.

Lawrence J. Brady is a personal friend, a New Hampshire native, and I am particularly glad to have you here.

My colleague, Senator Nunn, of Georgia, has been the moving force behind these hearings and I will ask Senator Nunn if he has any opening remarks this morning.

Senator NUNN. No; we are delighted to have Mr. Brady here.

The only thing I say to Mr. Brady before he starts, how long have you been on your present job?

Mr. BRADY. I was sworn in in June of last year.

Senator NUNN. I want to make it clear to you and everyone that the problems we are outlining about the Commerce Department and the Compliance Division are directed at not just this administration, but the previous administration and the administration before that. This is a longstanding problem and has no partisan origin and no partisan conclusion. It certainly does not relate to you because a good many things we are talking about have been ongoing problems. We are afraid they are still ongoing, but we will hear from you on that subject when we get into questions.

Senator RUDMAN. We have a practice here before the permanent subcommittee of swearing in all witnesses. Please rise and raise your right hand.

Do you swear the testimony you are about to give in the course of this hearing shall be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. BRADY. I do.

TESTIMONY OF LAWRENCE J. BRADY, ASSISTANT SECRETARY OF COMMERCE FOR TRADE ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Senator RUDMAN. Mr. Brady, your entire statement will be put in the record, and you may summarize it or handle it in any way you are comfortable with it.[1]

Mr. BRADY. Mr. Chairman, I would like the written statement I have provided the subcommittee to be inserted in the record. I would like to summarize the statement which I think puts this entire problem into focus.

First, I would like to commend the subcommittee for the work it has done in this area. I think one of the problems we have in dealing with the whole technology transfer problem is one of public awareness. And although we have some reservations about some aspect about the minority staff report, these hearings certainly will have the result of focusing the public's attention, the business community's attention on the problem. And I think that is a very positive step.

[At this point Senator Roth entered the hearing room.]

---

[1] See p. 596 for the prepared statement of Lawrence J. Brady.

Mr. BRADY. Mr. Chairman, it is a privilege for me to be here again. I have testified before this subcommittee previously. As a matter of fact, it is 3 years ago this month that I testified over on the House side before the House Armed Services Committee in which I disagreed with the political appointees of the Carter administration and indicated that the technology which we were licensing to the Soviet Union, specifically for the Kama River plant, was being diverted to the Soviet military. It is 10 years ago this month that the President of the United States inaugurated the era of détente with a trip to Moscow.

A central component of that historic trip was the hope that greatly expanded trade ties between the East and the West would lead to mutual cooperation and understanding.

Obviously, those hopes have not taken place. In that 10-year period, as we in the administration have indicated in the last year, we have been exploited both legally and illegally by the Soviet Union and Eastern Europe. This technology which has helped the Soviets immensely in their military-industrial infrastructure. Again, 3 years ago, I personally disclosed the failures of the Commerce Department in the licensing process, referring to it, as I said in my testimony, as a shambles.

It is only now that as a nation we are beginning to understand the extent of these technology transfers during the past decade. Stopping the extensive acquisition by the Soviets of sensitive, dual-use Western technology in the ways that are both effective and appropriate in our open society is one of the most complex and urgent issues facing all of us.

Moreover, Mr. Chairman, only now are we beginning to recognize that the technology transfer issue is much more than simply an enforcement problem. Apart from strengthening enforcement, in order to deal successfully with the increasing Soviet effort to acquire advanced Western technology, we need to do a number of things.

First, we need to understand what technology the Soviets need; how such acquisition has helped the Soviet Union achieve its goal of military superiority and what methods the U.S.S.R. is using to obtain it; second, on a multilateral basis, we need to marshall the support and the commitment of our allies to prevent further technology leakage to the Soviet Union by Western concerns and by U.S. subsidiaries and licensees operating abroad; third, we must build up our counterintelligence efforts to counteract the Soviet intelligence organization; fourth, we must work closely with industry segments involved in the development and production of high technology to assess ways of retarding the growing industrial security problem; and examine all possible avenues for identifying and protecting defense-sensitive technologies, including technical documents which are not now subject to our classification system.

Strategically, we need to recognize that the U.S.S.R. is far more powerful militarily than the nation we faced at the end of World War II, when these controls were first put in place, and it is far more capable of procuring and applying our latest technological advances.

However, we in the administration, within the last year, could not take adequate protective action until we accurately assessed the na-

ture of that threat. Therefore, one of the first actions taken by this administration was to request the intelligence agencies to prepare a comprehensive analysis of Soviet technology acquisition methods.

Not until the fall of 1981, when we started to receive these analyses, did we begin to appreciate the magnitude of the Soviet's activities against the West. In April of this year, the CIA released the unclassified version of its report, "Soviet Acquisition of Western Technology," which verified the fact that the U.S.S.R.'s efforts were massive and planned at the highest level of government, including the KGB and the military.

It now appears that the U.S.S.R. is placing greater emphasis on the procurement of production equipment technology as opposed to actual weapons designs in some cases.

The commercial sector, which is generally not adequately protected against penetration by hostile intelligence services, is being targeted.

Industrial espionage has become one of the most productive areas for Soviet and East European intelligence services. We anticipate greatly enhanced activity in the years to come with regard to heavy technology, energy, chemicals, microelectronics, computers, and lasers. The list goes on.

Revolutionary advances in technology and the structure of business enterprises have also created formidable new obstacles for our efforts to regulate strategic trade with the Warsaw Pact.

The rate at which new technologies are conceived and applied to industrial processes continues to accelerate. We are in the midst of perhaps the most rapid period of technological advancement in many years.

The private sector has now risen to prominence in technology leadership, with Government following behind. Leading-edge technology, once primarily generated by the military, is now frequently developed first in the civilian sector. It has thus become more difficult for national governments to control the dissemination of technology to foreign recipients.

Identification and protection of new and emerging technology remains one of our toughest challenges.

At the same time, the rise of the multinational corporations, combined with the speed of modern communications and transportation, has intensified the proliferation of advanced technology. Overseas, corporate acquisitions, joint ventures, manufacturing associations, cross licensing, and multinational data communications transfers all make the task of national enforcement more difficult.

We also discovered that third country diversions constitute the largest source of illegal transfers to controlled destinations, far exceeding the number of illegal shipments from the United States. It therefore became obvious that the magnitude and the international scope of the technology leakage far exceeds our previous assessments.

Mr. Chairman, this administration, even prior to taking office, was acutely aware of the technology transfer problem. The President certainly was and expressed his feeling during the course of the campaign. In the months since assuming office, we have moved systematically to ascertain the threat posed by this leakage, to ascertain how the Soviets and East Europeans are working to acquire Western technology and finally to take remedial actions to deal with this matter.

We recognize the magnitude of the whole technology transfer problem and pertinent Federal agencies are working closely with the intelligence community and industry.

Since the major part of the technology transfer problem is international, we turned our attention to that aspect first. We examined the effectiveness of the multilateral controls because of the technological advances archieved in Communist countries: It was evident that Cocom had become obsolete. This administration concluded that while Cocom prevented many sensitive exports which would have contributed significantly to the military capabilities of countries, such as sophisticated computers, it was still far from being totally effective.

We identified the major reasons for this. One, the limited scope and concept of the control list. Weaknesses in the multilateral enforcement, the availability of goods from non-Cocom countries and inconsistencies in licensing procedures among Cocom member countries.

Having identified these problem areas, President Reagan, at the Ottawa Summit in 1981, made a personal appeal to the leaders of Europe, Canada, and Japan to join with us to tighten export controls and prevent illegal exports.

As a result, the Cocom high-level meeting, the first in 25 years, took place in January of this year. Commerce played a key role both at that meeting and in serving as a central agency for the preparation of the materials for the U.S. delegation.

We are now actively following up on the political commitment achieved among the allies at that meeting. Several bilateral meetings have been held to discuss specific technical proposals. In addition, a Cocom subcommittee meeting will be held in Paris soon to review ways of improving the enforcement on a multilateral basis based on the commitments we received in January and based on the work done since then.

On another equally critical front, we have been actively engaged in bilateral discussions with our European allies to discuss the need to restrict Government-subsidized credits.

The Western countries have been pursuing a policy of competing among themselves, to provide efficiently subsidized or guaranteed credits to the U.S.S.R. These were going into a country that would otherwise at least be required to pay commercial or above commercial rates for credits.

These concessional credits shield the U.S.S.R. from the realities of the marketplace and allow them to pursue their military buildup. Another bilateral mission headed by Under Secretary Buckley is scheduled for next week to pursue further negotiations on this topic.

Also, another technology transfer issue this administration is concerned about is preventing the dissemination of sensitive, technical data and know-how through academic institutions.

Since 1971, the number of academic exchanges between the United States and the Soviet bloc countries quickly multiplied. On close examination of these agreements, it is this administration's view that exchanges we have had with the U.S.S.R. and its satellites have not in the main been reciprocal. Rather, it is apparent the Soviets exploited scientific exchanges as well as a variety of other means in a highly orchestrated, centrally directed effort aimed at gathering the technical information required to enhance military posture. In the area of schol-

arly exchanges, for example, the United States sends young masters and doctoral students to study the humanities. On the other hand, the Soviets send the equivalent of a Ph. D. to study the hard sciences.

In recognition of the serious technological drain occurring in the academic arena, Commerce is clarifying the technical data regulations to provide our scientific and academic communities with better guidance and export responsibility in this area.

We are currently reviewing this issue with other agencies, including the Departments of Defense, Justice, and State, to be sure the balance between important constitutional freedoms and legitimate national security interests is maintained.

In order to control technology transfers, this administration has further identified the critical need for Commerce to have available information and technological capabilities in both the free world and the Communist countries.

Acting on the recommendation of three independent contractors to establish within the Office of Export Administration a data base in order to assess foreign availability in conformity with the Export Administration Act of 1979, Commerce is in the process of developing research and analytical capability within OEA under a foreign technical assessment center.

In addition to analyzing foreign availability within a free world, we are also strengthening our capability to assess Communist-held technologies through the increased support in the intelligence community.

On the enforcement side, I have established a special analytical unit within the Office of Export Administration, which is staffed by both Customs and Commerce employees. This special unit has developed an innovative intelligence approach that relates the application of export licenses and analysis techniques to Commerce's license application files.

The analyses produced to date have been outstanding in identifying firms engaged in diverting critical technology to the Soviet Union and in pinpointing new diversion routes.

This intelligence is also being used to develop profiles for the Exodus inspection teams, and as a basis for major criminal investigations of Soviet diversions.

Our joint efforts with customs in this area have been described by other law enforcement officials as one of the most cooperative and productive relationships that they have witnessed in recent years.

Let me say, Mr. Chairman, that this partnership, which is an invaluable step for the enhanced enforcement efforts, resulted in large part from the enthusiastic backing of Commissioner Von Raab. The continued support for this cooperative relationship between Customs and Commerce will lay a cornerstone for future enforcement with the intelligence community as a whole. Customs has upgraded the inspection effort, and I am pleased to announce today a real organizational realinement and enhancement of the Compliance Division. The division itself is being elevated to the Office status, and together with the Office of Anti-Boycott Compliance, will comprise a new export enforcement organization in the Department of Commerce that will be headed by a Deputy Assistant Secretary reporting directly to me. The candidate we have selected for that post, Ted Wu, is currently an assistant U.S. attorney for the central district of California. He is a celebrated ex-

pert in the law enforcement community. His successful prosecutions of two of this country's most notorious export diversion cases render him highly qualified for this considerable undertaking.

Mr. Chairman, Mr. Wu has accepted this position because he knows we are strongly committed to enhancing Commerce's enforcement effort. Among the many changes Mr. Wu will oversee in the enhancement of the Compliance Office will be the creation of an in-house training program for our agents. This training program will feature not only instruction of conventional law enforcement such as surveillance techniques, but will also include development of skills associated with the carrying of weapons, arrest, and seizure search capabilities. We look forward to the near future when we will have an enforcement office operating at maximum efficiency with no shortages of manpower and resources.

I might interject, Mr. Chairman, at this point, both Secretary Baldrige and Under Secretary Olmer have indicated a thorough commitment to support whatever manpower resources are necessary to do the job.

I anticipate, Mr. Chairman, that once Mr. Wu has taken office, he will be happy to report to you on the achievements of Commerce's new Enforcement Office.

In sum, I believe that we have a sensible, ambitious program to upgrade and rehabilitate our enforcement responsibilities mandated by the Export Administration Act.

Our Enforcement Office will remain what it should be, a lean, efficient organization with no other continuing mission than the enforcement of the Export Administration Act. It will be well coordinated with the intelligence community and other enforcement agencies, such as the FBI and customs; it will also be able to utilize the invaluable benefits of Commerce's close relationship with the business sector.

Mr. Chairman, Senators, I will be happy to answer your questions.

Chairman ROTH [presiding]. Thank you, Mr. Brady.

Mr. Brady, the members of the subcommittee are, of course, aware of your personal commitment to this important area but I believe it is important that the record reflect fully your position on the specific question of export technology and particularly reference the efforts some years ago to help the Soviet Union construct some trucking facilities.

Would you, for the purposes of the record, explain your role in this matter?

Mr. BRADY. Mr. Chairman, about 3 years ago, the Export Administration Act was up for review for extension. As part of that review, the House Armed Services Committee decided that it was going to hold hearings on that extension, in addition to the committee of appropriate jurisdiction, namely, the Foreign Affairs Committee on the House side.

There were some statements being made on both sides in Congress that were not totally consistent with the facts. We had intelligence information that trucks were being produced at the Kama River plant for the Soviet military and, in fact, being distributed to Eastern Europe for use in East European endeavors.

An administration witness was asked about that and denied it. I was asked about it and confirmed it. And, as a result of that, I was labeled a whistleblower and eventually left the Department of Commerce.

95-929 O - 82 - 18

In point of fact, that was the tip of the iceberg. There had been apparently intelligence through the 1970's, particularly the latter half of the seventies, indicating that there was substantial diversion taking place. I think some of the hearings this committee held in 1980 and some of the hearings Senator Byrd held in another committee indicated that, for some reason, that intelligence just didn't get to the top.

So that was my role. I eventually had to leave Government for it.

Senator NUNN. In February 1980, you recommended the creation of an Office of Strategic Trade to both license high technology exports but also provide the compliance function. Do you still believe that such an office should be created?

Mr. BRADY. I think I would like to make two points, Mr. Chairman.

One, I strongly believe that there must be an enforcement arm with the licensing function, associated with the licensing function. It should not duplicate Customs, it should not duplicate the FBI. There must be a lean, efficient organization that coordinates the intelligence information procured from the agencies with the day-to-day impact, communications, dialog, that the Department or the licensing function has with the business community. They must be together.

Now, specifically with regard to where that entire function should be lodged. In 1980, the Carter administration, an administration that, although some individuals had indicated very serious concern with technology licensing, such as Dr. Brzezinski and his military attaché, General Odem, as concerned as it should have been with the technology transfer issue and, to a certain extent, the President's directives were not being implemented. It is actually in that cross fire that I got involved. So I felt in 1980 that this function could not be administered by the Department of Commerce, because it was unwilling to give it the attention and the resources that it needed.

When I took the job I now have, I had a lengthy conversation with Senator Garn, whose proposal this is. And I promised him that I would try to run Trade Administration, my office, which is fairly newly created because we are not now a part of the trade promotion arm of Commerce, as an Office of Strategic Trade. I think we have done a pretty good job at doing that.

The only concern that one can still express is not toward the licensing function although, and I accept the criticism made of the Compliance Division. I do not believe that it has been as effective as it might. Its agents are not as well trained as they should be and I accept some of what I call the micro-criticism in the staff report. But I do not believe the trade promotion arm impedes the enforcement. I do not think that is the problem. I think the problem that we have got to look at is strategic trade, or the use of the economic power of this Nation, what has been referred to as the wealth of the Nation. Is it being factored into the foreign policy process in a manner where it becomes as strong a factor as it might in trying to direct the policies of this Nation vis-a-vis a certain project or a certain policy. I think that may still be a legitimate criticism. I think we have done a good job in pivoting, so to speak, what some people would incorrectly call the elements of economic warfare, for instance, in the foreign policy structure.

Chairman ROTH. I am sure my colleague, Senator Nunn, will want to get into it in greater depth, but I am not sure I fully understand why

policymaking and compliance should be joined together. It seems to me organizationally you can make a pretty strong argument that it is better to keep them apart.

One of the problems, it seems to me, is that we go up the hill and down on this matter of exports, depending on the mood, and philosophy of the Nation at the moment. As a strong believer in trade, I think we have got to do everything we can to expedite it, but obviously not at the cost of security risks. Doesn't it make sense to keep compliance separate as you wrestle with some of these other philosophical and policy matters?

Mr. BRADY. Mr. Chairman, no. I don't agree with that. I don't think these ideas are philosophical. We have in the last year, immediately upon taking office, instituted a number of senior interagency groups that resulted in new policy directions by the President of the United States with regard to the licensing of high-technology products. We implemented that and are in the process of implementing that both domestically and internationally through negotiation with our Cocom partners.

I would point out that the list of controlled commodities to the Communist world is sophisticated and lengthy. One computer requires a license and another does not.

The committee states that Customs can easily implement or rather enforce the munitions regulations. I don't believe that Customs can enforce dual-use regulations because our list is much longer and more sophisticated. Military weapons are easily defined and there are few cases in this area.

Our licensing personnel are intimately involved and will have to be regardless of where the enforcement arm is. This is one very strong reason to keep it where it is.

Furthermore, the dialog that to a certain extent already exists and will exist to a much greater extent between the licensing officials and the business community and the enforcement personnel is the means by which we get many of our intelligence leads.

As a matter of fact, the major cases we have had in this area have not been as a result of inspection at the ports. All the major cases that we have prosecuted in the export control area, both we and Customs, have been the result of intelligence leads brought up by the business community.

Furthermore, Commerce has an extensive apparatus both internationally and domestically of field offices and those field offices are out impressing upon the business community the requirements of licensing with regard to particular commodities. As a matter of fact, so much of the field offices time is being devoted to what we call the licensing or enforcement problem, my colleague has asked me to reimburse him for the people being taken away from the trade negotiations functions.

Chairman ROTH. A final question. I would like to congratulate you on hiring Assistant U.S. Attorney Ted Wu. He is well known by my staff. He is indeed an excellent choice. Could you elaborate on what his duties will be?

Mr. BRADY. Mr. Chairman, he is going to be setting up a new enforcement mechanism in the Department as a Deputy Assistant Secretary reporting directly to me. That will be composed of two

units, the Anti-Boycott Compliance as well as the Export Administration Act provisions regarding export controls.

Furthermore, we will take the Export Control Office that we have today and change it drastically. I believe, and Ted agrees, that it is silly to have 4 or 5 inspectors at a couple of the ports when Customs has 200 and they are much more able than we to do the inspection function and, therefore, we will most probably be abolishing the inspection function in the Department.

Our objective is to get a highly professional white-collar crime outfit working with the intelligence agencies and all those from whom we get leads to pursue in the best way we can with the FBI the illegal acquisition in the United States. I think we can do that and do it well.

Chairman ROTH. Thank you, Mr. Brady.

Senator Nunn?

Senator NUNN. Thank you, Mr. Chairman.

Mr. Brady, you mentioned that a good many of your intelligence referrals and I assume your other referrals to the Justice Department grew out of a coordination between your Licensing Division and your Enforcement or Compliance Division, is that right?

Mr. BRADY. I said that the dialog was a necessary one in a number of things. One, impressing upon the business community what is controlled, how the Soviets are operating and yes, we do get some leads back from the business community, very definitely, as to where commodities are in the Soviet Union. Very often, where a competitor's commodity has been exported to, with certain indications as to who may have exported it. So to that extent we do get leads.

Senator NUNN. How many criminal cases has Commerce worked on in the last 12 months?

Mr. BRADY. I think for fiscal year 1982, there are four criminal cases that have been referred to Justice.

Senator NUNN. How many?

Mr. BRADY. Four.

Senator NUNN. For fiscal year 1982, the whole year.

Mr. BRADY. I believe that, that's right.

Senator NUNN. The FBI was not familiar with any.

Mr. BRADY. Mr. Chairman, the FBI wouldn't necessarily be. They are in the espionage business, they are not in the export control area.

Senator NUNN. You did all the investigative work and referred to Justice for prosecution.

Mr. BRADY. I am sure we had help in the investigative work but it would be referred to——

Senator NUNN. Who did you have help from?

Mr. BRADY. I am sure it was Customs. I have to go over each specific case but I am positive that we got help, and I don't think there is anything wrong in that.

Senator NUNN. I don't either. The question is, what are you really doing in the Compliance Division, that is the question we are going to be coming back to over and over again in the course of my questioning this morning. Are you familiar with the *DeGeyter* case?

Mr. BRADY. Yes, I am, sir. Somewhat.

Senator NUNN. Was that a Commerce Department case?

Mr. BRADY. No, sir, it was not.

Senator NUNN. In the Compliance Division report, didn't they claim that was a Commerce Department case?

Mr. BRADY. Mr. Chairman, it is my understanding that the law requires the Export Administration Act to report the cases that have been prosecuted under that act and that is why that was included in the report.

Senator NUNN. We can get the exact language of that report but it was very misleading, I think, in terms of reporting to Congress. When was that report made, do you know?

Mr. BRADY. Fiscal 1980.

Senator NUNN. Fiscal 1980. Let me just go over a few of these. As I understand it, you are saying the subcommittee staff investigation is useful as a historic document, is that right?

Mr. BRADY. I say, Mr. Chairman, that the document does not reflect certainly what we have done in the administration. Let me be fairly candid. I think one of the problems that I personally have with the report is that it tends to equate the enforcement of the Export Administration Act, particularly the Commerce Department function, with technology leakage generally, and that is inappropriate, because the problem is much, much greater than that. It is industrial espionage, it is counterintelligence, it is scientific exchange agreement, everything I have discussed already.

Senator NUNN. Our hearings have covered the whole scope of all of that. As you well know, the staff report centered on some criticism with the Commerce Department and the Compliance Division, but that doesn't in anyway imply the subcommittee hadn't looked at the broad scope. If you review the testimony of the witnesses we had, most of our time has been spent in areas that don't directly involve the Commerce Department.

Mr. BRADY. I have accepted some of the criticisms of the Compliance Division.

Senator NUNN. You call them microcriticisms and historically useful. Let me just pursue "the historically useful" for a minute. Does that mean you are here today saying you have corrected these historic observations by the staff?

Mr. BRADY. I think we have corrected some of them. I think the analytical unit that we have created goes a way to correcting some of that. I think the fact that we are creating a Deputy Assistant Secretary, something we have been working on for months, is going to solve some of our problems.

As we go through and reshape and rehabilitate the division, reorganize it, I think there is no question——

Senator NUNN. How much of this is in the future as to what you intend to do and how much of it have you already done? Let's just take each item now. Tell me what has been accomplished so far today as opposed to what you plan to do? We have an awful lot of plans when we have a hearing and that is one of the purposes of a hearing, I think that is useful.

Mr. BRADY. I agree.

Senator NUNN. I have never had a hearing on any criticism of any agency where they didn't have plans to correct every item that had been identified. When you have another hearing a year later you find out it hasn't been done.

Let's just talk about what has been done now so we can really distinguish what is historic and what is actual.

Mr. BRADY. Senator, before I go to the specifics, let me make a point that I mentioned in my prepared remarks: We could not move to rehabilitate the Division before we had an assessment of what has happened. That is, what are the Soviets doing, how are they operating, what are they targeting. We didn't have that, but we do now. We have addressed the international aspects of the enforcement. There are five major agenda items that we will discuss with our allies on Monday. So it is not only the Compliance Division. That is the point I am trying to point out in terms of what we have done over the last year.

Senator NUNN. I understand.

Mr. BRADY. Let me go specifically to the division.

Senator NUNN. Let me ask you this; do you have to have all of that before you can determine whether the Compliance Division officials have proper law enforcement training? It seems to me no matter what the Soviets have acquired, no matter what the record shows, you are going to need a group of people with adequate enforcement training there, would you not?

Mr. BRADY. You are right, Senator.

Senator NUNN. Do you have people with adequate enforcement training?

Mr. BRADY. We have some.

Senator NUNN. How many?

Mr. BRADY. I can't answer that because that is a judgment call. If you look at some of the background of the agents——

Senator NUNN. Your judgment would be the only one we have. How many people do you have that you think really have adequate law enforcement experience?

Mr. BRADY. Mr. Chairman, I can't answer that in specific terms. I can tell you that we were aware, and I was aware obviously before I came back to Washington, of the problems in the enforcement area. I called it a shambles. I was aware of it.

Senator NUNN. What do you call it right now?

Mr. BRADY. Let me——

Senator NUNN. What do you call it right now?

Mr. BRADY. It is in the process of getting new life, let me put it that way. Let me give you an example, for instance, on how to reshape the division. I could not have made a decision on that before Customs decided to put 200 people in the field to do its inspection, and they did that a few months ago. Now based on that action, and I hope that it is a permanent action, I don't need those four or five people and the field people in New York doing inspection. I think it duplicative.

We can take those four or five positions and use them for better purposes. I have got to be careful in public testimony because the personnel process we will go through in the next few months is going to reveal many problems in terms of actions taken to reshape the division, but that is simply one of the examples that delayed us in refashioning the organization itself.

Senator NUNN. So the organization hasn't been refashioned then; it is in the process?

Mr. BRADY. Well, no, I believe the order has been signed creating the Deputy Assistant Secretary. Ted Wu will be on board within 4 or 5 weeks as soon as he winds up on the west coast.

Senator NUNN. How do you deduct from that that the staff report is historic?

Mr. BRADY. Senator——

Senator NUNN. It seems to me everything you are saying is none of these changes has been made, that they are all in the process. So how do you conclude the staff report is historic when almost all the corrections you have identified are all perspective in nature?

Mr. BRADY. Senator, what I am saying is——

Senator NUNN. You were a candid witness when you were the whistleblower. Now you are here and it seems to me you have to maintain that same degree of candor. If you are going to correct these problems, I think you ought to just candidly say so but to come here and identify all the things you plan to do and then call the staff report historic implying you have already made those changes, seems to me is not in keeping with your past record of candor.

Mr. BRADY. Senator, some of the changes have been made.

Senator NUNN. Tell us what has been done?

Mr. BRADY. The analytical unit working with Customs is working well and it has been working well for a couple of months. It is a major addition to the enforcement apparatus in this area. The Deputy Assistant Secretary position has been created and an individual has been selected and he will be on board within 4 to 5 weeks as soon as he can sever his relationship with the Department of Justice.

Senator NUNN. He is not there yet?

Mr. BRADY. That's right.

Senator NUNN. All right.

Mr. BRADY. Third, there have been some major efforts made in the field offices of the United States Commercial Service of the Department of Commerce, to educate the business community as to what the Soviets are acquiring in the United States and how they are working. Now that program is not complete.

Senator NUNN. Every witness we had said they never even heard from the Commerce Department on that. In fact, the amazing thing is that Commerce is the agency that is supposed to have the liaison with the business communities. Yet we can't find any witness who has had a dialog with them on that subject.

We had a lot of witnesses, they talked to the FBI, Defense, but they haven't heard from Commerce. Maybe you can detail for us what you have done in communicating with the business community.

Mr. BRADY. I will be happy to and it goes, Senator, from writing to all exporters in the particular industry sector to alert them to the fact that there is a procurement effort under way, to staging major conferences in various areas of the country. Ted Wu himself has addressed, I know, at least two major conferences on the west coast.

Senator NUNN. Is he on your payroll now?

Mr. BRADY. No, but he did it because I couldn't go.

[At this point, Chairman Roth withdrew from the hearing room.]

Mr. BRADY. I specifically remembered those conferences and we had some across this country. I personally have traveled across this country dealing with the field offices to impress upon them the need to become more involved in the diversion problem and they have been. The criticism I have with the report is, I believe, it does not point out what we have done internationally. It is very relevant to the Compliance Division. The enforcement apparatus must be international if it is going to

be any good. And that is where the large part of the problem lies. And so I think we have moved in the last year, as I said, systematically and quite aggressively in dealing with the problem.

And the problem is not only enforcement but it is also licensing. We have cleaned up a backlog of 2,000 export license applications that we inherited from the previous administration. We have the process functioning, the interagency process functioning so we get decisions on cases and on issues.

Senator NUNN. Have you cleaned up the backlog in the investigations and intelligence branches?

Mr. BRADY. No; we have not.

Senator NUNN. That was one of the criticisms. Is that historic?

Mr. BRADY. It is a legitimate criticism, yes, sir.

Senator NUNN. Have you really revised your whole law enforcement training? Do you have people on board now who are capable in the law enforcement area?

Mr. BRADY. There are announcements out for 15 positions that we intend to put on the west coast—14 positions I guess it is—in which we are recruiting for those jobs.

Senator NUNN. But you are not satisfied with what you have got on board now?

Mr. BRADY. Absolutely not.

Senator NUNN. That is not a historic observation then?

Mr. BRADY. Well, it is in a sense, Mr. Chairman. I would have liked the opportunity or another policy level official at Commerce would have liked the opportunity to comment on the report and to indicate what we were doing and what we have done and, again, I want to stress the fact that the Compliance Division specifically is one small part of the overall enforcement apparatus that this Government directed to this problem.

Senator NUNN. Mr. Brady, you don't have to convince us of that. I have been in these hearings 5 years on the subject. We know that, we know you are not the only one. We don't put all the blame and efforts on the Commerce Department. We are just simply looking as to whether it makes sense for the Commerce Department to have a Compliance Division with a few people on board most of whom don't have law enforcement experience when you have a whole agency out there that is trained in this area. That is the question. You can broaden it and you are correct in broadening it, it is a much bigger question than this. This is only one aspect of our whole hearing.

You mentioned that the Inspector General of the Commerce Department has conducted a review of the Compliance Division whose findings and recommendations will be published later this month; is that correct?

Mr. BRADY. I believe so.

Senator NUNN. Have you seen those recommendations yet?

Mr. BRADY. No, I have not.

Senator NUNN. Do you know the Inspector General?

Mr. BRADY. Yes, I do.

Senator NUNN. Have confidence in him?

Mr. BRADY. Yes, I do.

Senator NUNN. Do you think he has a broad perspective?

Mr. BRADY. He is Inspector General. I think it is important that all factors be put into any assessment of the enforcement arm and that means the licensing function as well. And I know I may not be stating this very well, but in this dual use area, you are not dealing with a tank or an aircraft. You are dealing with a computer that may require a license or may not. The licensing officer very often has to work very closely with an investigator in determining whether or not a particular shipment is illegal, whether blueprints that may be exported require a license or not.

Senator NUNN. You say you have not seen the Inspector General's report?

Mr. BRADY. No, I have not. I have a feeling I know what he is going to recommend.

Senator NUNN. It is our information that that Inspector General reported started on April 19, 1982, less than a month ago.

Is that consistent with your information?

Mr. BRADY. I believe that is correct.

Senator NUNN. We understand it was formally concluded on May 11, that is yesterday.

Mr. BRADY. That is not my understanding.

Senator NUNN. Well, in any event, the Inspector General's report is not historic, is it, it would be rather current.

Mr. BRADY. I would hope that it would reflect the progress that we have made, yes.

Senator NUNN. It should reflect the progress you have made?

Mr. BRADY. That's right.

Senator NUNN. We have been informed that that report will verify all the findings, virtually all the findings of our staff. And that report has taken place in the last 30 days. So once you read the report, we would like for you to tell us whether that, too, is historic.

Mr. BRADY. I will be glad to, Senator. But I also think, or I would hope, that the report would take into consideration, one, the broader picture, and, second, the fact that we are well on our way to solving the problems.[2]

Senator NUNN. You mean by the broader picture, you want the report to center on the Department of Defense, Department of State, Customs Agency.

Mr. BRADY. I want them to center on the fact it is we at the Department of Commerce that asked the CIA to prepare this assessment, the fact that we asked for it to be released because we have problems in dealing with the business community.

We have problems in dealing with the press to elevate the level of public consciousness. There are many people out there who still do not believe that there is a problem. These are all part of an enforcement apparatus.

Senator NUNN. I agree with that, Mr. Brady, but everything you say, I grant everything you say is correct on that point but that doesn't answer the question of whether you need a Compliance Division in the Commerce Department.

---

[2] The final inspection report of the Inspector General's Office, Department of Commerce, regarding the Compliance Division was released to the Permanent Subcommittee on Investigations on July 16, 1982. The report is reprinted in full beginning on p. 696.

It doesn't answer the question about whether you should continue an operation that under several administrations has demonstrated very vividly that it is not capable or it is not serious, one or the other, about enforcing the law of the United States in this respect.

So you can broaden it all you want to and we will agree with everything you say on that but that is irrelevant to the purposes of what we are asking you, and that is whether the Compliance Division still should be in the Commerce Department.

Mr. BRADY. Let me give you a statistic. You talk about seizures and Customs seizures, 89 percent of the seizures made by Customs at the ports of exit have to be returned because the items do not require a license. That is the kind of fundamental basis that we hope to overcome.

I accept the fact that our investigators are not well trained or the bulk of them are not well trained in law enforcement but I think there is a compensating factor in some cases that they do have knowledge of the licensing system and they do have knowledge of the technological requirements involved in the licensing process. And so I am not using that as an excuse for not having good trained officials, believe me.

But what I am saying is, the situation is not black and white.

Senator NUNN. You are going to have maybe another 40 percent and if you add 40 percent to what you have got now, that will get you up to 59 persons and those 59 persons in the Compliance Division, it seems to me, are woefully inadequate to have any hope of enforcing this law unless they largely are in a position of liaison between licensing and Customs.

You are going to have to use Customs and the FBI to do it and the question is: Do we need a layer between licensing and Customs in order to communicate?

It seems to me you can shift a few of these people who are trained in law enforcement into the licensing division.

They are probably very good people in that respect and let them be liaison with an enforcement mechanism that is already in place and that has hundreds of agents around the country and around the world and has intelligence connections in almost every country of the world.

It just seems to me your position about compliance is just not a logical position.

Mr. BRADY. Senator, you asked me about the backlog of investigative cases. The Customs Service has 9,000 backlogged investigation cases. Now I don't understand——

Senator NUNN. In the export area?

Mr. BRADY. No, across the board. But I would also point out that their priorities shift on what the crises of the moment are.

I have been informed just in recent weeks that they cannot provide me the information I need to monitor our steel monitoring mechanism, basic steel imports pursuant to the steel trigger pricing mechanism we have and the 75 dumping and countervailing cases we are prosecuting because of lack of resources. So I think there is a question of going from the frying pan into the fire with regard to Customs.

What I am trying to say is the issue is not black and white and I think that a hard core, high level, professional establishment at the Department of Commerce working with the FBI, the CIA, and Customs is the best way to attack——

Senator NUNN. When can we expect that to occur? When can we expect that high level, competent, professional group at Commerce to be out there in the field enforcing the law?

What is the date that you are shooting for? Obviously you don't have that now.

Mr. BRADY. That is right.

Senator NUNN. If you had it now we might not be asking these questions.

Mr. BRADY. I think within 6 months we will have it.

Senator NUNN. Six months from right now?

Mr. BRADY. That is right.

Senator RUDMAN. We will stand in recess for the time it takes for the chairman to get back here.

[Members of the subcommittee present at the time of recess: Senators Rudman and Nunn.]

[Brief recess.]

[Member of the subcommittee present after recess: Senator Roth.]

Chairman ROTH [presiding]. While we are waiting for the other Senators to return, I believe the staff has some documents they want to put into the record.

Ms. HILL. Thank you, Senator; yes, we do. I have three exhibits we would like to have printed in the record. They are a signed and sworn affidavit of John Rennish, special agent with the U.S. Customs Service; a signed and sworn affidavit of Mike Dolphin, special agent with the U.S. Customs Service; a signed and sworn statement of Charles L. McLeod, special agent, U.S. Customs.

[The documents referred to was marked "Exhibit Nos. 29, 30, and 31," for reference and follows:]

EXHIBIT NO. 29

Affidavit of John Rennish

I, John Rennish, an officer of the U. S. Customs Service headquarters in Washington, D. C., make the following statement freely and voluntarily to Glenn Fry, Ray Worsham and Fred Asselin, who have identified themselves to me as being on the staff of the Senate Permanent Subcommittee on Investigations.

I am a Special Agent with the United States Customs Service. I am assigned to the Customs Service headquarters in Washington, D. C. I have been a Criminal Investigator with Customs for 15 years.

As a Criminal Investigator, I was assigned to the investigation of Manfred Swarovski of Wattens, Austria in 1975. A member of a wealthy and influential Austrian family, Swarovski, who was then about 34, owned and operated an optical equipment business in Austria that specialized in manufacturing glass beads used in reflection devices and paint for night vision purposes. The company was known as M. Swarovski Ges. Mbh & Co. and was located in Amstetten, Austria. The company's devices were used on highways in Europe and the United States.

Swarovski established two businesses in North America -- Swarolite of Canada, Ltd., also known as Canasphere Industries Ltd., located in Moose Jaw, Saskatchewan, Canada, and Swarolite, Inc., located in Columbia, Tennessee. In or about 1974, Swarovski entered into an agreement with the Soviet Union to construct a glass bead manufacturing plant in Russia.

In the spring of 1975, U. S. Customs agents were contacted by John Kiel, president of Photo-Sonics, Inc., of Burbank, California. Kiel said that Swarolite of Canada wanted to buy from Photo-Sonics a special gunsight camera, model KB25A, used on the U. S. Air Force F-4 fighter aircraft. Kiel said the order for the camera had been placed by Rod N. Parker, manager of Swarolite of Canada. Kiel said he had informed Parker that he could not ship a camera to Canada. To make such a shipment, Kiel said, would require a validated export license authorized by the U.S. Department of State.

Kiel said he was bringing this matter to the attention of the Customs Service because he suspected that Swarolite of Canada intended to ship the camera from Canada to Austria. Kiel considered it very questionable that Swarolite of Canada should want such a camera. He wondered what use Swarolite could make of it. The gunsight camera could be modified so that it would have functions other than its use on the F-4 fighter. However, even in a modified form, the camera would still be an item controlled on the U. S. Munitions List and would require a license for export. Moreover, the State Department did not want the camera exported anywhere, not even to Canada.

Customs agents instructed Kiel to keep them informed of what Swarolite of Canada did next. Shortly thereafter, Manfred Swarovski, through his Swarolite of Canada company, requested that Photo-Sonics sell the camera but, instead of shipping it to Canada, to send it to his plant in Columbia, Tennessee. Such a shipment would not require an export license. Following the instructions of Customs agents, Kiel agreed to ship the camera to Swarolite of Tennessee.

With the assistance of U. S. Postal Inspectors, Customs agents monitored the mailing of the camera. Rod Parker had indicated that the shipment would have to arrive in Columbia, Tennessee, by a specific date.

Customs agents controlled the delivery of the package. The camera package invoice and registered letter accompanying it were marked with these declarations: "Above items are of U.S.A. origin and manufacture. Above photographic equipment is under United States Department of State Munitions List Category No. XIII (a), and as such must be export licensed by the U.S. Department of State prior to export from the United States." A copy of the letter was also packaged with the camera.

Customs agents conducted surveillance of the package as it was delivered to the U.S. Post Office in Columbia, Tennessee. James Sproul, Swarolite manager in Columbia, received the camera and delivered it to Swarovski, who was staying in the Holiday Inn Motel at the outer city limits of Columbia.

Swarovski also was placed under surveillance by Customs agents. His activities in Columbia seemed routine and included dining out and shopping. The next day Swarovski was again under surveillance as he checked out of the Holiday Inn Motel and boarded a flight to Chicago. From Chicago he flew to New York City.

When Swarovski arrived in New York, I personally took full control of the investigation and coordinated the surveillance activities concerning Manfred Swarovski. Once in New York City, Swarovski checked into the Waldorf Astoria Hotel. Customs agents, continuing their surveillance, took a room adjacent to his. Swarovski spent the next two days in New York City. He seemed to be enjoying himself considerably, shopping, dining out, frequenting several bars and entertaining women friends in his room. In the midst of this round of activities, Swarovski took steps to suggest he might be trying to alter his appearance. He changed his manner of appearance frequently and began wearing dark glasses and began styling his hair in a different manner. However, our surveillance went on uninterrupted. Ultimately, 15 Customs agents were assigned to this detail.

Customs agents learned that Swarovski had reservations on a Lufthansa flight from Kennedy International Airport to Frankfurt. He decided to leave on an earlier Pan American flight for Munich. Swarovski checked out of the Waldorf Astoria Hotel and went to the airport where he checked all his luggage through at the Pan Am ticket counter. Swarovski then went to the predeparture lounge and waited for his flight to be called.

Customs agents, operating under 22 U.S.C. 401(a), which gives them the right to search luggage under these circumstances, went through his suitcases and found the special gunsight camera among his belongings. Swarovski, who was unaware that the search had taken place, was then approached by Customs Special Agent Grattan and myself. In a routine manner, we questioned him as to whether or not he was transporting anything of value in excess of $250.00 out of the country. I asked, "Do you have anything that you are taking out of the U. S. that requires a shipper's export declaration?" He was also asked if he had any merchandise requiring a U.S. Department of State license. Swarovski said no to all

three questions. I placed Swarovski under arrest. He was read his rights and given the Miranda warning in English and German. Customs agents also found several business cards of Soviet officials on Swarovski's person.

The export violation occurred, according to the U. S. Districts Courts' interpretation of the law, at that moment when Swarovski checked his luggage through to Munich at the Pan Am ticket counter in the JFK Airport terminal. We believed that Swarovski intended to take the camera into Austria and there have his freight forwarder ship the camera to a destination in the Soviet Union. If we could have had access to official shipping documents in Austria, we could have tried to demonstrate that he planned to transfer the camera to the Soviet bloc. Unfortunately, however, because U. S. Customs agents received very little cooperation from the Austrian government, we were not able to document or otherwise establish that Swarovski intended to ship the camera from Austria to the Soviet bloc. Austria, a neutral country which shares borders with the Soviets bloc nations of Hungary, Yugoslavia and Czechoslovakia, was not supportive of U. S. Customs' investigative efforts.

Records of Swarolite of Canada were given to U. S. Customs by a cooperating co-conspirator. These records revealed that on previous occasions Swarovski had bought American high technology equipment with military applications and sought to export it to an Austrian freight forwarder without the proper licenses. However, once again because the Austrian government would not provide assistance, the U. S. Customs Service was unable to document or otherwise establish that these items were shipped to Soviet bloc nations. Further inquiry by Customs indicated that Swarovski had tried but failed to buy from the National Aeronautics and Space Administration a NASA moon-mapping lens.

There is no attempt provision in the current export control statutes. Because of that, the violator can be apprehended only after he actually does the act of exporting; in Swarovski's case, the act of violating the law occurred at the moment he checked his luggage containing the gunsight camera through at the Pan Am ticket counter. It was then that he presented his merchandise for export. This requirement means that surveillance must be continuous on a suspect until that moment when he violates the law. The cost of such surveillance can be prohibitive if it goes on too long. Consider, for example, that instead of staying only two days in New York City he had stayed two months or longer. At some point, Customs might have been forced, because of financial considerations involving a 15-man surveillance team, to curtail the inquiry and hope to detect him at the airport. But any number of things can go wrong once the surveillance is stopped. Swarovski could have rented a car and driven to Boston or Newark and flown abroad from there. The slightest change in plans could have resulted in his escaping Customs and successfully carrying the camera out of the U. S.

The lack of cooperation in the Swarovski inquiry from Austria was not unique to this case. U. S. Customs receives poor cooperation from Austria in many export violations. Another neutral European nation, Switzerland, does not make a great effort to help in export violations in many cases.

U. S. Customs was fortunate to have had cooperation from the beginning of the case from John Kiel, president of Photo-Sonics, Inc. Had Kiel not reported

to us when he did, Swarovski might have taken possession of the camera in Canada and shipped it from there to Western Europe.

Customs agents enforcing export laws do not have the authority to arrest. They can investigate, search and seize but there is no statutory authority under the export laws to arrest. Arrests can be made if they are in states where Customs agents are deemed to be peace officers of that state. Customs agents have no state peace officer certification in New York. Swarovski's arrest by Customs agents was only one aspect of the inquiry that Swarovski's attorney challenged in court.

The attorney, Richard H. Kuh, instituted suppression arguments and appeals which lasted in court hearings for the next 26 months. Swarovski's search, seizure and arrest were attacked. Ultimately, the suppression and appeals hearings proved unsuccessful. But the arrest issue went all the way to the Supreme Court where it was upheld as a citizen's arrest. His appeals exhausted, Swarovski pleaded guilty and served a two-year prison term.

The judge in the trial, George C. Pratt of the U. S. District Court in the Eastern District of New York, noted the difficulties U. S. Customs agents must work under in export cases. Citing the fact that export laws give Customs agents the right to seize and search in connection with munitions violations, but not to arrest, Judge Pratt said:

> The fault, if there be any, lies with Congress which has failed to grant Customs officers statutory authority to make arrests under the Munitions Control Act. Congress passed the Act with broad powers of search and seizure, and commanded the Secretary of the Treasury to enforce it. Congress did not, however, take the additional step and grant to the Customs agents specific statutory authority similar to that granted to them to apprehend narcotics and revenue violators. As a result, Customs agents are powerless to arrest on the scene those persons who are caught in an attempt to illegally export under the Munitions Control Act.

The lack of statutory authority to make an arrest described by Judge Pratt is still a restriction that Customs agents must work under in export violations.

I would like to append to this affidavit two exhibits:

1. Docket No. 75 CR 795, Memorandum and Order on Suppression Motions, United States of America against Manfred Swarovski, U. S. District Court, Eastern District of New York.

2. Docket No. 76-1556, United States Court of Appeals, Second Circuit, United States of America v. Manfred Swarovski, September term, 1976.

I have read, reviewed and initialed each page of the foregoing statement, and I swear to the best of my knowledge that it is true and correct.

John Rennish

January 26, 1982

Sworn and subscribed to before me
this 26th day of January, 1982

Notary Public

My commission expires:
14 May 83

EXHIBIT NO. 30

AFFIDAVIT

I, Michael Dolphin, a Special Agent with the U.S. Customs Service, Baltimore, Maryland, make the following statement freely and voluntarily to Glenn Fry and Jack Key of the Senate Permanent Subcommittee on Investigations.

I have been a Criminal Investigator with Customs for four and a half years. I initiated the investigation of Werner R. Hilpert in July 1980. Later on, I discovered the involvement of Rolf Peter Herms and Volker Nast. Nast and Herms, natives of West Germany, conspired to purchase a Microwave Surveillance Receiver system and smuggle it out of the United States to Hungary without obtaining a validated export license from the State Department, Office of Munitions Control. Nast and Herms were assisted in their plan by Werner Richard Hilpert of Princeton, New Jersey.

The Microwave Surveillance Receiver system, known as the model MSR-903, is offered for sale by the Micro-Tel Corporation, 6310 Blair Hill Lane, Baltimore, Maryland. Designed to receive, display, and analyze microwave signals, it is primarily intended for military and other surveillance uses. The MSR-903 has been designated as a defense article by the President of the United States and is also included on the United States Munitions List under Category XI(c). For that reason, a special export license or written approval from the Department of State is necessary to export the MSR-903. An applicant for such a license is required to reveal the country of final destination, purpose of its use, and the intended end-user of the equipment.

Customs learned that in June, 1980, Rolf Peter Herms wrote to Werner Hilpert requesting him to place an order with Micro-Tel Corporation, Baltimore, Maryland for a MSR-903. Soon thereafter, Hilpert contacted Micro-Tel and placed the order. Micro-Tel advised Hilpert that he must apply for a license with the State Department if he intended to export the MSR-903. In August, 1980 Herms wired $12,000 to Hilpert for a down payment on the MSR-903. Hilpert subsequently remitted a check to Micro-Tel for a $10,000 down payment. At this time, Micro-Tel again advised Hilpert, in writing and orally, that a license was required for export.

Hilpert passed that information to Herms about the export license. Herms, after consultation with Nast, told Hilpert to go ahead with the purchase but that an export license would not be obtained.

Before the delivery of the MSR-903 officials of Micro-Tel Corporation once again advised Hilpert of the export license requirements.

Hilpert told the officials from Micro-Tel Corporation that the export license would be obtained by someone else associated with the purchase.

It was arranged for the MSR to be picked up in Baltimore by Hilpert in January 1981 after a motion activated beeper had been installed pursuant to a Court Order, in the fiberglass suitcase used to transport the MSR-903. The MSR weighs 78 pounds and is the size of a large suitcase. In January 1981, at the time Hilpert was to receive the MSR, Customs established surveillance of his residence, and Micro-Tel's location.

Hilpert's wife and Rolf Herms picked up the MSR at Micro-Tel and paid the balance of the $47,000 purchase price. It was learned that Volker Nast provided part of the funds with which the MSR-903 was purchased. In particular, on January 15, 1981, Nast purchased Bank America travelers checks in the amount of $39,000 in West Germany.

Special Agents of the U.S. Customs Service, with the aid of a Customs helicopter, followed Mrs. Hilpert and Herms to Princeton, New Jersey to Hilpert's residence. The Hilperts and Herms spent that evening at Hilpert's residence. The next morning Mrs. Hilpert and Herms placed a large package in their car and drove to Mr. Hilpert's office. From the office they went to lunch and proceeded to New York City. Herms left Mrs. Hilpert's vehicle in New York City with the package and took a taxi to JFK Airport. Customs continued following Herms until he checked all baggage with Pan American Airlines at JFK Airport. At that point Customs agents arrested Herms, advised him of his rights, and took custody of the MSR-903 which had been checked in as baggage. After initially denying any knowledge of the MSR, Herms admitted that he was sent by Volker Nast to pick up the equipment.

From the time of the initial pick-up of the MSR-903 on January 19, 1981, until Herms' arrest the next day approximately eighteen (18) Customs personnel

were involved. Four separate Customs vehicles from Baltimore followed the Hilpert vehicle to the beginning of the New Jersey Turnpike when surveillance was taken over by personnel from the Philadelphia Office. The vehicle was followed to Hilpert's residence in Princeton, New Jersey, where other personnel were manning a command post. A fixed video surveillance unit was installed in the vicinity of Hilpert's residence to monitor the activities. Customs personnel from Newark, New Jersey, had Mr. Hilpert under surveillance at his place of employment and followed to his residence.

The surveillance was also aided by a helicopter which followed the vehicle from Baltimore, Maryland, to Princeton, New Jersey, on January 19, 1981. On the next day the helicopter followed Herms from Princeton, New Jersey, to the vicinity of JFK Airport.

Nast is a fugitive from justice residing in West Germany. He was previously involved in the illegal exportation of controlled commodities in 1976 with two U.S. businessmen, Gerald R. Starek and Carl E. Story of I. I. Industries, Sunnyvale, California.

In the United States District Court in Brooklyn, New York, Rolf Peter Herms pled guilty on February 27, 1981, to a charge of attempting to export the MSR-903 without the required license. Mr. Herms was confined in the Metropolitan Correctional Center in New York from his arrest on January 20, 1981 until his sentencing on May 11, 1981. Chief Judge Jack B. Weinstein, United States District Court, Eastern District of New York, imposed the maximum sentence of two years, which was suspended, and placed Herms on probation for a period of five years. Herms was permitted to return to West Germany.

On May 26, 1981, Volker Nast was charged with a two-count indictment in Baltimore, Maryland, for conspiracy in violation of Title 18, United States Code, Section 371, and with aiding and abetting an attempt to violate the Arms Export Control Act, in violation of Title 18, United States Code, Section 2, and Title 22, United States Code, Section 2778.

Werner Hilpert pled guilty, pursuant to an agreement with the Government, on May 1, 1981, in United States District Court in Baltimore, Maryland, to a charge of aiding and abetting the attempt to export the MSR-903 from the United States without the requisite license. He was subsequently sentenced on

July 9, 1981, and placed on three (3) years probation and ordered to pay a $10,000 fine. Under his plea agreement, Mr. Hilpert agreed to cooperate with the Government and to provide any information within his knowledge concerning the alleged conspiracy.

During the course of this investigation the Customs Attache in Bonn, West Germany, also played an important role in following up on investigative leads and responding to these leads within a short period of time. When the MSR-903 was picked up on January 19, 1981, the Customs Attache in Bonn was notified and was prepared to coordinate a continued surveillance with the West German authorities if this was required.

The Department of State Office of Munitions Control had to research their records in order to determine that an export license had not been issued for the MSR-903. During the investigation it became necessary to immediately check the names of individuals and companies which became known. An up to date review of all applications was necessary in order to be positive that an export license was not submitted.

The Federal Bureau of Investigation was kept aware of developments in this investigation and provided excellent cooperation to the U.S. Customs Service.

I have read, reviewed and initialed each page of the foregoing statement, and I swear to the best of my knowledge that it is true and correct.

Michael T. Dolphin

Michael Dolphin

April 5, 1982

Sworn and subscribed to before me this 5 day of April, 1982.

Notary Public

My commission expires:

July 31, 1986

EXHIBIT NO. 31

STATEMENT OF CHARLES L. McLEOD

Special Agent, U.S. Customs Service

For The

U. S. Senate Permanent Subcommittee on Investigations

My name is Charles L. McLeod and I am a Special Agent with the U. S. Customs Service assigned to San Francisco, California. I have been employed with the Customs Service for eleven years, ten as a criminal investigator and one as a Customs Security Officer. I am a college graduate with a B.S. degree in business administration from Babson College, Wellesley, Massachusetts. I have, as a criminal investigator, attended U.S. Treasury Department Criminal Investigator School, Customs Basic School, Customs Fraud Investigation School and White Collar Crime School. I am thirty-four years of age.

During my career as a criminal investigator, I have conducted and participated in investigations involving smuggling, fraud, theft and violations of export laws. In 1977, I was the recipient of the Treasury Secretary's Award for the investigation I conducted of II Industries, an investigation I will discuss later in this statement.

I have been involved in export control cases since 1975. During a period of three years between 1975 and 1978 I worked export control cases exclusively. In 1980 I was assigned by Customs to set up a program in the San Francisco office which was to be geared to work export violations that involved the Soviet Union or Soviet Bloc nations. The program was headed by me with the assistance of John Bloom, a Customs Inspector. After two months I concluded that no one agency appeared to have a good intelligence data base. The FBI was willing to cooperate; however, it had no real in-depth information. The State Department only had information relevant to export license applications. It had no valuable intelligence data that could be used to get a handle on violations. There was no reservoir of information because there simply was not but a handful of prior cases in which to refer. The intelligence community did

not communicate, at least to my level, what the Soviets needed regarding technology or what the Soviets considered a priority.

Customs has been mandated to enforce violations of the Arms Export Control Act, which is administered by the State Department's Office of Munitions Control. To this end I can say that Customs has received excellent support from OMC. OMC has always expeditiously provided me whatever information I requested during my investigations. To my knowledge and experience there has been effective coordination and cooperation between Customs and OMC.

The Department of Commerce is mandated to enforce the Export Administration Act. Customs has delegated jurisdiction to enforce this statute; however, Customs has been effective and is capable of investigating violations of both statutes. My personal opinion is that export control violations are an area which demand thorough attention and priority, particularly those which have an impact on national security. It is a relatively new investigative area that contains inherent problems that few investigators have confronted. I would like to relate to you one investigation I conducted during 1975 and 1976 of II Industries and Kasper Instruments. The II Industries case related to violations of the Export Administration Act. Many of the investigative impediments I confronted during my investigation still exist today.

I first became involved in the II Industries case in July, 1975 when I assisted the Department of Commerce in a preliminary investigation of II Industries and Kasper Instruments of Sunnyvale, California. During March or April of 1975, Commerce received an allegation that certain semi-conductor manufacturing equipment from II Industries and Kasper was appearing in the Soviet Union. The equipment was being shipped via an exporting company named Semi-Con of Mays Landing, New Jersey. Semi-Con was run by Edward Breslin, a former U. S. military intelligence officer. It was subsequently learned that Semi-Con was a creation of Richard Mueller, a West German businessman, whom I will describe in more detail later in this statement. Commerce's initial action was to telephone officials at II Industries and Kasper Instruments and inquire as to whether either firm had sold equipment for use in the Soviet Union. Officials at Kasper admitted to trading with Semi-Con but not with Mueller or the Soviets. II Industries

indicated that they had not conducted business with any of the aforementioned entities.

In July, 1975, three months later, Commerce sent one investigator to the West Coast to interivew officials at II Industries and Kasper Instruments. I and three other Customs agents and an Assistant United States Attorney assisted Commerce with interviews. Examination of business records revealed that semiconductor manufacturing equipment originally destined for Semi-Con in New Jersey was in fact to be shipped to USA Trade and Semitronics in Montereal, Canada. Documentation for the equipment disclosed that although the electrical power usage had been converted for European voltage standards, Canada was to be the "end use" destination. There were even invoices for charges of $175.00 per unit for the conversion of the electrical systems.

Following the interviews and records examinations, Customs prepared a report for Commerce concluding that illegal activity appeared probable. Customs did not pursue the investigation because, at this point in time, its role was to assist Commerce. In August, 1975, Commerce prepared a report which recapped the activities of the preliminary investigation. The report had no indications of further actions to be pursued, no conclusions, and no recommendations.

In September, 1975, the import/export manager of II Industries informed Customs that II Industries and Kasper Instruments had in the past and were presently exporting, through diversionary means, licensable semiconductor manufacturing equipment that was ultimately intended for end use in the Soviet Union. Customs learned that Robert C. Johnson, President of Kasper Instruments, Gerald Starek and Carl Storey, officers of II Industries, and Richard Mueller conspired to circumvent licensing regulations in order to export equipment to the Soviet Union.

Richard Mueller is a West German businessman who operated at least two known businesses in West Germany named Technimex and Semitronic. Mueller was no stranger to U.S. authorities. He had previously been implicated in 1974 where he was involved in the illegal diversion of high technology equipment to the Soviet Union by Honeywell, A.G. of West Germany.

Mueller allegedly established Semi-Con in Mays Landing, New Jersey, as

a means to export semiconductor equipment to Europe. It was learned that when Commerce made inquiries of Semi-Con, Mueller came to the United States and met with Johnson, Starek and Storey to determine a new export route for the II Industries and Kasper Instruments equipment. It was decided that Montreal, Canada, would be the route in which to export the equipment through two companies, USA Trade and Semitronics. Canada was an acceptable route in that export licenses are not required when shipping products for end use in Canada. Therefore, equipment originally destined for Semi-Con in New Jersey was rerouted to Montreal, Canada. Following the July 1975 on-premises interviews and records examinations by Customs and Commerce, II Industries and Kasper Instruments decided to seek another exporting route. It should be noted that Customs coordinated with the Royal Canadian Mounted Police (RCMP) and learned that USA Trade and Semitronics did not physically exist; however, the address of USA Trade was occupied by Kuhn and Nagel, a Canadian freight forwarding company. The RCMP investigated Kuhn and Nagel's dealings with shipments from II Industries and Kasper Instruments and learned that the equipment was shipped to Semitronics in Zurich, Switzerland, without validated licenses. This was a violation of Canadian law and Kuhn and Nagel were prosecuted by Canadian authorities.

Customs learned that II Industries and Kasper were planning to ship equipment, ultimately destined for the Soviet Union, via Kansas City, Kansas, through an intermediary "dummy" company. II Industries and Kasper recruited a West German National, Frederick Linnhoff, who resided in the Kansas City area, obtained and operated warehousespace in Kansas City and traded as Paul Allen of Allen Electronics. Linnhoff was to receive II Industries and Kasper equipment from the West Coast, alter the supporting documentation to misrepresent the description and value of the freight and to change the ultimate destination to Hamburg, West Germany. Altering the supporting documentation of freight is a method used so as not to arouse suspicion of Customs or Commerce Inspectors thereby circumventing export licensing regulations. Once the freight is shipped to Hamburg, there is little that can be done to prevent the goods from being forwarded to the Soviet Union.

II Industries sent two shipments of licensable equipment through Kansas. The first shipment was ultimately traced, due to efforts between German Customs and the U.S. Customs Attache in Bonn, through Hamburg, West Germany, and on to East Germany. Through information received, Customs was able to monitor the second shipment II Industries was sending through Kansas. This shipment contained a sensitive "state of the art" piece of equipment. Through coordination with Commerce, who did not want the shipment to leave the U.S., it was decided to substitute the shipment. The state of the art equipment was substituted with sand bags through the cooperation of the freight forwarder. The original shipment was seized. The purpose of the substitution shipment was to trace the export route and determine its ultimate destination without risking losing the equipment to the Soviets. Linhoff had changed the inscription on the original shipment (did not exist) and the destination as Reimer Klimatechnik, Hamburg, West Germany. Reimer, we later learned, was an alias used by Volker Nast, a West Germany associate of Richard Mueller, who was also known to be in the business of procuring U.S. technology for the U.S.S.R.

While the substitution was being made, searches were conducted of II Industries, Kasper Instruments, Allen Electronics and Linnhoff's residence. Incriminating evidence indicating shipments were going to the U.S.S.R. was discovered. Indictments were drawn and issued for Robert C. Johnson of Kasper Instruments, Linnhoff, Starek and Carl St[illegible] of II Industries. Linnhoff fled to Germany and the others ultimately pled guilty to a felony.

Linnhoff was subsequently interviewed in Germany by German and U.S. Customs and stated that the shipments were destined for the U.S.S.R. and that he had been advised by Nast that the Soviets had received a shipment of sand.

During the investigation of II Industries and Kasper, I learned that Richard Mueller elicited the services of John Marshall through Carl Storey. Marshall is the former owner of Advanced Micro Devices, Santa Clara County, California. Marshall, an expert in the semiconductor manufacturing industry, agreed to provide consulting services to the Soviet Union on behalf of Richard Mueller. Marshall visited the Soviet Union on at least two occasions to provide

consultation for the proposed construction of semiconductor manufacturing facility. Marshall eventually stopped providing consultation to the Soviets; however, his business partner, John McCracken, succeeded him. McCracken made at least one trip to the Soviet Union, again on behalf of Mueller, to provide similar consulting services. McCracken, like Marshall, soon stopped providing any services to the Soviets.

As I mentioned earlier, Richard Mueller played a role in the diversion to the U.S.S.R. of technology involving Lother Haedicke, a representative of Honeywell, West Germany. Customs learned that II Industries and Kasper Instruments were linked to Haedicke during this time. Haedicke conducted business with a West German, Jerry Gessner, who was the European sales representative for Applied Materials, a Silicon Valley firm which produces semiconductor manufacturing equipment. Gessner also acted as the European sales representative of II Industries and Kasper Instruments. It was eventually learned that Gessner was also in the employ of Richard Mueller. Haedicke processed orders through Honeywell to export semiconductor manufacturing equipment from II Industries and Kasper. Kasper and II Industries would export the equipment to Gessner at Applied Materials in Germany who would work with Haedicke to ship it to the eventual customer. Haedicke was subsequently prosecuted by the West German authorities for providing the Soviet Union with information detrimental to its national security.

It is my personal observation that the Soviet Union lacks advanced technology relating to the semiconductor manufacturing industry. During the past six to eight years, there has been evidence which illustrates that the Soviets have made great efforts, at a great expense, to obtain technology relating to semiconductor manufacturing. The Soviets attempted in 1974 to obtain, through illegal means, semiconductor manufacturing equipment through Lother Haedicke of Honeywell, A.G Further attempts were made in 1975 through Richard Mueller, Volker Nast, II Industries and Kasper Instruments. Most recently, it has been documented that from 1976 until 1980, the Soviets obtained similar equipment through Anatoli Maluta and Werner Bruchhausen, another West German business intermediary. The Soviets even solicited consulting services from U.S. citizens, John Marshall and John McCracken.

It seemed evident that the Soviet's aim was to construct a semiconductor manufacturing facility by using U.S. technology and equipment. The equipment the Soviets obtained from II Industries and Kasper Instruments comprised only 20% of the equipment necessary for a semiconductor facility. Assuming the Soviets wanted 100% U.S. technology for its proposed facility, where were they obtaining the remaining 80% of the necessary equipment? Our law enforcement operations, Commerce and Customs, have not assumed a proactive approach to detecting where the Soviets intend to obtain needed equipment. It would be possible, however, to more effectively control that which the Soviets have targeted through adequate intelligence to the agents level of operations and by devoting adequate resources to the investigation. For instance, if law enforcement had intelligence that the Soviets were planning to construct a semiconductor plant using predominatly U.S. technology, those agencies responsible for export controls could more effectively monitor the most likely industry to be approached by them. The Soviets have taken advantage of the weak export control efforts of the U.S. to obtain whatever they need. The Soviets, in most instances, know exactly what technology or equipment they need. They contract to procurement groups such as Mueller, Nast, Bruchhausen and others to obtain what is needed. Cost is no object to the Soviets, making it an extremely lucrative line of work for intermediaries. These intermediaries form companies with the U.S. to purchase equipment which is then exported to a friendly West European nation or neutral nation (Switzerland, Austria, or Lichtenstein) and transshipped on to the Soviet Union.

Circumventing or violating the U.S. export controls is a relatively easy task. There simply has not been enough attention or priority devoted to the enforcement of this area. Most federal agencies have little or no jurisdiction in this area. Those that do, Commerce and Customs, have had limited success. The past efforts made by the U.S. to enforce export control laws has been weak. Today, I can state that Customs has given high priority to this area of enforcement and I am optimistic about potential results. Export violation cases require investigation both domestically and abroad. In the past, the U.S. had received little cooperation or empathy from our allied law enforcement agencies when pursuing export violators. Neutral nations strictly

prohibit U.S. investigations of any kind within their countries whereas other allies do not appear to consider the violations serious enough to cooperate. This attitude may possibly be encouraged by our own lack of priority to export violations.

Today, Richard Mueller, Volker Nast, and Frederick Linnhoff are all fugitives from U.S. justice but are free men residing in West Germany. Nast was indicted by U.S. authorities a second time, as late as 1981, for attempting to illegally export a U.S. Munitions list item destined for Hungary; yet he is still a free man in Germany. Starek, Storey and Johnson never served prison sentences, and to my knowledge those U.S. perpetrators in the past received light prison terms and even lighter administrative sanctions. I believe it is time for our Government to approach export control with dedication, priority and with the cooperation and coordination of those agencies who have been mandated with the responsibilities and jurisdiction.

I have read, reviewed and initialed each of the eight pages of the foregoing statement, and I swear to the best of my knowledge that it is true and correct.

CHARLES L. McLEOD

Sworn and subscribed to before me this 10 day of May, 1982.

Notary Public

My commission expires:

Witnessed by me as Acting Special Agent In Charge.

Ms. HILL. Also we have several other statements that I would like to introduce as exhibits to be filed with the subcommittee.

One is a briefing on duel use technology transfer prepared by Col. Kenneth Evans with the U.S. Army, a statement prepared for the subcommittee by the American Society for Industrial Security, a statement prepared by the Computer and Business Equipment Manufacturers Association, a statement prepared by the Electronics Industries Association and a statement prepared by the Scientific Apparatus Makers Association.

[The documents referred to was marked "Exhibits Nos. 33, 34, 35, 36, and 37, for reference, and are retained in the files of the subcommittee.]

Ms. HILL. In addition, we have a bulky exhibit which contains numerous documents and court exhibits which have been received by the staff during the investigation which I would like to make part of the record, and, Mr. Chairman, I would ask that the record be allowed to remain open for about 10 days because we do expect to receive other exhibits that we have requested at this time.

[The documents referred to was marked "Exhibit No. 38," for reference, and are retained in the files of the subcommittee]

Chairman ROTH. So ordered.

Mr. WEILAND. Mr. Chairman, just so it is clear for the record, does minority counsel want to have all of those affidavits and association statements published or merely the affidavits?

Ms. HILL. We want them all in the record as exhibits. Mr. Chairman, we ask that the statements be introduced into the record as exhibits but we ask that only the three affidavits be printed.

Chairman ROTH. With that amendment, it will be so ordered.

[At this point of the hearing, Senators Nunn and Rudman entered the hearing room.]

Chairman ROTH. Senator Rudman?

Senator RUDMAN. Mr. Brady, I don't know whether the reference to historic should have been prehistoric but let me just get a few things straight.

What was the date of your swearing in?

Mr. BRADY. June 13?

Senator RUDMAN. I thought it was last spring.

Mr. BRADY. Right.

Senator RUDMAN. Around the 13th of June, which means you have been on the job now for just a bit short of a year. In terms of results, actually results of getting things turned around, I think you would be the first to say that at this point that really hasn't happened, wouldn't you agree?

Mr. BRADY. In terms of the organizational changes and retraining the personnel, making the changes we want made, you are absolutely right. Senator, I think, however, the changes you are implying should have taken place, do not happen overnight.

Senator RUDMAN. That is exactly what I am getting to. There had been really two or three major criticisms of Commerce and, of course, the suggestion, I think, made out of frustration on the part of many of a transfer.

[At this point of the hearing, Senator Nunn withdrew from the hearing room.]

Senator RUDMAN. I have read with some interest this February 1980 hearing at which you and others testified, and you, yourself, addressed some of those very problems in that hearing.

The problem is that you are now here at this hearing and the burden is on your back. And I think Senator Nunn is probably correct in his assessment of the progress made to date. But believe me, just so we have the record straight, in those two or three areas that you believe were problems when you arrived there, which in response to a question just before we had to leave for that vote, you said would be addressed, you thought with results within 6 months. Just in terms of getting the record very clear at this point in the hearing, let me now just recap those initiatives which you have undertaken that you think will lead to those results over the next 6-month period, so that if we have a hearing 6 or 8 months from now we can now go back to the hearing record and take those items, look at what you have done and see what the results actually are.

Mr. BRADY. Senator, I would first have to preface my remarks by saying that without the knowledge of what the threat was, knowing how the Soviets were operating, we could not take the specific organizational steps that we have taken.

[At this point of the hearing, Senator Nunn entered the hearing room.]

Mr. BRADY. We have, one, created a deputy assistant secretary for enforcement which will vastly upgrade the function in terms of its visibility.

Second, the Compliance Office has already received additional resources in the form of 15 positions for the west coast and we now have personnel actions in process to hire those individuals.

Third, we have created an analytical unit within the Office of Export Administration, cutting across a couple of divisions, as a matter of fact, including the compliance division as well as the licensing division, that is being tremendously successful in terms of showing us the routes of diversion, likely diversions, et cetera.

Fourth, we are creating a foreign availability assessment center. We have an individual on board now and there is recruitment action out for others.

Within the intelligence agency at the prodding of Secretary Baldrige, Secretary Olmer, and myself, there has been created a functional unit totally dedicated to the technology transfer question in terms of intelligence information. This information is now being made available to us.

Every week, and my deputy twice a week, as well as the director of the Compliance Division, the position that is now vacated, we review all of the intelligence leads provided.

Very often we have difficulty on sources and we have to wait to use the information, but nevertheless, we get it. We are using that.

We will be restructuring the office, abolishing positions, abolishing certain units, and I would wrap this up by saying that the Secretary, as well as the Under Secretary, have indicated a total commitment to do whatever is necessary in terms of resources to get the job done.

Senator RUDMAN. So if I understand your testimony correctly, what you are telling us here this morning is that upon taking over last June,

with the background you have and your knowledge of some of the problems, but obviously not all, you proceeded to evaluate the threat, to look at the organization, to meet the threat once you had that evaluation—I assume CIA and DIA probably with their input—and finally sometime midway into your year, you started these four major initiatives, the latest of which has been the hiring of someone who obviously we have a great deal of respect for who understands the nature of the kind of litigation which is highly specialized.

Mr. BRADY. Precisely.

Senator RUDMAN. So you took about 6 months to find out what you really needed. You are now in the process in the second 6 months of organizing that task to meet the threat, to meet the problem, and you are telling us sometime between now and the first of the year, you should be able to come and show us specifically, (a) the evaluation, (b) the implementation to meet the requirements set forth in the evaluation, and (c) the results.

Mr. BRADY. That is right. That is absolutely correct, Senator. I forgot to add the major impetus that we undertook as an administration was to deal with the international aspects of the diversion problem, which are far, far greater than the purely diversion aspects or even the intelligence, counterintelligence problems domestically. We did this, beginning a year ago, when the President went to Ottawa. So to say we have not been very active and very aggressive in the general technology transfer area is simply not consistent with the facts.

Senator RUDMAN. I think in fairness to your committee staff and yourself, the report done by the staff is probably historically correct and it probably is currently correct in some areas because by your own testimony you have only started to implement during this year what you want to do.

In fairness to assess whether or not there ought to be legislative action to change jurisdictional lines, I think we ought to give you an opportunity to do what you think has to be done and then to look at it again at some time in the future.

I have one last very brief question, Mr. Chairman.

In your testimony back in February, I believe it was February 20, 1980, one of the things that you referred to, which is quite understandable, was the difficulty in assessing the nature of some of the items that had to be licensed or decisions to be made on licensing because of their highly technical nature; you were having difficulty at the grade levels of entry into Government service to hire the people with the kinds of technical background to look at a particular chip, microchip, microprocessor, a piece of laser technology, a piece of grinding technology and you say this has very serious implications.

People have to know what they are looking at. My question is: Has that become any better?

Mr. BRADY. No; it has gotten worse. As a matter of fact, Senator, we had thought throughout the Government that the Soviets, or generally for that matter, even the West, were not able to extract technology, to any significant extent, from a chip or a number of high technology practices.

Frankly, we are reassessing it in that respect because they may be able to do it in a better way than they have which makes, again, the problem that much more difficult.

I would not be candid if I didn't say today that this problem is monumental. We are never going to solve it entirely; we are never going to stop the total leakage of technology to the Soviet Union simply because we are a free country. We have free borders. It is just a massive problem, and the things I outline in my oral statement today, such as the growth of multinational communications, the mobility of people, the role of the academic institutions are all vast problems and we will address them, and I think we can make substantial progress in stopping the leakage but it will never be shut.

Senator RUDMAN. What resources do you have available to you to give you the kind of advice that you need to make decisions which are going to be based on the evaluation of highly technical information?

Mr. BRADY. This is one of the areas we have addressed in the last year, and my deputy has addressed much more directly. We are having difficulty because of the grade structure to bring the people onboard, the engineers we need. We have some very good engineers onboard. We need more and we are recruiting for that.

As a matter of fact, one of the things we have done is to try to shrink the support arm of the licensing function to get more actual engineers, people to deliver the product. We have had fairly good success with that. To address the backlog of the 2,000 applications that we had when we came into office, we got on loan from the Department of Defense, as well as NBS, some technicians and scientists to address that backlog.

Senator RUDMAN. Do you still have access to them? Is there any formal or informal working relationship? That is the reason for my question because over at the Defense Department, NASA, and a few other agencies, there are very sophisticated scientists as well as engineers who are able to do some assessments.

Do you have accessibility to them?

Mr. BRADY. We use the Department of Defense personnel, including the people in the labs extensively. I am not sure if there is a formal agreement. DOD has a veto over some of the actions we might want to take and, therefore, they have a statutory responsibility. So that we use them extensively.

Senator RUDMAN. Thank you, very much.

Chairman ROTH. I have no more questions but I would like to make an observation.

I support both what Senator Rudman and Senator Nunn have said. The problem, Mr. Brady, has been too often in these hearings that we hear about plans and then when we hold hearings later, nothing happens. It is very aggravating and disappointing. I don't think that is going to be the case here, but I think that the subcommittee has underscored a very important need for corrective action.

I would urge you to take that action because one of the things I am determined in this committee is that we are going to have follow-through hearings. We are not just going to investigate and forget. I am sure you will agree with that being appropriate.

So I just want to urge that you proceed as expeditiously as possible because sometime later this year or early next year we would like to know what progress has been made.

Mr. BRADY. Mr. Chairman, as you know, the act is up for extension in September 1983, and so we will be going through an extensive

95-929 O - 82 - 20

thought process within the executive branch. I would urge you to take a very close look at us within the next few months to see whether or not we fulfill the commitments that I have expressed today.

I assure you I will do everything in my power to fulfill those commitments, and I have the Secretary's support in that. Again, with regard to the report, I am not going to disagree with portions of that report. I just think that it doesn't tell the whole story.

Chairman ROTH. Senator Nunn?

Senator NUNN. Thank you, Mr. Chairman.

I just have a few more questions.

When you get that Inspector General's report, Mr. Brady, that we all agree is current, having started in April and ended yesterday, I would like for you to give us your answers to that.

Mr. BRADY. Absolutely.

Senator NUNN. Let's get your answers and whether you think it is historic or micro, little things like whether law enforcement people carrying out law enforcement tasks, have law enforcement capabilities, whether that is micro or whether that is macro, I guess it depends on whether you are running the Commerce Department or the world.

Anyway, we would like to get your evaluation of that report.

Just a few other questions. I know you have heard about section 12(C) of the Export Administration Act. That is the section that deals with proprietary information, and I know there has been a source of friction between Customs and Commerce on that.

We got information from Customs that there were about 24 cases that were held up or could not be completed by Customs because of not getting information from Commerce on that. I am not suggesting it is a simple problem and easy answer. But what has been done in that area?

Mr. BRADY. Senator, with regard to those 24 cases, I have had a number of people look over those and there are some we simply are not aware of in terms of any problems. I have to admit that there has been a problem between Customs and Commerce and Commerce and some of the other agencies concerning 12–C, business confidential information. I think with regard to Commerce and to Customs, that problem has been primarily at the working level.

I assure you that it has been worked out, that we no longer have that problem. We have negotiated or are negotiating memorandums of understanding with all the intelligence agencies and with Customs and the FBI regarding sharing of information. There is still the problem that we must, according to our law, get a Secretarial determination if the information is going to be used in the public, disclosed to the public.

[At this point, Chairman Roth withdrew from the hearing room.]

Mr. BRADY. I understand there is a divergence of opinion as to what we construe as public and what the Department of Justice construes as public, so we will address that. But the 12–C problem which has existed, which I concede has probably been used at times by Commerce individuals inappropriately, is behind us.

Senator NUNN. I am encouraged on that point. We will follow that with interest.

You have been critical yourself in the past with the licensing function of the Commerce Department. We have centered so far on the

Compliance Division in questions and so forth. But what has been done in the licensing areas? What do you plan to do to improve the things you pointed out in the past yourself?

Mr. BRADY. Basically three things, Senator. One, when we came into office, we wanted to have a review of the policy, and we got that. So that the President, before he went to Ottawa and discussed the whole East-West trade situation with our allies, did so on the basis of an extensive, indepth policy review which was agreed upon. We have probably had more NSC meetings in this area in the last year than have ever been held previously with regard to the whole subject matter.

We have policy guidance from the highest level, both with regard to the Soviet Union, with regard to Eastern Europe, with regard to the PRC, and with regard to the pipeline and the oil and gas question, as a matter of fact. That is one area.

Second, the interagency machinery that was in existence but had no life under the previous administration has been put to use and from the top on down. We have an Export Administration Review Board which is chaired by the Secretary and that has met on a couple of occasions to decide certain cases and policy elements. The rest of the structure, namely what we call the ACEP, which is chaired by me at the Assistant Secretary level, my deputy at the Deputy Assistant Secretary's level, and staff level is working and working well. The issues are being resolved and I believe we can verify that with the fact that we had over 2,000 cases that were over the statutory deadlines in the process when we came into office a year ago.

They have been eliminated. We have something like 30 or 40 cases, depending on the particular week we are in, which are over the stated timeframes and, frankly, there will always be a handful of those. That doesn't mean we have done the task in terms of, one, interagency cooperation, or in looking at what should be controlled, because that is based on the policy decisions that were made by the President a year ago.

We went to our allies, both in the NATO framework as well as in the Cocom system, and we got a political direction in January and we are now moving to redesign the list of controlled commodities so that we move away from what was controlled in the fifties and sixties when we concentrated on products. We are now focusing on technology, design, manufacturing, and production of technology.

Senator Rudman referred to microprocessor chips. In the final analysis there is no way we can keep somebody from walking into Radio Shack or any computer store in the country and buying a handful of those chips and putting them in a diplomatic pouch and leaving. We recognize that. But it's the technology to make that chip or that microprocessor which is really important to the Soviets, and that is what we are trying to concentrate on, particularly in nondefense priority industries.

Senator NUNN. I certainly agree with that priority, and I think that one of the most important things is to have a continuing update of the critical technologies that the Soviets are likely to target and are likely to need and to really prioritize those. That is not to say that others are not important, but to concentrate on those and to educate the pri-

vate sector on those. I don't believe there is any way that the Government of the United States, no matter what you do in the Compliance Division or the Licensing Division, no matter what State, Defense, Customs, no matter what they do, they are not going to be able to control this problem without tremendous cooperation from the private sector.

It seems to me, forgetting our disagreement on compliance right now, that one of the areas Commerce really can move forward in is this educational campaign, and you are in contact with businesses. They do respect you. You do have a little leverage there. They will come to meetings when Commerce talks. So I think it is very important for you to carry out this education function.

I consider that the most important function Commerce has got, even if you have everything ironed out in the Compliance Division, I think that pales in comparison because of the limitation of the numbers, and so forth, and because of the ability to try to educate and stop this stuff at the source rather than at the borders.

Mr. BRADY. Senator, I agree with you entirely.

Senator NUNN. Stuff is not a good word for high technology. We will strike that word. Just high technology transfer instead of stuff.

Mr. BRADY. What we are talking about is a massive problem. In a way, industry is behind the times because they are worried about certain aspects of their security and they have allowed it to go unnoticed. That is a task in the Department. It is a task we have spent quite a bit of attention on. Frankly, we are sending out to the field something like 60 additional Commerce individuals that are associated with our field offices, who are normally associated with trade activities, but whose job is also to educate the business community on the needs if they are exporting.

There is no exporting seminar that is ever given in this country without either participation from the Office of Export Administration with regard to the needs of licensing. It is a complex function and it is one that we are going to try to do a lot more of.

Senator NUNN. Regarding the critical list, you can let business know in these seminars what is on that list. Then private industry, those who are loyal and patriotic, and that is 99 percent of them in my view, will, I think, pay close heed to this. A real educational campaign about internal security also would be useful. I know the bigger businesses have it. Sometimes it is not very good. But smaller businesses sometimes don't even think about it.

A lot of our technological innovation is coming from small business people. I would say most of them.

Mr. BRADY. That is right.

Senator NUNN. I would hope you would really bear down in the educational effort. It seems to me that Commerce has a unique kind of capability in that respect because you do have people out in the business community, with your seminars, and other programs. Of course, I think on the other side, Customs has a real law enforcement advantage because they have people who are naturally involved in that all the time. But nevertheless, I would hope you would really give top emphasis in the Commerce Department to that educational function.

Mr. BRADY. We will, Senator.

Senator NUNN. Assume all your plans take place, everything happens in the Compliance Division that you have outlined and 6 months from now you come back here and say we have done all of these things, we have corrected all the problems, we have all the people, so forth, what then do you envision as your role with compliance?

For instance, will you have people that visit airports, will you have people that visit ports? What will the Compliance Division in the Commerce Department in a perfect world be doing?

Mr. BRADY. Senator, assuming that Customs continues its inspection operation, the Exodus operation, I think it would be duplicating that action for us to be doing inspections for inspections sake. That doesn't mean we would not send special agents when they are working on a case to a particular port, but I think it is important that we not duplicate what, in fact, is done by Customs and can be done better because they do have the manpower at the ports, as far as inspections are concerned.

Senator NUNN. The same thing would be true with airports?

Mr. BRADY. Yes, sir.

Senator NUNN. You are saying all ports?

Mr. BRADY. I am saying all ports, water and airport. So I would not expect us to have an inspection function as such. I would expect us to have a very strong special agent force that works closely with the CIA and FBI to get the leads to get at the diversion problem. We do get them, but there are sometimes problems because we can't use them because of the sources. To get at the diversion problem, our efforts will also include an education campaign. That also spills over to other agencies in Commerce, both in the United States and overseas, personnel helping us extensively in our enforcement efforts.

When we get a case of licensing and we don't know the end user, we request information from our personnel overseas.

Senator NUNN. I am going to have a few observations at the close of the hearings and one of them is going to be that licensing should remain at the Commerce Department. So my critique of Commerce is going to be on the Compliance end as well as other things. But what I am trying to get at, in a perfect world when the Compliance Division is operating effectively and efficiently as you envision it, what are you going to be able to do that Customs can't do? That's the central question. If you are not going to have them at ports of exit and you are not going to inspect and so forth, and I agree with that. I think you are absolutely right on that, it would be duplicative. But if they are not going to do that kind of thing, it seems to me that what you are describing is really a liaison between law enforcement and licensing.

Mr. BRADY. I think it is more than that. Senator, it goes to the fact that the inspection at the ports of exit which Customs does is a small part of the problem, a very small part of the problem, and none of the major cases we have had have grown out of inspection of crates at the ports. What we need are special agents who can prosecute investigative cases.

Senator NUNN. That is the Justice Department.

Mr. BRADY. I mean prosecute to the point of turning the case over to Justice.

Senator NUNN. You mean investigate special cases?

Mr. BRADY. Precisely, investigate diversions, work with the FBI and the CIA to get the information.

Senator NUNN. Why can't the FBI do that? What is it that Commerce brings ——

Mr. BRADY. FBI deals with espionage only.

Senator NUNN. This comes darn close to espionage. The *Bell* case and other cases it seems to me are very, very close to espionage. I can't understand what it is Commerce brings to this that the FBI or Customs doesn't already have.

Mr. BRADY. It brings the entire knowledge and expertise of what is licensed for dual-purposes. In other words, which computer requires a license, which doesn't, where they are going, the fact that before we license cases we must get a rundown on some of the end users.

Senator NUNN. Why can't the FBI or Customs do that?

Mr. BRADY. Because they just don't.

Senator NUNN. They don't——

Mr. BRADY. Frankly, the working relationship with Customs has not been all that high and it is not one sided.

Senator NUNN. I am not shocked to hear that after a year of investigation.

Mr. BRADY. And I am not pointing fingers. I think the close association between what the enforcement arm that we envision with a licensing process, as well as with the intelligence community is going to provide the insight, the expertise to go out and investigate the cases that are truly the major cases. And the analytical unit that we are talking about that we have established in recent months, for instance, is coming up with a substantial number of cases. This is just as a result of the information we have.

Senator NUNN. Looking back for a moment historically, has there been a major case that you can identify that Commerce has done the majority or the bulk of the investigative work in and has been successfully prosecuted?

Mr. BRADY. Well, I know both the *Spawr* and *Maluta* cases, Senator, were closed out by Customs at one point. If it had not been for a certain inspector in our Division, there is a very good question as to whether those cases would have been prosecuted.

They are two of the largest cases we prosecuted in recent years.

Senator NUNN. We have heard testimony that the agent that you had who handled those cases is an excellent agent and did a very good job. I think we are in agreement on that. Do you have any others?

Mr. BRADY. There are four cases now—well, there are more than four cases now. But I understand there are four cases that are either in transmission to Justice or are there for criminal prosecution so that, again, the criticism is valid, however——

Senator NUNN. How many years have you had a Compliance Division?

Mr. BRADY. I believe it goes back to 1949. Yes.

Senator NUNN. We would like for you to furnish for the record all the significant cases in which Commerce has played a major—I won't say the major, but a major investigative role.

Mr. BRADY. OK. Senator, two points. One, I do not think it is necessarily bad that Commerce, once it discovers a lead or once it

begins an investigation, has to go to the rest of the Government for help.

Senator NUNN. I don't either.

Mr. BRADY. I think that is the kind of coordination this Government desperately needs, and we are trying to accomplish it. I think that I, Ed O'Malley, Willy Von Raab, and the CIA have made great strides in this direction.

There is another point, however, which we have not discussed this morning, and that has been the legislative participation in the whole technology transfer process. Beginning in 1969, this act was changed and over the 1970's, every extension was successively liberalized to not only permit but actually to encourage the executive branch to be more liberal in terms of its exports. In retrospect, that was a mistake. But the point is that through the 1970's, there was not a very strong compliance arm simply because the whole process was not viewed as all that important because after all, we were establishing détente with the Soviet Union, and we were going to industrialize them without technology.

Senator NUNN. I certainly think that is an accurate observation. I do not think there is any doubt about that. That is an attitudinal situation that existed for a long time.

Let me ask you a couple of other questions. Have you looked into the grain embargo enforcement effort by the Commerce Department?

Mr. BRADY. Senator, I am aware——

Senator NUNN. Without asking any leading questions, why don't you tell us what you think about that since we both agree that is historic but perhaps also indicative?

Mr. BRADY. The President lifted the grain embargo because he said that others had moved in and simply taken up the slack that we had tried to curtail. Grain is an impossible commodity, as you know, to trace.

I am aware of the criticism in the report that there was one agent assigned to the enforcement of the grain embargo.

Senator NUNN. In the Commerce Department?

Mr. BRADY. Right.

Senator NUNN. He was responsible for all compliance and enforcement, is that right, for Commerce?

Mr. BRADY. I understand that he worked on an interagency committee, and he was the Commerce representative.

Senator NUNN. Wasn't Commerce the designated agency to enforce the grain embargo?

Mr. BRADY. Yes; it would be, but it was an interagency effort in terms of acquiring information. From what I understand, there are few agricultural exporters. Unlike a computer, it cannot be packaged in a small box. A ship leaving with a grain shipment is a fairly visible item. I am not condoning 1 person, and I am not even sure that 15 people can enforce the grain embargo. I don't know.

Senator NUNN. You would be pretty certain one can't; wouldn't you?

Mr. BRADY. Absolutely. I do know that as a result of what we call the "Great Grain Robbery" in the early 1970's, that transactions can actually, before start and finish, go through 40 different hands before a grain shipment finally gets to its destination.

I think there is a real problem with trying to enforce that kind of an effort, and based on the resources that they had, Mr. Chairman, I am not sure, in view of the high technology concerns and their impact on the military of the Soviet Union, I would prefer the agents in the high technology area rather than in the grain area. I was not at Commerce at the time the decisions in this regard were made.

Senator NUNN. Even if this was a major part of the President of the United States foreign policy at the time, one of the major moves he made in the whole 4 years? If you were President Carter and the Secretary of Commerce came over and the President said to him, "Oh, incidentally, Mr. Secretary, how many people do you have working on the grain embargo enforcement?" Would you want to reveal to President Carter at that stage—I am not saying whether the policy is correct. That is a macrodecision. Let's talk micro. Would you want to be the Secretary of Commerce who came over and said to President Carter, "We have got one person who is sitting in the Commerce Department making sure that everyone complies with your grain embargo. He hasn't had time to leave the office for the last 6 months because he is so overwhelmed with reports, but we have priorities elsewhere." Would you want to be the Secretary of Commerce who conveyed that message?

Mr. BRADY. Well, if that Secretary had told the President that it was unenforceable to begin with, I wouldn't mind being that Secretary. But I do not know if the President was ever told that it was unenforceable.

Senator NUNN. I would doubt very seriously anybody told him one person was working on it. That becomes a self-fulfilling prophesy if you only have one person working on it.

Of course, based on Commerce records, there was 100 percent compliance anyway. Maybe we didn't need enforcement.

Mr. BRADY. Senator, I am not going to condone one person being assigned to the grain embargo.

Senator NUNN. That again, is historic and I hope we can learn by that.

Whether Presidential policy is correct or not and whether it really is completely enforceable or not, I do not think is a decision for people who are supposed to carry it out to make. I think they have to do the best job they can with resources.

Let me ask you one other question. Have you heard of the *Polamco* case?

Mr. BRADY. I am aware of it, yes.

Senator NUNN. This is a case where we heard considerable testimony. William Bell, a Hughes Aircraft radar specialist, was convicted of selling military secrets to Polish spies. The President of Polamco, or the President-designate of Polamco was convicted and according to all information we had was really pretty much admittedly an agent of the Soviet Union. This was a case made by the FBI.

We understand Polamco is a company that is still not on the denial list of the Department of Commerce. Is that correct, and if it is correct, could you tell us how that situation operates?

Mr. BRADY. There is a difference between the denial list, which is the result of an administrative proceeding where a company is denied export privileges, and a screen where we review license applications against the possible problem companies. It is my understanding that

the company is on screen and not on the denial list. It is not denied export privileges because we do not have the authority to deny it.

Senator NUNN. What is the screen?

Mr. BRADY. The screen is a review. It is a list of the companies of individuals against which a license application is checked initially when it comes into the office.

Polamco is on that screen but it is not denied export privileges. It is my understanding that we do not have "an export administration case" against the Polamco. As you know, it is, I think a Polish company chartered under the laws of California or Illinois. That is a growing phenomena that concerns law enforcement people throughout this Government.

Senator NUNN. What do you have to do to have an export administration case? I assume you are saying to be on the denial list there has to be a case made?

Mr. BRADY. That's right.

Senator NUNN. Will you walk us through that? In order to get a company on an export denial list, what has to happen?

Mr. BRADY. We either have a criminal prosecution or administrative prosecution with sanctions being levied. As a matter of fact, one of the real——

Senator NUNN. You had a criminal prosecution here.

Mr. BRADY. But not under the Export Administration Act. It was an espionage, I believe, prosecution. And there is a difference. We do not have the legal authority to do what you and others would like us to do.

Senator NUNN. Doesn't that law need to be changed, then?

Mr. BRADY. It may well, Senator, it may well. And the whole area of Communist firms chartered in the United States is, we believe, ripe for diversion. It is one we are looking at. There are constitutional questions as to whether we can require Federal Government approval prior to those companies being chartered in the United States. We are looking at a reporting requirement.

Senator NUNN. We are talking about two things, as to whether they are chartered and the second thing is whether they can export.

Mr. BRADY. They can export legally if they come in and get a license application and we grant it to them, which is a big "if." If they export illegally, then we can prosecute them. We cannot, however, prosecute them for, first, being chartered here or, second, acquiring technology within the United States. And that is what is taking place.

In other words, these Communist-owned chartered entities are acquiring U.S. technology and we are concerned that it is one of the strong vehicles by which it is leaving the country. That is something that a number of individuals and organizations are looking at and working on.

Senator NUNN. What do you have to have in order to put somebody on the denial list? Tell me that again.

Mr. BRADY. Again, a criminal prosecution——

Senator NUNN. Criminal prosecution only under the Export Administration Act.

Mr. BRADY. Or an administrative prosecution. I will have to turn to——

Senator NUNN. If you have a lawyer here, let's have the lawyer explain the exact state of the law here.

Ms. BREED. In order for a company——

Senator NUNN. Give us your name.

Ms. BREED. Pamela Breed.

In order for a company to be placed on the denial list, we would have to go through an administrative procedure which is a charging letter alleging certain acts had taken place, give the respondent an opportunity to answer the charges and perhaps go to a hearing on the charges before a hearing commission.

Senator NUNN. That would be a civil proceeding?

Ms. BREED. Civil proceeding.

Senator NUNN. What are the grounds for your bringing that?

Ms. BREED. For a civil proceeding?

Senator NUNN. Yes.

Ms. BREED. A variety. Illegal export, re-export, diversion, causing, aiding or abetting a violation.

Senator NUNN. Wouldn't the *Polamco* case, when the president of the company has been convicted of espionage——

Ms. BREED. It is a violation of the Export Administration Act.

Senator NUNN. The only thing that you can put them on the denial list for is for violating the Export Administration Act.

Ms. BREED. That is right.

Senator NUNN. I thought you just listed several other reasons.

Ms. BREED. Aiding and abetting in violation of the Export Administration Act.

Senator NUNN. It is a very narrow statute. You can only put someone on the denial list if they have been convicted of an Export Administration Act violation. You bring a proceeding alleging violation of that act.

Ms. BREED. Alleging violation.

Senator NUNN. Even if they committed espionage, that is not grounds for denial?

Ms. BREED. That is correct. You have to tie in the sanction under an act to the violations in the act.

Senator NUNN. You are saying there would be a constitutional problem if we were to amend the law and say if you have been convicted of espionage, that there be ground for civil proceedings under the Commerce Department.

Ms. BREED. There could be a problem. We have not studied that aspect of it.

Senator NUNN. It seems to me this is a very large loophole, Mr. Secretary.

Mr. BRADY. Senator, yes, it is, and it is one of the things that we are looking at. I started to say that we are looking at the constitutionality and legality of a reporting requirement to require that, one, a firm is chartered when it is reported to us, or when they acquire technology within the United States, they report it to us. But, again, it is a question as to how much enforceability there is to that kind of provision. It is a problem that we are all looking at and I think as we go through the next few months, particularly later this year or early next year, in looking to the extension of this law, this is very definitely one that we all should concentrate on.

Senator NUNN. I certainly agree.

I would like to formally ask, Mr. Brady, you give us your opinion after consulting with your legal department as to exactly what that

act provides, and what needs to be done in the view of the Commerce Department to plug up the loophole if it is as large as it appears to be.

I am going to ask the staff to pose a similar letter to the Attorney General and have him look at it, too.

Mr. BRADY. Senator, it may be we can actually use as one of the sanctions in an espionage prosecution the denial of export privileges to an individual form.

Senator NUNN. It seems to me that is something that would be logical. Senator Rudman, I know I have taken too much time.

Senator RUDMAN. Mr. Brady, thank you very much. This concludes 5 days of hearings on this subject.

You will, of course, respond to those questions asked for the record.

Senator NUNN. Mr. Chairman. I do have a statement.

Senator RUDMAN. Proceed with your closing statement.

Senator NUNN. Thank you, Mr. Chairman. Mr. Secretary, we thank you for being here today. We don't agree on everything. I know you are sincere in your efforts and will continue to work on it. We will continue to follow your progress with a great deal of interest, both in licensing and in compliance.

I would like to make a statement giving my observations here as to what we have learned in the last 5 days and at least a partial list of recommendations that Senator Chiles and I will at least make to the subcommittee. These are certainly not subcommittee findings. That will be for the full subcommittee to make a decision on.

The Senate Permanent Subcommittee on Investigations has concluded 5 days of hearings on the transfer of American technology to the Soviet Union and Soviet bloc nations.

The hearings, in my view, underscored the need for improvement in U.S. efforts to halt technological drain, both in the governmental and private sectors.

Based on information developed in the hearings, we believe the subcommittee should recommend to the full committee and the Senate the following legislative proposals and corrective actions.

First, the Soviets dedicate substantial resources to highly focused and increasingly adept attempts to secure American technology. By contrast, the American response often has been unorganized.

A restructuring of American efforts to halt undesired technology transfer is called for. Through improved intelligence, we must determine what it is that the Soviets want and then model our response accordingly. Our Government should seek to prioritize the critical technology the Soviets need for military purposes and devote considerable efforts to education and enforcement of the prioritized items.

No. 2. there is a need for reassessment of the ability of the Department of Commerce to carry out its present enforcement responsibilities under the Export Administration Act. Commerce presently carries primary law enforcement responsibility, with secondary jurisdiction resting in the U.S. Customs Service.

Commerce maintains both licensing and enforcement under the act; by contrast, under the Arms Export Control Act, those functions are handled separately by the Department of State and the U.S. Customs Service.

And I might add we understand from both State and Customs that that arrangement has worked very smoothly.

The enforcement responsibilties under the Export Administration Act should be altered, first, by delegation of full enforcement responsibility to the U.S. Customs Service, with the licensing function remaining at the Commerce Department. In addition, for a long-range solution, Congress should consider the concept first put forward by Senator Garn to create an Office of Strategic Trade that, among other things, would absorb the functions of the Office of Export Administration.

I reserve final judgment on that. I certainly think that should be the focus of another hearing, Mr. Brady, after you get a little further along with your licensing proposal. Because I can see some real advantages in having the licensing and education functions that I already enumerated that I think should be your top priority in one department.

No. 3, the Export Administration Act should be amended to include as a criminal offense, the possession or attemped possession of restricted goods with the intent to export such goods unlawfully.

Hearing evidence established the many difficulties law enforcement authorities encounter in the prosecution and investigation of export offenses. One problem lies in the absence of any offense until a suspect actually exports the goods in question.

When arrest is delayed until the moment of export, law enforcement necessarily risks the loss of territorial jurisdiction if the subject departs the country. In export cases, where the offense is often nonextraditable, that risk can be fatal to the success of the case.

No. 4, the enforcement tools currently available to the U.S. Customs Service should be broadened. Consideration should be given to granting Customs officers express statutory authority for warrantless arrest, search or seizure in cases of outbound cargo and persons, generally equivalent to that authority which Customs now possesses in cases of inbound cargoes and persons. Express statutory authority would embrace Customs' effectiveness in full enforcement of the export laws. This authority has been implied by the courts in some cases.

No. 5, the Federal electronic surveillance statutes should be amended to permit court-ordered surveillance where there is probable cause to believe that a violation of either the Export Administration Act or the Arms Export Control Act is being committed. As with the recommendations to Customs' authority, this revision would enhance law enforcement's ability to investigate complex export cases.

No. 6, the RICO statute should be amended to include, as predicate offenses in proving racketeering activity, violations of the Export Administration Act. Export violations often have been treated as "minor" offenses, resulting in minimal sentences. Prosecution under RICO would expose offenders to a possible 20 year prison sentence.

No. 7, the Freedom of Information Act should be amended to eliminate the application of the act to information requests made by foreign nationals. Faced with the disclosure of sensitive information to foreign nationals, "cottage" disclosures industries, and others, such statutory revisions would inject a reasonable sense of national security considerations into disclosure practices mandated by the Freedom of Information Act.

No. 8, the Department of State should seek mutual assistance treaties between U.S. allies and neutral nations to obtain greater law enforcement cooperation in the enforcement of export laws.

The State Department should seek the inclusion of export violations as extraditable offenses in agreements with foreign governments.

No. 9, the region in Santa Clara County, Calif., popularly known as the Silicon Valley, the heart of America's growing microprocessor industry, is a prime target of Soviet efforts to transfer sensitive technology. Yet we were told that a strong Federal law enforcement presence has been lacking in the Silicon Valley in the past. State enforcement efforts must be supplemented by a Federal interest in the problem. We note assurances from the FBI that it is aware of this problem and is taking steps to increase its presence in the Silicon Valley and other high technology centers. The Bureau is to be commended for its corrective action in this regard.

No. 10, the technology transfer problem is, by all indications, a massive one requiring the attention of both the Government and the private sector. Law enforcement and industry spokesmen suggested that many high technology companies remain unaware of the extent of the problem. Reportedly, industry interaction with the Commerce Department is inadequate; unfamiliarity with the lists of controlled exports is common within the industry. The FBI's DECA program, aimed at improving the level of communication with the private sector, directly educates companies involved in Defense contracts with the problem of technology transfer. The Defense Department has begun a similar program with the business community. There is a need for similar governmental programs designed to inform the private sector dealing in sensitive but nonclassified technology.

No. 11, private industry must contribute directly to any effort to halt the technology drain. There is a lack of sufficient security precautions at the sources of production in the technology industries. Lax security measures were cited in some Silicon Valley plants. William Bell, a Hughes Aircraft engineer convicted of selling military secrets to Polish spy Marian Zacharski, had access to sensitive information on the basis of a security clearance which had not been reviewed in 28 years. The private sector, through the efforts of individual enterprises and trade and professional associations, should be encouraged to maintain more effective security measures in plants producing sensitive high technology items.

Massive Soviet efforts to obtain our technology resources can be countered only through vigorous Government and law enforcement efforts, bolstered by the strong support of America's high technology industries.

I might add, Mr. Chairman, that there will be other recommendations. We will have some detailed recommendations on the Department of Defense and I will have others, but at this point in time, I did want to submit those as initial observations by Senator Chiles and myself.

Senator RUDMAN. Thank you, Senator Nunn.

I am sure there will be other observations and conclusions reported out by other members of the subcommittee and possible suggestions that will be joined together.

Certainly I commend the chairman and the minority staff for your leadership in these hearings which I think are informative and will lead to improvement on a very serious situation.

This subcommittee will adjourn now subject to the call of the Chair.

[Whereupon at 12:27 p.m., the subcommittee adjourned to reconvene at the call of the Chair.]

INTENTIONAL
BLANK

APPENDIX

PREPARED STATEMENT OF SENATOR WILLIAM S. COHEN

Mr. Chairman, I am pleased to have this opportunity to participate in these hearings to examine the ability of our government to enforce our export control policy.

Congress passed the Export Administration Act and the Arms Export Control Act to establish a mechanism for controlling the export of materials which might damage our national security. The administration of this policy requires a careful balancing of competing interests. Our economic goal of promoting exports must be weighed against protecting our technological lead upon which our national security is based. And the freedoms of our academic community to conduct research without government intrusion must be weighed against the extent to which Soviet technology can benefit from U.S. science.

An area that has been of particular concern to me is that of academic exchanges. These occur through personal letters, visits, journal articles, and conferences and can be beneficial to the well-being of both nations. However, in certain circumstances, exchanges can be counterproductive and damaging to our national security. American students studying in the Soviet Union, for example, study marriage patterns in that country between 1897 and 1975 and the economy of Catherinian Russia. At the same time, Soviet students in the United States are studying chemistry, physics, laser technology and applied computer science.

Recent events, however, call into question the adequacy of existing policy to address these concerns. According to press reports, the Soviet Union has increased its covert operations to obtain technology that can be used for military purposes. Similarly, we must question why, for example, Soviet officials nearly won approval of an export license for industrial material until the Defnese Department noted that the same article is used by the U.S. Air Force to improve the hardness of our concrete missile silos. Perhaps most disturbing of all is the dis-

covery by Pentagon officials of Soviet electronic circuit boards. The computer chips in this circuit worked perfectly when American chips were used as replacements, providing evidence that the technology had been copied. This is the very technology on which the Pentagon is relying for our future weapons improvement.

I would like to commend Chairman Roth for his timely investigation of this critical issue. I look forward to examination of how the government's resources and information could be utilized to promote a more effective export control policy. Specifically, we need to address the current staff allocations at the Commerce Department where only 25 investigators are charged with the entire responsibility for export controls even though there are more than 300 exit points throughout our country. Since the U.S. Customs Service has more investigative resources, does it make sense to transfer responsibility for the Export Administration Act to this agency? And how can the information collected by our intelligence agencies be used in a more effective manner in the enforcement of our export control policy?

I believe that the efforts of the Administration in reviewing our export control policy should be commended, and I look forward to working with them to develop an improved policy.

PREPARED STATEMENT OF SENATOR HENRY M. JACKSON

Mr. Chairman:

I congratulate you, and Senator Nunn, and the Members and staff for holding these hearings. The problem of assessing the loss of our technology and developing effective measures to control its transfer is one of the most important facing the United States.

Documents and other information made available to the Senate by the Select Committee on Intelligence, of which I am a member, as is the distinguished Chairman of this Subcommittee and the Committee on Governmental Affairs, Senator Roth, establish that the Soviets are pursuing a purposeful and determined campaign in this field. Their activities are numerous, diverse, and well-funded. And they have, in far too many cases, been successful. We now know, and I believe these hearings will further demonstrate, that in many ways the United States has in effect been supporting the metastasizing power of the Soviet Union. As I stated in remarks to the Senate several weeks ago, "There is no longer doubt that our technology has materially aided Soviet expansion. It has improved Soviet weapons, intelligence devices, and economic leverage."

The need for a clear and comprehensive technology transfer policy is compelling and urgent -- yet our government still has a long way to go.

PRIOR SUBCOMMITTEE RECORD

The hearings we begin today continue this Subcommittee's distinguished history of investigation and legislation concerning technology transfer problems. Our past activities have included detailed scrutiny of particular licensing issues, such as the Dresser Industries case, as well as studies of broader related issues, such as East-West financial credits. The Subcommittee's review of this latter problem, I might note, was conducted about five years ago, and it accurately presaged the Soviet bloc debt issues that are causing such serious concern today.

95-929 O - 82 - 21

The Subcommittee also laid the groundwork for significant legislation. During the 1970s, the Department of Commerce was regularly approving licenses for exports of strategic goods and technologies to Soviet bloc nations without adequate analysis of the adverse impact on American national security. In 1974, legislation based on the Subcommittee's work helped correct this problem by amending the Export Administration Act to provide for Department of Defense review of certain applications for export licenses and permits. In 1979 this approach was improved and expanded with further amendments to the Export Administration Act, again based on Subcommittee work. These amendments assigned the Secretary of Defense primary responsibility for identifying control list items, as well as military critical technologies and goods.*

The critical technologies concept is intended to lead to tighter control over transfers of design and manufacturing know-how and production capabilities while relaxing control over products not transferring such knowledge. A related element of legislation requires that the implementing regulations take into consideration the difficulty of devising effective safeguards to prevent diversions of critical technologies to military use, to protect critical goods such as computers, and to prevent the re-export of critical technologies to third parties.

Another 1979 amendment to the Export Administration Act was designed to correct a major deficiency that the Subcommittee's work had identified in U.S. licensing procedures. Except under special circumstances an export to adversary nations may not be denied if comparable goods or technology is available from foreign sources in substantial quantities. But it was found that determinations of foreign availability had been predicated on unsubstantiated assertions by exporters and superficial analysis.

*I might add that Senators Nunn and Cohen of this Committee, as well as Senator Moynihan, the Vice Chairman of the Intelligence Committee, joined me in 1979 in sponsoring these and other key amendments.

The 1979 legislation dealt with this problem in three ways. First, it requires that any determination of foreign availability must be made in writing and be supported by reliable evidence, which specifically excludes uncorroborated representations by an exporter. Second, it indicates Congressional intent that the President initiate negotiations with other potential suppliers when he has reason to believe that they may make controlled items available to an adversary nation. Third, the legislation mandates that all departments and agencies that have export control responsibilities share foreign availability information.

CURRENT PROBLEMS

Despite this effort, it has become clear that Soviet actions to acquire our technology have seriously outstripped our preventive undertakings.

In recent months there seems to be greater public concern about this problem. Such concern is a promising development, because there are so many ways that Soviet acquisition efforts exploit our open society. Our first defense here is public awareness. These hearings can help substantially by further documenting the Soviet threat to our technology and providing a better base of public information about this subject.

These hearings will, I am sure, identify many of the improvements needed in our transfer control policies and procedures and develop the basis for appropriate remedies. In this context, I want to highlight five matters that strike me as continuing sources of weakness in our national efforts.

One is the slowness in implementing the critical technologies approach called for in the 1979 legislation. In large part, this delay has been due to inadequate funding of the Defense Department's undertaking. In addition, the policy-related activities in Defense -- particularly those dealing with such crucial matters as relations with allies in NATO and

COCOM -- are seriously lacking in permanent staff and support. These shortcomings have impeded progress on major policy matters as well as the day-to-day processing of licensing cases. A related problem is that current regulations do not require license approval for exports of most critical technical data to most non-Communist destinations. This loophole, of course, presents significant opportunities for leakage of our technology to the East.

Second, the government's current approach to questions of "foreign availability" remains a source of weakness. The Commerce Department has primary responsibility for monitoring and gathering of foreign availability information, but its capabilities to do so appear to have been and to remain seriously inadequate. It is also not clear that the intelligence community's role in these matters has been sufficiently strong, wide-ranging, or coordinated. On the other hand, when it has been evident that foreign availability does substantially exist, the government has not vigorously implemented the 1979 Congressional intent regarding negotiations for cooperative controls. Too often, it seems, U.S. export licenses have been granted based on untested assumptions that our allies would not cooperate with us in controlling the items in question.

A third major weakness of current U.S. controls is the government's willingness to accept end-use representations to permit the export of dual-use technologies and items even when those certificates are essentially unverifiable. The current Administration, better attuned rhetorically than its predecessor to the dangers of technology loss, approved the sale of pipelayers to the Soviet Union with the understanding that those machines would not be used on the Siberian gas pipeline proposed for Western Europe. But because there is simply no way that national technical means can differentiate a pipelayer from that sale under those assurances from one that was sold a year earlier under no such assurances, and because there is no

on-site inspection of engine block numbers, end-use representations are irrelevant if not downright sham. Computers provide another example of items in which such representations are irrelevant or spurious. There are no functionally related observable differences in a computer when it is working on military problems rather than civilian ones; even on-site constant observation of the machine will not reveal whether it is being "diverted" in part or in whole to military tasks.

The fourth weakness is that current U.S. controls fail to include all equipment and technologies relating to oil and gas development in the national controls list of strategic defense industries. I have twice written President Reagan on this matter; in the more recent letter, on 8 March, I urged that the Administration act "to finally recognize the strategic importance of energy supplies and to start treating technologies and end-products related to them accordingly. Procedurally, this would mean giving the Secretary of Defense the same review over exports of oil and gas equipment that he now has over strictly military exports." (I ask unanimous consent that the text of this letter and supporting materials be included as part of the Record.)

The immediate problem that prompted this letter is the proposed East-West gas pipeline between the Soviet Union and Western Europe -- a pipeline which, when completed, would provide the Soviet Union with huge amounts of hard currency, estimated by some to reach $6 to $8 billion, which in all likelihood will be used in significant part to acquire and exploit further Western technology for Soviet aims. In the face of such strategic consequences, it would be disastrously short sighted to permit the transfer of pipeline-related technology on the grounds that it has no immediate military applications.

Fifth, the strategic trade policy of the United States does not include credit controls. Current Soviet and Warsaw Pact shortages of hard currencies suggest that those countries would be getting a lot less of our technology if they had to pay for it on a cash-and-carry basis. The Subcommittee, as I noted earlier, has been a pioneer in terms of Senate attention to the matter of Western credits for the East. Today the debt of the Warsaw Pact countries to the West is about $80 billion. Poland is unable to service its $26 billion share of that debit, and there are increasing signs that Moscow's hard currency shortages are mounting. The export of Western capital through extensions of credit permits the Soviets to fortify their military-industrial system every bit as much as the transfer of technology. We need to develop comprehensive controls on credits to the East and work with our allies to forge an effective multilateral approach.

Mr. Chairman, there are other improvements that should be made promptly in our national system of export controls; I have not touched, for example, on the complex problem of enforcement. I understand that our hearings will address this matter. But there is one aspect of the enforcement matter I should mention. During the course of its oversight studies of technology transfer and loss, the Intelligence Committee staff has found that responsible intelligence and law enforcement agencies have encountered significant difficulty in obtaining relevant information from the Department of Commerce. The Department of Commerce has asserted that, before this information can be released, the Secretary of Commerce must make a special finding in each case. The delays involved in these case-by-case determinations by the Secretary of Commerce have significantly impeded effective counterintelligence and law enforcement investigations, particularly those of the FBI. I understand that this problem is still unresolved after months of inter-Departmental negotiation,

NEED FOR COMMITMENT

Mr. Chairman, this set of hearings will help focus top-level attention by the Administration on these technology transfer matters. There is, I believe, no single step that would have greater consequences for improving our national posture. It is unfortunately still true that there is much that could be done here -- what is lacking, in large measure, is the political will to do it.

Room 131
Russell Senate Office Building
Washington, D.C. 20510
(202) 224-5641

United States Senate
WASHINGTON, D.C.

ENERGY AND
NATURAL RESOURCES
ARMED SERVICES
GOVERNMENTAL AFFAIRS
INTELLIGENCE

March 8, 1982

The President
The White House
Washington, D.C.

Dear Mr. President:

Some seventeen months ago, on November 14, 1980, I sent you a letter questioning the Carter Administration's policy of excluding the oil and gas industry from the list of strategic defense industries, and its policy of presuming that licenses would be granted for the export of oil and gas equipment. I urged you to reassess this position as part of an overall national security assessment of the world energy situation. As I received no acknowledgment or response to my original letter, I am presuming that you did not see it. It may have been held at the staff level.

Meanwhile, the potential catastrophe of Moscow's gas pipeline to Europe underlines what I was warning about. In view of the serious threat of that pipeline to U.S. and allied interests and future security, and given your own current consideration of U.S. policy toward the pipeline, I want to be sure you see my original letter to you and my recent speech to the Senate on the issue of technology transfer and loss, during which I made that letter public.

In my speech, I summarized the danger of the pipeline as follows:

> "Only on the surface is this deal an economic one, whereby the Western Allies provide funding and technology in exchange for Soviet natural gas. Both sides, in fact, are fully aware of the significant political relationships involved. The pipeline deal will provide Moscow with a substantially increased flow of hard currency and political leverage for years to come, and we would be reckless to gamble that these resources will not be used against us and our European allies. For one thing, Moscow's revenues from the pipeline will facilitate acquisition in the West of sophisticated technology useful in strengthening the Soviet military. Even without direct Soviet action, the project creates the possibility that significant portions of allied economies and societies could fundamentally shift away from the West toward the Soviet Union. There would be massive diversion of energy-related capital, talent, and effort away from Western economic development."

I know that at Ottawa you made known your own concerns with the Siberian pipeline, but for one reason or another the Administration did not get itself together for an effective follow-up. You must be aware of the widespread dismay in Congress that our government is still hemming and hawing about a project that would indefinitely profit our adversary some $7 to $8 billion in hard currency annually. This dismay on the Hill has now boiled over into threats to "bring the boys home from Europe," and into other isolationist portents which you and your colleagues should be taking with utmost seriousness.

I believe there is still time for the Administration to rally itself against the pipeline.

Specifically, I urge you to prohibit the use of any American technology in connection with the pipeline, to press American lending institutions not to extend credits or other financial assistance that might be related to this deal, and to use your personal authority to persuade the American multinational oil companies involved not to participate in the project.

We must recognize that in talking about opposing the pipeline we are talking about energy self-sufficiency for the industrialized West, and so we are talking about protecting the Western alliance, not damaging it. Therefore, I urge that you promptly convene meetings at the highest allied levels to develop alternatives for Western European energy. The United States should provide substantial assistance in developing such alternatives, including technological and financial measures. And we should provide strong incentives for our allies to develop Western energy supplies rather than Soviet ones.

Also, this strikes me as an opportune time to finally recognize the strategic importance of energy supplies and to start treating technologies and end-products related to them accordingly. Procedurally, this would mean giving the Secretary of Defense the same review over exports of oil and gas equipment that he now has over strictly military exports.

It is my hope that this letter and the enclosed material will further encourage your personal involvement in the critical current issues of technology transfer.

With best wishes.

Sincerely yours,

Henry M. Jackson

Henry M. Jackson, U.S.S.

Enclosures

[illegible]

[illegible]

[illegible]

RICHARD A. HYDMAN
CHIEF COUNSEL AND STAFF DIRECTOR

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS
SENATE PERMANENT SUBCOMMITTEE
ON INVESTIGATIONS
WASHINGTON, D.C. 20510

[illegible]

MARTY STEINGALOS
CHIEF COUNSEL
[illegible]
GENERAL COUNSEL
W. P. GOODWYN, JR.
STAFF DIRECTOR
JOSEPH B. BLACK
CHIEF COUNSEL TO THE MINORITY

November 14, 1980

The Honorable Ronald Reagan
President-elect
of the United States
901 South Highland
Arlington, Virginia 22204

Dear Mr. Reagan:

For several years now, the Senate Permanent Subcommittee on Investigations has been concerned with the transfer of technology, directly and through third parties, to the Soviet Union and other Warsaw Pact members. Evidence adduced in the Subcommittee's studies and hearings has demonstrated that our policies in this area have been seriously flawed and have enabled the Soviets and their allies to acquire technology which has contributed significantly to their military-industrial capabilities.

The protection of our technological lead times is crucial to the maintenance of strategic parity with the Soviets. To achieve this objective it is necessary that the U.S. develop a coherent, consistent and effective policy to prevent the transfer of security-sensitive technology to our adversaries.

During the past two years, some steps have been taken in the right direction. In 1979, Congress adopted certain amendments to the Export Administration Act which are designed to strengthen national security controls. Also, subsequent to the Soviet invasion of Afghanistan, the Carter Administration took some long overdue actions to restrict exports of high technology to the Soviets. However, these efforts are only in their early stages. Much work remains to be done before years of mismanagement and neglect can be corrected. In the following I have outlined my major concerns.

1. A Clear and Comprehensive Policy

During the past decade, our strategic trade policy has been made on an ad hoc, license-by-license basis, generally at a fairly low level in government. Top level policy guidance has consisted largely of short-sighted notions of detente or trade promotion which were not grounded in a thorough national security assessment of technologies and their relative importance in the military balance between the U.S. and the Soviet Union and other adversary nations. Indeed, the government has lacked an adequate ongoing assessment capability. As a consequence, evaluations of technical criteria such as the military significance of the technology and foreign availability were shaded in order to justify license approvals or were otherwise inaccurate. The quality of analysis has also suffered due to chronic shortages of qualified personnel who must process over 70,000 license applications annually within statutory deadlines.

The lack of a clear and effective policy has resulted in other problems such as U.S. government agencies working at cross-purposes, inconsistent decisions, uncertainty for U.S. exporters, and the weakening of COCOM as an effective multilateral control mechanism.

Deficiencies in controls on technology transfer have not been limited to the export licensing area. The U.S. has engaged in educational and other technical exchange programs in which the benefits have flowed almost exclusively to the Soviets and their East European allies. Moreover, there has been inadequate official review or control over the nature and extent of technology transfer in these arrangements.

In addition, the U.S. has not had an adequate program to enforce our export control laws, despite aggressive Soviet efforts to acquire controlled and classified technology through clandestine and illegal means both in the U.S. and abroad. For example, the Defense Intelligence Agency recently told the Senate Committee on Governmental Affairs that the Soviets and some of their allies have acquired interests in or have established businesses in the U.S. in order to acquire restricted technical data and equipment.

An important task for your Administration will be to develop a clear export control policy based upon a comprehensive technological assessment and to communicate that policy downward to the officials charged with its implementation. My views as to additional elements of this policy are discussed below.

2. The Critical Technologies Approach and the Department of Defense

In response to the foregoing problems, a bi-partisan group of Senators co-sponsored my amendments to the Export Administration Act of 1979 which gave the Secretary of Defense the primary responsibility for identifying militarily critical technologies and goods and formulating controls to prevent their transfer to our adversaries. The critical technologies approach is intended to lead to tightened controls on know-how and to the relaxation or modification of controls on products which do not transfer technology or have significant intrinsic military capability. On October 1, 1980, the Department of Defense published its initial version of a critical technology list. On the same day, the Department of Energy separately published its significant input to the list. Significant additional technical analysis and regulatory work is necessary before the critical technology list can be fully integrated into the export control system, as contemplated by Congress.

This work should be completed on an expeditious basis so that we can have the kind of assessment capability necessary for an effective policy. To do so, DoD will require adequate funding and staffing as well as the active support of the Energy Department and other governmental agencies and the business community. In its fiscal year 1981 budget request, DoD asked for $2.5 million to continue support work on this project. I am concerned by reports that DoD is planning to allocate only half the funds requested. I am also concerned by the failure of DoD to adequately staff its export control activity. In view of DoD's significant responsibilities in the strategic trade area, I believe it would be helpful if DoD established a separate budget line item for this activity.

My views concerning the critical technologies project are discussed in more detail in my letter of October 1, 1980, to the Secretary of Defense, a copy of which is enclosed.

3. Foreign Availability

An important factor in determining whether to export an item to an adversary nation is whether the item would be available from foreign sources in sufficient quantity and quality that denial of export would be ineffective. My 1979 amendment to the Export Administration Act requires that any determination of foreign availability which is a basis of a decision to approve a license or remove a control on the export of a good or technology shall be made in writing and be supported by reliable evidence. This provision should be stringently enforced.

At the time of enactment, the Export Administration Act in September 1979, neither the Commerce Department nor any other agency of government had an adequate foreign availability assessment capability. Unfortunately, this continues to be the case today. Although the Commerce Department is assigned the primary responsibility for coordinating the collection and monitoring of information on foreign technology, this responsibility of necessity must be shared by DoD, the intelligence community, and other agencies with export responsibilities. In order to carry out Congress's mandate, the agencies need to be mobilized and adequately staffed and budgeted (including provision for travel funds to investigate allegedly competitive technology).

When a good or technology which would make a significant contribution to the military potential of an adversary is determined to be available from foreign sources, this should not lead to automatic approval of the export as has been the case too often in the past. Instead, negotiations to secure cooperation in restricting availability should be initiated immediately.

If the United States resumes its position of leadership, I believe that our allies and friends will be inclined to cooperate in multilateral control efforts. Should a nation refuse to cooperate with the United States in denying alternative sources it hardly enhances U.S. credibility to compete to sell the very item we had argued would be contrary to our security interests for the other nation to sell. If you determine that you need additional authority to encourage other nations to cooperate in multilateral controls, I would be happy to support appropriate legislation.

4. Exchange Programs

Since the invasion of Afghanistan, the Carter Administration has imposed more stringent control on a number of government-to-government technical exchange programs with the Soviet Union. There currently is an informal interagency body which reviews some aspects of certain exchange programs. The scope of the body's responsibilities needs to be expanded to assure that Soviets and other adversaries are not gaining access to critical technologies in private and commercial exchange programs, as well as in governmental arrangements. To achieve this objective, I believe the new Administration should formulate a policy to guide the decision-making of the review body. In this regard, the Soviet Union and other adversaries should be denied technologies, if the Secretary of Defense determines that such access would adversely affect national security, subject, of course, to the final decision of the President. This is consistent with the intent of Congress in the Export Administration Act which gives the Secretary of Defense such a veto in the licensing and control list area.

5. Enforcement

During the past several months, the Carter Administration has been conducting various interagency studies of problems in the enforcement of export control and other laws which protect controlled and classified technologies. Recently, the Department of Commerce announced that it has stepped up its enforcement of the Export Administration Act. However, that Department still does not have an adequate investigative and support staff to enable it to carry out an effective program. A thorough assessment of our government-wide enforcement program is required, including the adequacy of (a) resources, (b) coordination of the U.S. agencies internally and with foreign governments, and (c) existing legislation.

6. Post-Afghanistan Developments in Export Policy Toward the Soviet Union

Since the invasion of Afghanistan, there have been a number of changes in U.S. strategic trade policy toward the Soviet Union. These changes are generally steps in the right direction, but I have had some reservations. One of my broader concerns is that the Carter Administration has suggested that these steps are intended as a short-term response to the invasion, rather than as part of the development of tighter control policy for the long-term. For example, President Carter stated that he hoped that, if the Soviets withdraw from Afghanistan, we can restore normal trade relationship with the Soviets.

A firm and consistent policy is essential if we want our friends and allies to take us seriously when we ask for their cooperation. The reluctance of our COCOM allies to give specific or formal support to some of the recent U.S. proposals may be attributable in important part to questions about the seriousness and steadiness of U.S. intentions. I think it would be helpful to the successful implementation of the new policy, if you would tell our allies that these new policy directions represent a long-term strengthening of U.S. controls on the transfer of security-sensitive technology.

I also have a number of concerns about the substance and implementation of the new policy.

(a) The Administration has stated that it will not approve exports to the Soviets of items which are under COCOM control and which require formal COCOM permission prior to export. But the policy provides for possible exceptions on a case-by-case basis for spare parts for computers and other previously exported items. A large number of spare parts cases have been held in abeyance. I see no persuasive basis for granting exceptions for spare parts for items which we would not presently export.

(b) The new policy provides for tightening criteria used in reviewing applications for the export of technology, including process know-how for plants in militarily relevant industrial sectors (e.g., trucks, aircraft, metallurgy). A large number of significant technology cases have not been decided because of delays in formulating specific criteria. Development of interim criteria should proceed as quickly as possible so that these cases can be decided. Long-term criteria should be developed in the critical technologies project.

(c) The new policy provides for careful review of proposed exports to Eastern European countries to assess the risk of diversion to the Soviet Union. The implementation of this policy should be carefully examined.

(d) The Carter Administration has established a presumption of denial for exports of technology for manufacturing oil and gas production and exploration equipment. However, I understand that no effort has been made to enlist the support of our allies for this policy. Although the U.S. has dominance in certain oil and gas technologies, a multilateral approach would make the policy more effective.

The Administration has also continued its policy of presuming approval of exports of oil and gas equipment. I believe that the equipment policy should be reassessed by your Administration as part of an overall national security assessment of the world energy situation.

I am gratified by your letter of October 24, 1980, expressing support for the Jackson-Vanik Amendment. I very much hope that you also share my basic point of view concerning our strategic trade policy and that your new Administration will accord this matter a high priority.

Sincerely yours,

Henry M. Jackson

Henry M. Jackson
Vice Chairman

SENATOR JACKSON / News

U.S. Senator Henry M. Jackson of Washington (202) 224 9378

FOR RELEASE: P.M.'s
Thursday, February 11, 1982

TECHNOLOGY TRANSFER POLICY -- THE HIGH STAKES

Address by Senator Henry M. Jackson

U.S. Senate Floor - Thursday, February 11, 1982

Mr. President, as my colleagues are aware, my concern for the flow of security-sensitive technology to the Soviet Union and its allies is of long standing. For several years, the Senate Permanent Subcommittee on Investigations, which I chaired, demonstrated through its studies and hearings that our policies in this area have been seriously flawed. Moscow and its associates have acquired the West's latest technology and thereby significantly enhanced their military-industrial capabilities. I and several others have repeatedly pressed for tighter controls on technology transfer.

NEED FOR A CLEAR, COHERENT POLICY

On November 14, 1980, I wrote President-elect Reagan calling his attention to this problem and suggesting several measures that merited his prompt consideration. I noted the lack of a clear and comprehensive policy regarding technology transfers which had led to inadequate technical analysis, weaknesses in export controls, serious imbalances in East-West exchange programs, inconsistent governmental decisions, uncertainty for U.S. exporters, and a weakening of COCOM. I urged that he act quickly to strengthen the government's work on critical technologies, foreign availability assessments, national security safeguards in exchange programs, cooperation with allies, and enforcement.

In the fifteen months since that letter was sent, events have reinforced my earlier conclusion: there is much we can do, if only we will. But we have a long way to go.

There is no longer doubt that our technology has materially aided Soviet expansion. It has improved Soviet weapons, intelligence devices, and economic leverage. We are still much too far away from a vigorous program to effectively meet the danger.

MOSCOW'S GAS PIPELINE TO EUROPE

As proof, Mr. President, we need only consider the Administration's handling of the Siberian gas pipeline project.

In my November 14, 1980 letter to President-elect Reagan, and my enclosed letter of October 1, 1980 to Secretary of Defense Harold Brown, I questioned the policy of excluding the oil and gas industry from the list of strategic defense industries, and the policy of presuming that licenses would be granted for the export of oil and gas equipment. I urged the new Administration to reassess this position as part of an overall national security assessment of the world energy situation.

Yet the Administration started off by approving a first shipment of Caterpillar pipelayers to the Soviet Union. It is claimed that these pipelayers will not be used on the West Siberian pipeline, a generous supposition given Soviet practice of violating end-use representations. More importantly, in licensing this equipment, the Administration sent the signal that in principle the export of technology and products relating to oil and gas production and shipment are not considered strategic items.

President Reagan at Ottawa made known U.S. concerns with the West Siberian pipeline, but the Administration didn't get itself together for an effective follow-up. It took the crackdown in Poland to energize the government. And even now high officials are talking about the decision regarding U.S. technology and the pipeline in terms of "weighing the damage to the Soviet Union against the damage to the alliance."

What accounts for the confusion and the footdragging?

Because this pipeline project is supposed to be a strictly economic arrangement? Nonsense. If it is, why have the Germans so steadfastly rejected serious consideration of any alternatives to dealing with the Soviets? The United States has offered some alternatives, and a pipeline to exploit Norwegian gas was also proposed. The price of Siberian gas promises to be quite high. Furthermore, the deal requires an enormous amount of Western credit, at a time when the German government is joining many others in complaining about the price of money.

Only on the surface is this deal an economic one, whereby the Western allies provide funding and technology in exchange for Soviet natural gas. Both sides, in fact, are fully aware of the significant political relationships involved. The pipeline deal will provide Moscow with a substantially increased flow of hard currency and political leverage for years to come, and we would be reckless to gamble that these resources will not be used against us and our European allies. For one thing, Moscow's revenues from the pipeline will facilitate acquisition in the West of sophisticated technology useful in strengthening the Soviet military. Even without direct Soviet action, the project creates the possibility that significant portions of allied economies and societies could fundamentally shift away from the West toward the Soviet Union. There would be massive diversion of energy-related capital, talent, and effort away from Western economic development.

What we should be doing is quite plain.

First, we should recognize the strategic importance of energy supplies and treat technologies and end-products related to them accordingly. Procedurally, this means giving the Secretary of Defense the same review over exports of oil and gas equipment that he now has over strictly military exports.

Secondly, we should recognize that in talking about energy self-sufficiency for the industrialized West we are talking about protecting the alliance, not damaging it. The Administration should immediately prohibit the use of any American technology in connection with the pipeline. It should promptly convene meetings at the highest allied level to develop alternatives for Western European energy. It should provide substantial assistance in developing such alternatives, including technological and financial measures. And it should provide strong incentives for our allies to develop Western energy supplies rather than Soviet ones.

RECENT IMPROVEMENTS

Mr. President, certain developments of the past months encourage me to hope that some effective steps will be taken, both on the Siberian pipeline and for broader issues of technology transfer.

Most importantly, key assumptions about the importance of trade to détente are now critically questioned. During the past decade, three Administrations acted on the assumption that increasing economic ties with the Soviet Union would moderate Soviet behavior in ways that would improve our security and build a peaceful world order. With this assumption came a consistent effort to relax controls on strategic trade with the East and to define quite narrowly what we meant by "strategic" trade.

Today, we can view those years as a costly experiment. The results included an increasingly adverse military balance, both strategic and conventional; renewed Soviet military expansionism; increased Soviet subversion in the Third World; a sharp escalation in the anti-U.S. Soviet political offensive around the globe; and a dramatic increase in Soviet espionage and clandestine operations against the West. Our technology, acquired and exploited by Moscow, contributed to each of these developments. There is now a growing awareness that our technology in Soviet hands is a threat to our security.

Also of importance, there is a broader appreciation that the Kremlin is determined to try to get our technology by any means available. The public press, as well as government reports and defense estimates, have reported how Western developments in design, materials, components, and production have been acquired by our adversaries. The techniques have included classical espionage as well as the evasion of export controls through diversion, re-transfer, and the use of foreign-owned but U.S.-chartered front corporations. The result has been weapons aimed at us that are higher in quality, greater in quantity, more lethal in effect, and quicker in the field than would likely have been the case if Moscow had to rely solely on its own technical/industrial base.

The present Administration has begun some remedial action. The Department of Defense is taking the export control problem more seriously than before and is beginning to improve its ability to evaluate and control critical technologies. There seems to be more awareness in licensing decisions about the need to safeguard national security as well as to advance commercial interests abroad. And the intelligence community has sharpened its awareness of this threat and has begun implementing new procedures to monitor, evaluate, and report on technology transfers and developments.

95-929 O - 82 - 22

CONTINUING SHORTCOMINGS

Mr. President, these new beginnings are a fragmentary start. What is needed is a clear, comprehensive government-wide policy that frontally addresses the hard, central issues of technology transfer and loss. To date, the Administration has lacked the top-level conviction and participation needed to shape such an overall policy.

Time Perspective

For one, it is not yet clear that the Administration's efforts have deeper roots than a concern to impose sanctions. They should. Technology transfers involve vital long-term issues of our national security, and they should not be turned on and off for foreign policy considerations of the moment. It may be appropriate to use normal commercial exchanges of butter and grain to reward and punish Soviet behavior. But national security concerns must be protected in times of cooperation as well as strain, and judgments about the wisdom of transferring certain technologies should be separate from the prevailing winds of foreign policy advantage. I am not sure that we yet have a firm national conviction on this matter, and I am worried that our recent efforts will not outlast the current sanctions resulting from events in Poland.

National Security Perspective

In this regard, it is important to emphasize that national security involves more than strictly military considerations. The notion of "strategic" trade needs a much broader interpretation than it received in the past ten years.

The Siberian gas pipeline is a salient example.

Even purely civilian/commercial transfers can indirectly help increase the Soviet threat to our security. By acquiring and exploiting Western technology, Moscow has been able to fill selectively gaps in its industrial base and to profit from the modernizing effects of, for example, Western microelectronic and computer technologies. It has been able to concentrate funding and manpower on other priority projects, and to alleviate consumer dissatisfaction. By taking Western "proven designs" as road maps, Soviet research and development activities have saved funds and important developmental time.

The point is not that all trade should be stopped on national security grounds. Many of our exchanges with the Soviets are only remotely linked with security threats, and the level and quality of such exchanges are the appropriate province of commercial and foreign policy considerations. But the fact that a particular exchange involves nominally commercial/civilian technologies does not ipso facto mean that national security is unaffected. The key here is informed judgment -- the United States needs to examine carefully the possible effects of each proposed transfer.

Dual-use Technologies

This is particularly true for transfers involving "dual-use" technologies, items proposed for sale for civilian/economic purposes but which could readily find military applications as well. There is now a clear pattern of such diversions once Western technologies are in Moscow's hands. The U.S. government allowed American business to build the Soviets a truck plant at Kama River, somehow assuming that only civilian trucks would be built there. As we all know, that plant builds military vehicles as well -- some of which carried Red Army units into Afghanistan.

Our experience with several other cases is similar. For example, American bearing grinders licensed for sale to the Soviet Union contributed greatly to various Soviet military programs. In other cases, we have seen that there is no real control over the use to which a computer is put once it is under Kremlin control; that another "truck" plant supported by American technology produces missile launchers; and that Soviet plants to produce farm machinery also produce weapons.

But requests for U.S. export licenses are still processed under a system that is biased against protecting national security. The political pressure exerted by commercial interests together with our government's structure and system for processing such licenses effectively create a presumption of license approval. The onus of disapproval then falls on small, underfunded governmental units that are asked in effect to prove that such transfers will be diverted to military ends -- definitive proof that is often only available once our security has in fact been breached. Experience suggests reversing this approach -- the risks of diversion are high, and great caution is necessary.

Allied Cooperation

I am also concerned that we have not achieved more progress toward effective controls with our allies in COCOM. Recent discussions led to several agreements in principle which appear to promise more vigorous cooperation in the future. But it is particularly true of these matters that the "devil is in the details." Alliance-level mechanisms for oversight and harmonization of national efforts on technology transfers are still inadequate. National-level procedures are also still quite weak; among our allies, only France has a national approach to export licensing similar to ours in providing formally for military advice and review.

At the same time, the inadequacy of COCOM measures has helped corrupt our national control systems. Arguments based on the "foreign availability" of even dual-use technologies are repeatedly and successfully pressed within our government to permit transfers. There is little sense in permitting transfers that could threaten our security merely because the items could be obtained elsewhere; logic like this would have parents supplying heroin to their children. A punitive unilateral approach, however, risks creating a system of penalties that would have the effect of driving high-technology firms abroad. Dealing effectively with this type of problem requires strong allied cooperation, which the Administration should do much more to encourage.

Other Measures

Furthermore, there is too little recognition of the fact that problems of technology transfer and loss require more than effective export controls. Moscow's campaign to acquire our technology is sophisticated, diverse, and well-coordinated. Opportunities are fully exploited: visits and exchanges, exploratory contract discussions, academic meetings and programs, public information services, and applications under the Freedom of Information Act. Covert and clandestine methods, however, have virtually become the method of preference for the Kremlim, apparently because they are so effective. A host of espionage techniques are involved, including intercepting communications, suborning or otherwise recruiting personnel, and theft and black-market operations. And all of these techniques are in addition to the methods I noted earlier to avoid and evade our export controls -- illegal diversions, front and dummy corporations, and foreign re-transfers.

ACTION NEEDED

Specifically, Mr. President, I urge the following improvements and innovations in government programs:

First: The role of the Defense Department needs to be considerably strengthened. Responsibility for defense concerns with technology transfer should be centralized in a policy level office with adequate resources to discharge DoD's responsibilities regarding license applications as well as intelligence monitoring and cooperation with our allies. In previous years, DoD failed to fund its technology transfer offices adequately to perform its statutory role. Congress should consider this need specifically in reviewing the FY'83 budget and earmark funds for it, preferably by establishing a separate line item.

Second: The role of the Intelligence Community should also be strengthened. The Senate Select Committee on Intelligence, of which I am a member, has been particularly interested in problems of technology transfer and loss. Initiatives to improve our intelligence process in this area have recently been undertaken by the Administration, and we will look carefully at their budget requests and performance. Here again, earmarked funds might prove helpful. Particularly important is the structuring of the policy process so that coordinated, current intelligence from the community as a whole can be brought to bear on policy judgments about technology transfer and loss. Sound information and analysis cannot alone ensure prudent policy decisions, but it will help considerably.

Third: All U.S.-Soviet exchanges and agreements need to be carefully reviewed for full reciprocity -- not just on paper, but in practice. Academic exchanges, for example, should involve people of comparable professional level and interests as well as simply equal numbers. It is particularly important that we keep in mind the difficulties posed by such exchanges and agreements for our foreign counterintelligence programs, and that we strive to reduce the exploitation of our political freedoms by hostile intelligence services. Here, too, Congress should investigate how legislation could help to accomplish genuine reciprocity in our dealings with the Soviet Union and its allies. An important part of full reciprocity would be requiring the disclosure of ownership for communist-owned U.S. chartered commercial entities.

Fourth: More far-reaching public awareness programs need to be implemented. The FBI and Defense Department have begun awareness programs of the hostile intelligence threat for U.S. defense contractors, and various concerned officials have been cooperating with the press in bringing this story to the public. Much more needs to be done, however, particularly to make the academic community aware of the threat from hostile intelligence agencies. Information and awareness are more secure safeguards than censorship.

Fifth: Consistent and determined U.S. leadership is required to forge an effective consensus on these matters within COCOM. Sustained evidence of a serious U.S. conviction to control transfer and losses is the key to effective allied cooperation. Both our government and the governments of our allies can be victims of "union-busting" pressure from large commercial interests. Congress should undertake hearings and investigations aimed at reducing this and other obstacles to improving COCOM's effectiveness.

Sixth: Strategic trade policy should include credit controls. The Soviet lack of hard currency means that a great deal of the hemorrhage of our technology might be restricted if the Soviets and their allies had to pay for their acquisitions in cash at time of purchase. Today the debt of the Warsaw Pact countries to the West is about $80 billion. Poland is unable to service its $26 billion share of that debt, and there are increasing signs that Moscow's hard currency shortages are mounting. The export of Western capital through extensions of credit permits the Soviets to fortify their military-industrial system every bit as much as the transfer of technology. The United States, in concert with its allies, should begin now to develop a multilateral approach to comprehensive controls on credit to the Soviet Union and its allies. This might be done under the aegis of COCOM.

Seventh: Technology transfer control considerations should be incorporated into the design and production of sensitive advanced products. For years, the United States government and others have struggled with the problems of controlling loss of selected technologies by political and diplomatic means. Many of these problems could be obviated at the engineering stage. Semi-conductors and integrated

circuits, for example, could be coated with commercially-available substances that would preclude reverse engineering of the products, thereby improving both national and proprietary security. Counter-intelligence considerations should be incorporated more systematically at the earliest stages of product development.

Eighth: The contribution of business to effective export controls should be strengthened. The export business community has long played an important role in the formulation of export control policy. Their advice is sought on technological advances and types of controls. In the course of the critical technologies studies conducted by the Department of Defense, representatives of our nation's leading aerospace, electronics and other high technology have made a substantial contribution.

In at least two other ways business can make a broader contribution.

One is in the area of foreign availability. I urge business to aid our government's efforts in developing effective allied controls. In effect, I am inviting American businessmen to "blow the whistle" on companies that put greed above Western security.

Second, I urge exporters to develop voluntary procedures to further the aim of national export controls. Recent Soviet practices in this country make it especially desirable now that American businesses know their customers and the ultimate use and destination of their products. Perhaps Congress can help here by legislation requiring some form of identity and end-use certification for purchasing agents of foreign nations.

* * * *

Mr. President, what I said on April 30, 1980 about the post-Afghan strategic trade policy of the Carter Administration is still applicable: "the flaws in our export controls are due to an absence of conviction, not of resources; it is within our capacity and that of our allies to remedy them. It is still possible to improve our export controls. But the time is long overdue to translate rhetoric about our tough new policy into effective action."

TALKING NOTES FOR DR. LARA H. BAKER, JR., TO THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

In my testimony today, I would like to follow up on Senator Nunn's opening statement in which the senator constructed, for purposes of discussion, a composite of a department within the Kremlin whose sole function is to obtain strategic and dual-use technology from the United States, Japan, and from other Western democracies.

In an interview published in US News and World Report on March 8, 1982, the Director of Central Intelligence, Mr. William Casey, said:

> We have determined that the Soviet strategic advances depend on Western technology to a far greater degree than anybody ever dreamed of. It just doesn't make any sense for us to spend additional billions of dollars to protect ourselves against the capabilities that the Soviets have developed largely by virtue of having pretty much of a free ride on our R&D. They use every method you can imagine--purchase, legal and illegal; theft; bribery; espionage; scientific exchange; study of trade press, and invoking the Freedom of Information Act--to get this information.
>
> We found that scientific exchange is a big hole. We send scholars or young people to the Soviet Union to study Pushkin poetry; they send a 45-year-old man out of their KGB or defense establishment to exactly the schools and the professors who are working on sensitive technologies.
>
> The KGB has developed a large, independent, specialized organization which does nothing but work on getting access to Western science and technology. They've been recruiting about 100 young scientists and engineers a year for the last 15 years. They roam the world looking for technology to pick up. Back in Moscow there are 400 or 500 assessing what they might need and where they might get it--doing their targeting and then assessing what they get. It's a very sophisticated and far-flung operation.

Thus, Senator Nunn's composite is basically accurate. There are offices and bureaus within the Kremlin, throughout the USSR, and throughout the Soviet Bloc, whose principal purpose is to transfer high technology from the West to the Soviet sphere of influence. I will describe several of the vehicles the Soviets use in their efforts to obtain our strategic technology, and then give some examples of how successful these efforts are.

Classical Espionage

The newspapers are full of accounts of how Soviet and Soviet Bloc individuals, some of whom have diplomatic immunity, have been involved with traditional hand-in-the-safe spy rings. We have all seen photographs in national magazines about the communications intercept apparatus at the Soviet embassies and consulates. These traditional methods are used primarily to obtain high-priority technology that cannot be obtained through less risky techniques. The effectiveness of these methods is shown by the amount of effort the Soviets put into them and by the amount of priority they give these activities. Such traditional theft methods are most effective at obtaining technology that is considered most sensitive by our side.

A recent trial in California gave public evidence of the extent of Soviet Bloc efforts in acquiring information on a proposed US satellite system at TRW, Inc. The trial of two US citizens, Christopher Royce and Andrew Dalton Lee, showed the extent and effectiveness of the Soviet espionage activities. In this case, the Soviets supposedly acquired the Top Secret details on a proposed communications system for the CIA. I am not knowledgeable about the classified details of the system. In this case, all I know is what I read in the newspapers. Regrettably, such Soviet espionage efforts are not rare.

Open Literature and the Freedom of Information Act

We live in a free society and are proud of that fact. One of our greatest strengths is the information transfer that our Constitution allows and that we encourage among our own people. Tapping into this information flow is an extremely fruitful technique for the Soviets to use. The United States government is the focus for much of the information flow on sensitive, high-technology items. Through use of the US government repositories set up to handle unclassified documents and through use of the Freedom of Information Act (FOIA) to retrieve formerly classified or currently classified documents, foreign agents have been able to acquire information of significant strategic value. Also of high importance is the fact that they have been able to tie up a significant quantity of US government resources. These resources are dedicated to answering Freedom of Information Act requests, checking for downgrading and classification of documents, and evaluating national security implications of compilations of documents. Many US government agencies have had to set up offices to handle these requests and divert highly competent people from analysis activities to evaluation of FOIA requests, some from foreign nationals.

In our society, one of the most treasured freedoms is free speech. This reaches its epitome in the freedom of organizations to produce periodicals covering whatever they wish to talk about. As a result, magazines in this country, such as Aviation Week and Space Technology, carry a large quantity of information of particular defense interest. While these publications do serve an extremely useful purpose in keeping the defense community informed about the complex activities going on in the Free World, they also provide a conduit for information to the Soviets. Information suggests that the Soviets place a very high priority on Western technical journals, including providing translations in near real time with publication. In many cases, the information available in these journals is of higher quality than that available in government documents.

Student Exchanges

As part of the spirit of detente, the US and the Soviet Union entered into student exchange programs. This was a particular coup on the part of the Soviets, since the best technology transfer organization in the world is the United States university system. In the US universities, a very large number of highly qualified, highly motivated, superbly trained people spend their working lives trying to come up with better ways to transfer technology to their students. These people are called university professors. It's their job, and they do it very well.

Currently, approximately one-half of the graduate students in the United States are not US citizens. The non-US fraction for many science and engineering programs is higher. Projections indicate that by 1985 at some universities, such as the University of California at Berkeley, up to 90% of the graduate students may not be US citizens. This is particularly worrisome when one considers the quality of graduate education available in the United States.

While there are US Government restrictions on Soviet participation in graduate programs, these restrictions are not applied as stringently to Soviet Bloc students. Strong evidence indicates that information that is transferred to the Soviet Bloc is immediately available to the Soviet Union. Thus, the best in US graduate studies is available, albeit indirectly, to the Soviets. This helps alleviate the Soviet problems with training really first-rate engineers.

As an example of the kind of information that is available, let us examine some Electrical Engineering programs. At several United States universities, including MIT and Cal Tech, one can start a particular program in Electrical Engineering with a blank notebook; at the end of one year, the successful student will leave this particular set of courses holding in his hand a microprocessor chip, a microprocessor being a computer on one integrated circuit. During that year, the student will have used computer-aided design to design the microprocessor, he will have used computer-aided layout to lay out the processor on silicon, manufactured the chip either in the laboratory or in collaboration with a manufacturer, tested the circuit, packaged the circuit, mounted the microcomputer on a printed circuit board, and made the resulting computer work. Thus, in one year, the student will have been exposed to an intense, carefully orchestrated program covering the United States integrated circuit industry. This would have been done under the supervision of experts, with careful hand-holding throughout the program to make sure that the student understood his activities. Fortunately, evidence indicates that the number of foreign students who have gone through these programs so far is minimal.

Foreign-Owned Corporations

The tangled web of ownership of many US corporations obscures the identity of their true owners. In the event Eastern Bloc or Soviet corporations exist in the United States, they can be recipients of US technology without the donors of that technology realizing that the information is going to a foreign government. This kind of foreign ownership of US corporations presents a potential serious hazard. I have not delved into this particular topic enough to give detailed examples.

Scientific Exchanges

Again, as part of detente, the US entered into several bilateral agreements with the Soviet Union on various scientific and technical subjects, including atomic energy. As part of these agreements, the US furnished technical information and equipment, such as a superconducting magnet for a Soviet magnetohydrodynamics (MHD) system. This magnet was produced with state-of-the-art US machining and quality control equipment, and was far beyond anything the Soviets could build for themselves. It was loaned to the Soviets as part of an exchange agreement in return for participation in the MHD experiments.

The loan of the magnet to the Soviets was approved after review by the DoD, the DOE, and various intelligence agencies. It was felt that the US would acquire experience operating the magnet in a facility whose equivalent would not exist in the West before 1986 or 1987. Since all the US technical reviewers agreed that the Soviets could not reverse-engineer the magnet to acquire the critical manufacturing techniques, the loan was approved.

We received some return, but, as often happens in scientific research, not all that we had hoped for. This kind of transfer, wherein we loaned a multimillion dollar magnet in return for intangibles, provides a source of technical equipment to the Soviets.

Business Intermediaries

As a final area for consideration, business intermediaries--that is, US corporations that act as intermediaries for Bloc firms without the manufacturers being aware of such arrangements--are a major source of Soviet covert technology acquisition. The use of these companies provides an open conduit, lubricated by greed, for transferring immense quantities of materiel and technology to the Bloc.

The use of business intermediaries is an especially attractive device for the Soviets. Much of the strategic and dual-use high technology the Soviets obtained from the US is obtained through this particular approach. The best known--and certainly one of the most successful for the Soviet Union, and perhaps one of the most damaging to the US--was a business intermediary syndicate headed by a 34-year-old West German named Werner J. Bruchhausen.

The Bruchhausen scheme was based on his ownership of more than ten electronics firms in southern California and West Germany and his close ties to other firms elsewhere in western Europe. He would meet with Soviet and Soviet Bloc high-technology customers, they would discuss what specific high-technology components the Soviets needed, and Bruchhausen would then have his companies in California buy the desired goods. Then, by use of false shipping declarations, Bruchhausen's organization would ship the goods, illegally, out of the United States into Western Europe. From there, they were transshipped into the Soviet sphere.

In 1981, the west coast part of the Bruchhausen syndicate, after at least four years of very successful operations, was immobilized, and two of its principals brought to trial.

Of particular interest to me in the Bruchhausen case is the information it gives us about Soviet intentions. We delude ourselves if we think the Soviets enter the black market in search of strategic components in a helter-skelter style, buying up dual-use commodities without rhyme or reason.

The truth of the matter is that the Soviets and their surrogates buy nothing they don't have specific, well defined need for. They know exactly what they want--right down to the model number--and what they want is part of a carefully crafted design.

As an example of this kind of acquisition, among the strategic components that Bruchhausen directed his accomplices at the Continental Technology Corporation (CTC) in Southern California to buy for the Soviets were the following:

The above list of Soviet acquisitions includes many examples, but, by no means, is it exhaustive. The equipment detailed above was a fraction of the exports--part of the fraction used in preparing for litigation. From personal examination of the air-waybills, I believe that there were about six times as many illegal exports by CTC over a 3-year period.

Because my specialty is advanced computer systems, I can see an obvious pattern. Let's consider overall what the Soviets obtained and what use they can make of it.

The Soviets are having serious problems developing their integrated circuit/microcomputer industry. These problems are centered around the areas of process control and quality assurance. The result of such problems is a serious lack of reliable hardware for developmental systems. The above-mentioned items alleviate this lack by significantly contributing to the Soviet availability of hardware for developmental and production systems. In addition to miscellaneous, but important, hardware, the categorization of the larger hardware--test equipment, etc.--that is in the above list, is clear.

There is no question in my mind that the major pieces of hardware purchased from Continental Technology Corporation over the last four years of the corporation's operation, taken together, include at least one complete integrated circuit processing plant. This conclusion is ineluctable when you examine the totality of information available on the case. The Soviets

purchased everything they needed for such a plant, including: saws for cutting silicon crystals, equipment for making masks for integrated circuit production, plotters to draw the circuits, basic computer-aided-design systems for integrated circuit design, diffusion ovens for circuit production, ion-implantation systems for circuit production, photo-lithographic systems for integrated circuit production, scribers for separating integrated circuits on wafers, testers for testing integrated circuits on wafers, bonding equipment for bonding connecting leads to integrated circuits, and packaging equipment for packaging the circuits. As a result, they have purchased clandestinely all the hardware they need for equipping a good integrated circuit production plant. They showed minimal interest in purchasing production hardware that was not state of the art. In summary, they showed very good taste.

High-quality integrated circuits are the heart of modern military electronics. Integrated circuits form the basis for military systems which are more flexible, more capable, and more reliable than systems using discrete electronic components. The production tooling and equipment obtained by the Soviets from Continental Technology Corporation will significantly improve the Soviet's capability to produce such circuits.

The Soviets purchased everything they needed for their plant, among the many other things they bought. The sequence in which they purchased things and the quantities indicate the production plant would be of medium size and should be capable of delivering a high-quality product. There is a significant question in my mind as to whether or not they have enough trained people available to use this plant 24 hours per day, 7 days per week, but they do have the hardware.

Because of Werner Bruchhausen and his associates, the US gave up technology, much of which the Soviets could not have obtained elsewhere. It would have taken them considerably longer to equip the plant, if they could have equipped it at all, with indigenous capabilities.

What is lost is lost; we cannot get it back. But there is a positive side to the case: it is in what we can learn from it. There is a wealth of intelligence to be learned from the Bruchhausen case. It tells us much about Soviet shortcomings and Soviet strengths and their long-term strategic objectives.

Technological Development

In general, the development of a technology can be broken into several areas: theoretical research, applied research, development, and production. Let us examine these areas separately.

The Soviets have historically spent a large amount of their efforts supporting theoretical research. The Academy of Sciences in the Soviet Union is heavily populated with theoreticians. As a result, the Soviets have the theoretical basis for almost any technology they wish to exploit. In addition, the theoretical bases for technology in the West exist in the minds of the theoretical scientists who develop it. Much, if not most, of this technology is put in the open literature. Scientists would not be doing their jobs if they didn't like to advance the cause of human knowledge. There are many more lucrative ways to spend your life than doing theoretical research. You don't do it if you don't want to. The way to survive doing theoretical research is to publish. Scientists do.

Experimental research has very slightly less support in the Soviet Union than theoretical research but still, by Western standards, extraordinarily good support. Again, experimental research in the West is done by people who are advancing the cause of science and, for that and personal reasons, want to and do, publish thoroughly. The Western literature is available to the Soviets. Although their literature is carefully censored, much of it is available to us. In the theoretical and experimental research areas, to varying degrees, the two countries support each other.

In the area of development, the West has a tremendous lead. This lead is enhanced by the flexibility inherent in the Western political and economic system. Western countries are encouraged, by tax advantages and simple self-interest, to do research into appropriate areas in order to increase their profitability. In the Soviet system, on the other hand, the incentive for doing broad-ranging and possibly risky research is low. The penalty for failure is high. The penalty for failure in the US is economic and professional, at worst. (It isn't always even that, of course.) The ready availability of components and technology in the West encourages wide-ranging developmental efforts. There is a true pyramiding effect--we build on each other's work.

The Soviet system in preproduction can manage to produce a few of almost any product they want, provided they are willing to devote the resources to it. The best example of this would be the Soviet "civilian" space program, in which they managed to put people in orbit before the US did, but at a high cost.

In the area of serial production, i.e., the day-to-day production of large quantities of a product, the differences between the two systems become most obvious. The US is world renowned, and justifiably so, for the quality of its serial production facilities. Other parts of the world, notably Japan, are approaching the US quality and quantity in this area. The Soviet Bloc, however, is not.

Serial production is the Achilles' heel of the Soviet Bloc. Especially in high technology areas, the big problem the Soviets have is quality assurance. There may be aspects of the Soviet system which encourage poor quality in their production--or rather, provide no incentive for high quality in production. The Soviet system counts products, not quality products. The monopolistic, centralized control inherent in the Soviet system provides no incentive for the broad range of industrial workers to become better than adequate at their jobs. One of the things that characterizes high-technology fields is the need for superb manufacturing control. It is in this area that the Soviets exhibit weakness and need the most help. As a secondary part of this, they have serious problems manufacturing the tools to manufacture other high-technology equipment. This is what the Bruchhausen case helped alleviate by providing a full complement of high-quality working production equipment.

Available Manpower

One of the serious problems afflicting the Soviet economy is the lack of qualified, highly-trained, technical people in the areas of computers and microelectronics. One cause of this is the lack of enough computing and electronic equipment to train the next generation of scientists/engineers. They simply don't have enough equipment to allow students sufficient "hands-on" practice at an early stage in their education. The Soviets are trying to alleviate this problem by producing large, for them, numbers of RYAD computers--copies of the US IBM System 360's and 370's.

Many of the export license requests, both in the US and elsewhere, are for computer systems going to universities or scientific research institutes in the Soviet Bloc. It is difficult to turn such requests down on the basis of end-user since such organizations support the Soviet war machine only indirectly. Cases like the Bruchhausen organization are more obvious.

Unfortunately, we are not making the most of the kinds of information that result from episodes like the Bruchhausen case. When I brief various parts of the Executive Branch on Soviet Bloc Computing, I find a suprising lack of knowledge of the Bruchhausen case. Thus, one of the few examples of effective compliance action is not widely understood.

Analysis

It is necessary that the US Intelligence Community coordinate information derived abroad with data that surfaces here in the US. With expert analysis, we can discern Soviet objectives in the area of strategic commodities. When we know their objective, we can estimate what strategic and dual-use items they are going to be in the market for, overtly or covertly, and when we know what they are buying, we can make far better efforts to make sure that such equipment and technology is not available to them. We need to integrate the data and, from our conclusions, we can then predict with a satisfactory level of accuracy where the Soviets will be trying to tap into technology.

One cannot prevent the dissemination of data forever. One can only slow down a transfer and thereby make it more expensive for the adversary to acquire the data. Eventually, the adversaries get any information they want badly enough.

In the United States, the most advanced technology is often used in the civilian sector. Fielded US military equipment is often many years behind its civilian counterpart because of the need for greater reliability, delays in the acquisition process, or for other reasons. On the other hand, the Soviet military gets the best, most modern equipment as soon as it is available. Thus, delays in the transfer of high technology to the Soviet Bloc affects the military more seriously than it affects the "civilian" sector.

I would like to emphasize that there is no real "civilian" sector in the Soviet economy--it is all a State enterprise. If a plant produces civilian shoes, and the military needs shoes, the plant's output will be modified to fulfill the military's needs. We delude ourselves when we accept the Soviet assurances about the "civilian" characteristics of an enterprise.

The fact that, in the long run, the information will be transferred does not mean that we should not control it. Any obstacle we can place in the path of technology transfer increases the amount of resources the Soviet Bloc must devote to acquiring the information and decreases the total quantity of information they receive. Such increases in demand on resources, albeit increases on the seemingly inexhaustable resources of the Soviet intelligence apparatus, are a drain on the Soviet system.

The Soviet system has difficulty in flexibly responding to new information. As a result, the longer information is delayed, the harder it is for the Soviets to integrate it into their production cycle. Their planning goes on many years in advance, and the inclusion of new technology does not automatically cause a revision in the plan. It may cause an addition to the plan, but not necessarily a reduction in other, less productive, areas. The highly structured environment in the Soviet Union often has a self-defeating result: factories or enterprises will produce obsolete equipment because they were ordered to although they have the ability to produce more modern equipment and know about the demand for that equipment but have no authority to produce it.

When we know better what the Soviets are attempting to acquire, we can more effectively prevent them from succeeding. That situation is reversed now. Many of our control efforts seem to be based on the assumption that we can control everything. We cannot. A more thoughtful enforcement approach is to decide which items are most important to the Soviets and focus our attention and resources on those items.

Let us return to the Bruchhausen case for a moment. A key ingredient in the Soviet acquired integrated-circuit manufacturing plant is a high-pressure oxidation system. One model of this kind of system is called by the trademarked name "Hipox." No modern integrated circuit production plant can operate without an accurate, effective, oxidation system. The Hipox system is an example of the state of the art in this area. It is basically a complex oven that precisely controls the atmosphere and temperatures involved in the conversion of a wafer of crystalline silicon into a wafer containing several hundred integrated circuits. Highly sophisticated integrated circuits cannot be produced without this kind of technology.

Most high-technology components wear out over time. In fact, engineers commonly refer to this cycle by use of the term "half-life." The half-life is the time after which half the systems in the field will require spare parts and/or extensive maintenance. In general, the higher the technology involved in the system, the shorter the half-life and therefore the greater the demand for spare parts.

The Hipox systems, so essential to the new Soviet integerated circuit factory, should begin to require spare parts within a few months after they are installed. Such an integrated circuit plant is useless without working high-pressure oxidation systems and the Hipox system does not work accurately, if at all, if more than a very few of its components need repair. Such an integrated circuit plant would be an integral part of the Soviets' economic system for years into the future. and if the Hipox and other critical systems cannot be serviced, that factory will slow down or be otherwise negatively affected.

That tells us that the Soviets will soon be in the market for spare parts for the Hipox systems, among others. Only a very few companies in the world manufacture high-pressure oxidation systems. They are all in the West and include, for example, Gasonics Corporation of Mountain View, California. If our nation's investigative and enforcement apparatus were working as effectively as it might, each of these companies could be put on notice to be on the alert for false documentation and other signs of a Werner Bruchhausen-type business intermediary activity.

I do not mean to imply by my earlier remarks that many, or even more than a few, of the US industrial manufacturers are venal or unpatriotic enough to close their eyes to this kind of technology theft. However, they are very busy; given prima-facie evidence of respectability, they do not often investigate further. I have every reason to believe that, given a proper warning, the companies would report suspicious inquiries promptly and effectively. In addition, suppliers to these companies can be alerted to potential unusual requests.

This kind of precision targeting for export control requires the availability of accurate technical evaluations of the components and systems involved in an export or diversion. The expertise needed for these evaluations is a scarce commodity. It is for this reason that the Department of Commerce continually calls upon technical experts from other agencies to review complex export cases.

The Assistant Secretary for Defense Programs, Department of Energy, provides technical expertise and policy guidance to other regulatory agencies with regard to export control matters; this service was also provided by the DOE's predecessor agencies. For example, I am the chairman of the Technical Task Group that is responsible for rewriting the US proposals to the Coordinating Committee (COCOM) for international control of exports of computers. Other National Laboratory experts chair other committees. My group is devoted to computers and directly related items. Also, Department of Commerce licensing officers call Laboratory experts, on a regular basis, to request technical advice on complex export cases.

In other forums, I have proposed the establishment of a Center of Expertise to provide a source of technical information for the various government agencies involved in technology transfer/export control activities. This will go far to help alleviate the scarcity of available technical expertise.

95-929 O - 82 - 23

In any decision to allow or to prohibit the export of a piece of equipment, or a technology, three factors come into play.

First are the procedural considerations: Are the forms filled out correctly? Are proper concurrences received? Are the overall characteristics of the equipment within appropriate limits, etc.?

Second is the technical evaluation of the item to be exported. Is the system truly appropriate for the stated end-use? Are the statements about the end-use/end-user true?

As I have previously stated, the technical evaluation of an export case is a very complex task requiring a particular expertise. The technical evaluation is best made by an individual who is technically competent in the field and who understands the state of the art in the West and in the Soviet Bloc. Such individuals are rare.

The third factor in implementing export controls is policy. The policy sets the rules: what we are allowed to export, what we are not allowed to export.

The key consideration among the three factors--procedure, technical, and policy--is the technical evaluation. In fact, policy is usually the result of technical evaluation. For example, a policy that includes a prohibition against the export of certain oscilloscopes is based on the technical evaluation of what national security uses the adversary could make of oscilloscopes. The US is frequently criticized for having a poorly articulated policy on export controls or, at best, an uncertain policy.

That point may not be as clear as I would like to make it. Let me try to say it another way. I cannot overstress the importance of having an effective system of technical evaluation. To achieve the goal of such an effective evaluation, we must optimize three functions.

First, we must be able to look closely at a commodity and be able to assess its capabilities in both the commercial and the military sectors. Obviously, the knowledge of its military uses is critical. That question can be answered only by competent technical evaluation--implying an evaluation done by a technically competent analyst.

Second, we must decide whether or not the stated end-user is who the purchase documents and export documents purport him to be. For example, is the end-user really a tractor factory, or is it a tank factory? That question can be answered only with competent intelligence data. The analysis of such intelligence data requires intelligence expertise as well as technical expertise.

Third, we must assess the adversary's capability to use the commodity in a manner that cound harm us. That question can be answered only with detailed technical knowledge and competent intelligence data about the adversary's system.

I would like to conclude my prepared testimony with the recommendation that, in evaluating export controls, the Committee take into account the very important distinction between strategic and dual-use equipment versus strategic and dual-use know-how. Even if our investigative and enforcement capabilities were near-perfect, they would still be directed primarily against equipment. In both the law, and in the Federal regulations, controls should be strengthened with reference to the know-how that accompanies a product.

If the Soviets clandestinely acquire a piece of equipment, and the equipment works, they have acquired a capability that presumably they did not have before. Along with that equipment, especially if it is high-technology equipment, they need the technical data that goes with it. They need the technical manuals that support the product; they need the technical art that enhances the equipment. In many ways, it may be difficult to control the shipment of technical manuals that accompany manufactured equipment. However, I believe that we can control the art and the support that goes with legally acquired equipment. Showing the Soviets how to make the rope with which to hang us does not strike me as a reasonable approach for the US to take.

I thank you very much for the opportunity to testify, and I hope that my testimony has been useful to you.

RÉSUMÉ OF DR. LARA H. BAKER, JR.

He received a Bachelor of Science in Civil Engineering, Master of Science in Civil Engineering, and Doctor of Science Degree in Environmental Engineering, all from New Mexico State University, the last degree being granted in 1970. He is a Registered Professional Engineer in the State of New Mexico. Since 1968 he has been employed by the Los Alamos National Laboratory in the Engineering Department and in the International Technology Office. Since 1975 he has been involved half-time or more in the area of Critical Technologies and Technology Transfer. Since 1972 he has been involved in the detailed study of Soviet Computing Capabilities, and the study of Soviet Bloc Computing Capabilities. He is a member of the Computer Systems Technical Advisory Committee, a statutory committee which reports to the Department of Commerce and to the United States Congress on matters involving the export control of digital computers and digital computer components. He is the DOE representative on technology tasks groups which define the US position on the export control of computers and which define and evaluate the rationale for the US position.

Since 1975 he has been actively involved in export case determinations, both for the Department of Energy and the Department of Commerce, and in evaluating the technical risks and merits of various export proposals. These cases, at the rate of 200 to 400 per year, involve everything from integrated circuits through spare parts and components, through complete computer systems, through supercomputer systems.

He has been an Adjunct Professor of Electrical and Computer Engineering at the University of New Mexico since 1969. He teaches Graduate Computer Science, Computer Architecture, Computer Programming, and Computer Graphics. He has presented invited papers at the National Computer Conference and other national conferences. He is a member of the Association for Computing Machinery, of the Computer Society of the Institute for Electric and Electronic Engineers, and various other professional and honorary organizations. He has presented briefings on Soviet Bloc Computing to staffs and members of Congress, throughout the Executive Branch of the US Government, and to non-government agencies.

Responses of Lara H. Baker, Jr., to the Custom Bureau, Regarding the Continental Technology Corporation Case

CTC Invoice Number: 21 021

Manufacturer: INTEL Corporation

The commodity on this invoice is the INTEL System 80/20-4, a single board microcomputer. Single board computers/microcomputers have many commercial applications, principally in original equipment manufacturer (OEM) applications where they are used as the controlling part of other equipment such as a sophisticated sewing machine, a sophisticated machine tool, or a sophisticated piece of automatic test equipment. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 037

Manufacturer: INTEL Corporation

The commodity on this invoice is a Programmable Read Only Memory (PROM) expansion board for single board computers. The board provides 16K (K = 1024) bytes of programmable, non-erasable, memory for a microprocessor system. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products would match the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: Unknown

Manufacturer: INTEL Corporation

The commodity on this invoice is an optical isolator board, i.e. a printed circuit board containing circuitry to isolate the input from the output electrically. This kind of circuitry is normally used in a very high noise environment, such as a real time military system or a civilian system involved with aircraft or other transporation equipment.

This board is used with single board computer microprocessor systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 010

Manufacturer: Unknown

The commodities on this invoice are involved with single board computers. They are the central processor with 4K (K = 1024) bytes of read/write memory, analog input/output, that is boards for connecting to non-digital environments, and a Direct Memory Access (DMA) controller. These commodities are used as parts of single board computer systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1194

Manufacturer: INTEL Corporation

The commodity on this invoice is an analog input/output board which is used to connect single board computers to the outside world. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 004

Manufacturer: INTEL Corporation

The commodities on this invoice are a single board computer with analog input/output to connect to the outside world and with Direct Memory Access (DMA) for high speed memory access. These particular commodities taken together provide the basis for a workable control system for a relatively small piece of equipment such as a gun firing system or a radar. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 033

Manufacturer: INTEL Corporation

The commodity on this invoice is a universal prototype board which is used in the design and development of applications for microcomputer systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 016

Manufacturer: INTEL Corporation

The commodity on this invoice is a high speed arithmetic board used with single board computers. It has particular application in military and civilian signal processing applications. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 064

Manufacturer: INTEL Corporation

The commodity on this invoice is a relatively small single board computer with 1K (K = 1024) Bytes of random access memory (RAM) and 8K Bytes of programmable read only memory (PROM). Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 066

Manufacturer: INTEL Corporation

The commodity on this invoice is a 64K (K = 1024) byte random access memory (RAM) with a speed of 700 nanoseconds (ns) per access. This board would be used in the design, development, and use of microcomputer systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 065

Manufacturer: INTEL Corporation

The commodities on this invoice are equipment for use in developing microcomputer systems. They include an interface and execution modeling package as well as a universal PROM (programmable read only memory) programmer. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 011

Manufacturer: INTEL Corporation

The commodities on this invoice are peripherals and equipment used with microcomputer development systems. They would be embargoed because of their direct applicability to microcomputer development systems, an embargoed function. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 043

Manufacturer: INTEL Corporation

The commodities on this invoice are peripherals and equipment to be used in developing microcomputer systems. They include an in-circuit emulator, universal PROM (programmable read only memory) programmers, and a chassis for mounting the above equipment. Single board computer/microcomputer systems are used in most advanced weapon systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 006

Manufacturer: INTEL Corporation

The commodities on this invoice are used in microcomputer design and development. One of the commodities is a very high speed (60 nanosecond) 4K (K = 1024) bit Programmable Read Only Memory (PROM). One is a programmable interface for a microprocessor development system, the others are accessories for this effort. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 009

Manufacturer: INTEL Corporation

The commodities on this invoice are peripheral integrated circuits for use with microprocessor/microcomputers. These circuits are particularly useful for increasing the utility of microprocessors of the 8080 Family. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21-017

Manufacturer: INTEL Corporation

The commodities on this invoice are microprocessors and other circuits. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 002

Manufacturer: INTEL Corporation

The commodities on this invoice are peripheral integrated circuits for use with 8080 microprocessor systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 007

Manufacturer: Motorola Incorporated

The commodity on this invoice is a very high speed (15 nanosecond cycle) 64 bit capacity random access memory (RAM). This speed of RAM would normally be used in the central processor of a general purpose computer for civilian applications, or in military hardware that probably incorporates a microcomputer and is used particularly for signal processing. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: Unknown

Manufacturer: INTEL Corporation

The commodity on this invoice is a 2K (K = 1024) bit erasable programmable read only memory (EPROM) which is rated for military temperature ranges (minus 65°C to plus 125°C) and is packaged in a metal can. The components with this kind of temperature range and packaging have essentially no civilian applications; their military applications tend to be aerospace uses. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 005

Manufacturer: Motorola Incorporated

The commodities on this invoice are extremely high speed memory devices used in the design and development of military microcomputer controlled equipment. The random access memories (RAM's) are 256 bits in capacity and 15-26 nanosecond speeds. The quantities involved in this shipment imply use in a production system, rather than in a development system. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 8019

Manufacturer: INTEL Corporation

The commodity on this invoice is a 2048 bit, one microsecond cycle, erasable programmable read only memory (EPROM). This equipment is designed for use in developing microcomputer systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would match the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also match the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 051

Manufacturer: INTEL Corporation

The commodities on this invoice are integrated circuits of differing compositions. The HM-1-7460-5 is a 4096 bit, 60 nanosecond cycle programmable read only memory (PROM). This circuit is extremely fast and is designed for production versions of microcomputer systems. Civilian use of a circuit of this speed would be unusual, except in systems with extraordinary speed constraints. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 087

Manufacturer: Motorola Incorporated

The commodity on this invoice is an extremely high speed random access memory (RAM). The devices have a capacity of 64 bits and a speed of 15 nanoseconds. The quantity, 5,000, implies their use in a production system, rather than in a development system. Such devices are normally used as registers in general purpose computers and in military systems as part of signal processing hardware. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 8007

Manufacturer: INTEL Corporation

The commodity on this invoice is a 2048 bit erasable programmable read only memory (EPROM). At a cycle time of 650 nanoseconds, this EPROM is normally used in microprocessor development systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products match the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1196

Manufacturer: Motorola Incorporated

The commodity on this invoice, a 64 bit capacity, 15 nanoseconds cycle, random access memory (RAM), is normally used as high speed registers in the central processor of a general purpose computer or for high speed data storage in military signal processing computers. The extremely high speed of this RAM implies equipment of significant processing capability. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 031

Manufacturer: INTEL Corporation

The commodities on this invoice are integrated circuits used in the design and development of microcomputer systems. Both pieces of hardware are extremely fast, one being a 4096 bit programmable read only memory (PROM), with a cycle of 70 nanoseconds, the other a 4096 bit random access memory (RAM) with a cycle of 250 nanoseconds. Both these devices are used in microcomputer systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 015

Manufacturer: INTEL Corporation

The commodities on this invoice are microprocessors and integrated circuits associated with microprocessor development systems. Some of the integrated circuits are particularly fast, 70 nanoseconds, 4096 bit programmable read only memories (PROM's), most of the rest are peripheral circuits designed to support microprocessor systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21-013

Manufacturer: INTEL Corporation

The commodities on this invoice are integrated circuits of varying capacities. One of the circuits is a military-temperature-range-approved integrated circuit in a ceramic package, a circuit particulary designed for immediate use in military systems. Another circuit is an extremely fast (70 nanosecond) 4096 bit programmable read only memory (PROM) which is used in microcomputer systems and microcomputer systems developments. The other integrated circuits are faster than would normally be approved for export. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 115[illegible]

Manufacturer: Various, including INTEL Corporation

The commodities on this invoice are integrated circuits and other components, principally high speed, low powered, devices used in microprocessor/microcomputer systems, but also used in several other kinds of electronic hardware. The variety of the equipment in this list suggests it is a list of spare parts for other equipment. Most of the integrated circuits on the list are not approvable for export.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. Some of the products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 032

Manufacturer: Rockwell International

The commodity on this invoice is used in the design and development of bubble memory systems. These memory systems are used in microcomputers as mass storage and in aircraft, and spacecraft as replacements for tape recorders.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also match the state of the art of new designs in the destination country, as of the time of shipment.

The technical data shipped with these bubble memory boards is not approvable for shipment under the technical data regulations.

CTC Invoice Number: 1146

Manufacturer: Unknown

The commodity on this invoice is used in the manufacture of computer discs and would be embargoed for that reason. The equipment is within the state of the art of the equipment being manufactured in the destination country, as of the time of shipment. It has no direct civilian or military application outside of the manufacture of computer equipment.

CTC Invoice Number: Unknown

Manufacturer: Unknown

This equipment appears to be spare parts and tooling for use in manufacturing computer disc drives and, as such, is embargoed. The equipment is within the state of the art of equipment being manufactured in the destination country, as of the time of shipment.

CTC Invoice Number: 1137

Manufacturer: Unknown

The commodity on this invoice is used in the manufacture of magnetic discs for use on computer systems, and as such, it is embargoed under CCL 1355. This equipment matches the state of the art of equipment being manufactured in the destination country, as of the time of shipment.

The equipment has no direct military or civilian application except in the manufacture of computer discs.

CTC Invoice Number: 7039

Manufacturer: Various, including Hewlett Packard

The commodities on this invoice are equipment used in the manufacture and test of integrated circuits. As such, it is embargoed under CCL 1355. They are applicable to microcomputer systems. This type of equipment is often a bottleneck on a production line for integrated circuits. The lack of fast and accurate test equipment can virtually shut down a production facility. Often, the throughput of the test equipment is the controlling factor in the productivity of a plant. The test equipment can test integrated circuits for military use equally as well as it can test circuits for civilian use.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 22 005

Manufacturer: Unknown

The commodity on this invoice is used in checking the integrity of coaxial cables. Coaxial cables have extensive use in radar and in signal processing systems for the military. The need for ensuring the integrity of these systems is very high. As a result, these commodities have direct military application. They exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment.

CTC Invoice Number: 8015

Manufacturer: Gasonics Corporation

The commodities on this invoice are a high pressure oxidation system used in the manufacture of integrated circuits. This is the standard method of high speed, high quality integrated circuit production in the United States. Integrated circuits are used in virtually all modern civilian and military high technology systems. The technology to produce integrated circuits is embargoed because of the inability to differentiate between equipment that produces civilian integrated circuits and equipment that produces military integrated circuits, principally because there is no difference in the equipment.

The products on this invoice far exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment.

CTC Invoice Number: 8014

Manufacturer: Gasonics Corporation

The commodities on this invoice are a high pressure oxidation system used in the manufacture of integrated circuits. This is the standard method of high speed, high quality integrated circuit production in the United States. Integrated circuits are used in virtually all modern civilian and military high technology systems. The technology to produce integrated circuits is embargoed because of the inability to differentiate between equipment that produces civilian integrated circuits and equipment that produces military integrated circuits, principally because there is no difference in the equipment.

The products on this invoice far exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment.

CTC Invoice Number: 8021

Manufacturer: Gasonics Corporation

The commodity on this invoice is the technical data for the Hipox oxidation ovens referred to in the previous two entries. This technical data is embargoed by technical data regulations and far exceeds the data available on production or design systems in the destination country, as of the time of shipment.

CTC Invoice Number: 2049

Manufacturer: Rockwell International

The commodities on this invoice are bubble memory chips and bubble memory controller chips. These integrated circuits are used in equipment as mass memory for microcomputers and as replacements for tape recorders in military and space related systems. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 044

Manufacturer: INTEL Corporation

The commodities on this invoice are microcomputer development systems. They are used to develop microprocessor/microcomputer systems for civilian and military applications. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 035

Manufacturer: INTEL Corporation

The commodities on this invoice are microprocessor development systems. They are used to develop microcomputer/microprocessor systems for civilian and military applications. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 012

Manufacturer: INTEL Corporation

The commodities on this invoice are microcomputer development systems. They are used to develop microcomputer/microprocessor systems for civilian and military applications. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 024

Manufacturer: INTEL Corporation

The commodities on this invoice are microcomputer development systems. These are used for the development of microprocessor/microcomputer systems for civilian and military applications. Single board computer/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1155

Manufacturer: INTEL Corporation

The commodities on this invoice are microcomputer development systems. These are used for the development of microprocessor/microcomputer systems for civilian and military applications. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 8051

Manufacturer: Fairchild Instrument Corporation

The commodity on this invoice is a test system for the production testing of integrated circuits. This test system is necessary and critical for the test of civilian or military microcircuits. This is an area in which the destination country falls far behind the United States in capability, and the test system is applicable to integrated circuits for military applications. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1014

Manufacturer: Fairchild Instrument Corporation

The commodities on this invoice are spare parts and extensions for the Fairchild Xincom test systems referred to on CTC Invoice number 8051, among others. As such they continue and enhance the capabilities of the microprocessor test system previously referred to.

The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1016

Manufacturer: Fairchild Instrument Corporation

The commodities on this invoice are spare parts and extensions for the Fairchild Xincom test systems referred to on CTC Invoice number 8051, among others. As such they continue and enhance the capabilities of the microprocessor test system previously referred to.

The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1017

Manufacturer: Fairchild Instrument Corporation

The commodities on this invoice are spare parts and extentions for the Fairchild Xincom test systems referred to on CTC Invoice number 8051, among others. As such they continue and enhance the capabilities of the microprocessor test system previously referred to.

The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 8071

Manufacturer: Fairchild Instrument Corporation

The commodity on this invoice is a test system for the production testing of integrated circuits. This test system is necessary and critical for the test of civilian or military microcircuits. This is an area in which the destination country falls far behind the United States in capability, and the test system is applicable to integrated circuits for military applications. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1091

Manufacturer: Fairchild Instrument Company

The commodity on this invoice is a test system for the production testing of integrated circuits. This test system is necessary and critical for the test of civilian or military microcircuits. This is an area in which the destination country falls far behind the United States in capability and the test system is applicable to integrated circuits for military applications. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1040

Manufacturer: Fairchild Instrument Corporation

The commodity on this invoice is a test system for the production testing of integrated circuits. This test system is necessary and critical for the test of civilian or military microcircuits. This is an area in which the destination country falls far behind the United States in capability, and the test system is applicable to integrated circuits for military applications. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 073

Manufacturer: California Computer Products Incorporated

The commodity on this invoice is a complete off-line high-precision flat bed plotter system. The plotter involved, the CALCOMP-748 plotter, is precise enough and big enough to directly draw the masks needed for integrated circuit production. For that reason the plotter associated equipment is embargoed. The integrated circuits produced with masks drawn on this plotter can be used for civilian or military applications and as such are embargoed.

The products exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 074

Manufacturer: California Computer Products Incorporated

The commodities on this invoice are accessories for the high precision plotter referred to on CTC Invoice number 21 073. As such they are embargoed for that application. These particular pieces of equipment are within the state of the art of the country of destination, however, they could not be shipped as part of the plotter system.

CTC Invoice Number: 21 075

Manufacturer. California Computer Products Incorporated

The commodities on this invoice are spare parts for the plotter referred to on CTC Invoice number 21 073. As such they would be embargoed because of the direct military application of the plotter. The parts themselves may be embargoed because they contain embargoed technology. These products would exceed the state of the art of equipment being manufactured in the destination country as of the time of shipment.

CTC Invoice Number: 22 004

Manufacturer: Tektronics Incorporated

The commodity on this invoice is an extremely high speed (350 megahertz) oscilloscope with direct military applications in nuclear weapons testing, in high speed signal processing systems, and in other high speed electronic applications. This product exceeds the state of the art of equipment being manufactured in the destination country as of the time of the shipment.

The product matches the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1188

Manufacturer: Tektronics Incorporated

The commodities on this invoice are accessories for the high speed oscilloscope referred to on CTC Invoice 22 004. As such they are embargoed. These products exceed the state of the art of equipment being manufactured in the destination country as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1003

Manufacturer: Data General Corporation

The commodity on this invoice is a complete Data General Eclipse S/230 digital computer with substantial peripheral and input/output communication equipment. This general purpose computer could be licensed if a license were applied for and certain characteristics of the computer were deleted. As a general purpose computer it is applicable to many civilian and military applications. This particular configuration seems applicable to the control and monitoring of the manufacture of integrated circuits.

The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21089

Manufacturer: Data General Corporation

The commodities on this invoice are accessories and spare parts for the Eclipse S/230 computer referred to on CTC Invoice Number 1003. They would be embargoed as spare parts for an embargoed computer. These products are within the state of the art of equipment being manufactured in the destination country as of the time of shipment.

CTC Invoice Number: 1131

Manufacturer: Data General Corporation

The commodity on this invoice is a complete Data General Eclipse S/230 computer with a very large amount of accessory hardware and software. This is a medium size general purpose computer that is applicable to large numbers of civilian and military general purpose applications. This size machine, with the standard characteristics of the Eclipse S/230, would not be approvable for export. It contains characteristics such as a writeable control store, which are not within the allowable limits because of the direct military application of redesigning the system. This product exceeds the state of the art of equipment being manufactured in the destination country, as of the time of shipment.

CTC Invoice Number: 1186

Manufacturer: Unknown

The commodity on this invoice is a time delay reflectometer (TDR) cable tester. As such it is used for testing the integrity and utility of coaxial cables. Coaxial cables are intergral parts of military systems such as radars and military avionics systems. These cables are also used in civilian applications involving high frequency electronics.

This product would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The product also exceeds the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 1201

Manufacturer: Rockwell International

The commodities on this invoice are bubble memory and bubble memory controller circuits. Bubble memories are used as replacements for tape recorders on military aircraft and satellites. Bubble memories are also used as bulk memory for microprocessors/microcomputer systems. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 029

Manufacturer: Rockwell International

The commodities on this invoice are bubble memory and bubble memory controller circuits. Bubble memories are used as replacements for tape recorders on military aircraft and satellites. Bubble memories are also used as bulk memory for microprocessors/microcomputer systems. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

These products would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 21 086

Manufacturer: Rockwell International

The commodity on this invoice is bubble memory chip. Bubble memories are used as replacements for tape recorders on military aircraft and satellites. Bubble memories are also used as bulk memory for microprocessors/microcomputer systems. Single board computers/microcomputer systems are used in most advanced weapons systems throughout the free world, particularly in missile and aircraft systems. Their use provides a significant increase in effectiveness with an equally significant reduction in weight and power consumption.

This product would exceed the state of the art of equipment being manufactured in the destination country, as of the time of shipment. This product also exceeds the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 2059

Manufacturer: Memorex Corporation

The commodities on this invoice are very high speed, high capacity disc storage modules and controllers. These controllers are used as auxiliary storage on general purpose computers. Because their speed and capability make them applicable to nuclear weapons design, and to other large hydrodynamics calculations, such equipment is not available for export. These products far exceed the state of the art of equipment being manufactured in the destination country as of the time of shipment.

The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

CTC Invoice Number: 4004

Manufacturer: Tamarack Scientific Corporation

The commodity on this invoice is a contact printer used for reproducing the masks used in integrated circuit manufacturing. It includes ultraviolet lighting systems, which are at the state of the art of United States production equipment. This product is used directly in the manufacture of integrated circuits for civilian and military applications. It is not exportable because of the direct military utility of the equipment produced by the product. These products far exceed the state of the art of equipment being manufactured in the destination country as of the time of shipment.

The products also exceed the state of the art of new designs in the destination country, as of the time of shipment.

STAFF STATEMENT OF
FRED ASSELIN, INVESTIGATOR
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE

MAY 5, 1982

Mr. Chairman, I am Fred Asselin. I am an investigator on the Minority staff of the Senate Permanent Subcommittee on Investigations. Since 1969, I have been associated with the Subcommittee either on a full time basis as a Staff Investigator, or on loan from the personal staff of former Senator Ribicoff.

Under the Export Administration Act, the U. S. Department of Commerce, through its Office of Export Administration, has jurisdiction over most non-classified exports from the United States, its territories and possessions.

The Export Administration Act was passed in 1949 and has been renewed several times since then, the most recent instance being passage of the Export Administration Act of 1979. The Act will expire on September 30, 1983.

Mr. Chairman, I request that the Export Administration Act of 1979 be received as an exhibit to these hearings and that it be printed as an appendix to the hearing volume.

Enforcement of the Export Administration Act is carried out by the Compliance Division of the Office of Export Administration.

The Compliance Division has three Branches -- Investigations, Intelligence and Facilitation (Inspections).

The Minority staff of the Subcommittee has made an evaluation of the effectiveness of the Compliance Division. An assessment of Compliance Division resources and procedures was made. The Minority staff interviewed current and former executives of the Division, and current and former Special Agents of the Division. Also interviewed were law enforcement personnel from other agencies, government intelligence officials and officials of agencies whose mission brings them in contact with the Compliance Division.

Uppermost in our minds as we made this evaluation were the national security implications of the responsibility vested in the Compliance Division. The Export Administration Act itself spells out that national security responsibility when it says that export controls shall be used--

> . . . to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States . . .

The national security implications of the enforcement mechanism are stated at another point in the statute when it is asserted that:

> Exports of goods or technology without regard to whether they make a significant contribution to the military potential of individual countries or combinations of countries may adversely affect the national security of the United States.

In addition to measuring the effectiveness of the Compliance Division in terms of its role as an organization pledged to protect the national security, the Minority staff evaluated the Compliance Division in terms of its being a law enforcement entity.

It is apparent that the Commerce Department views the Compliance Division as a law enforcement organization. Its professional personnel, who carry the title of Special Agent, are classified as Series 1811 federal criminal investigators. The 1811 series of federal criminal investigator is the classification that Customs Service and drug enforcement agents and many other federal criminal investigators are under.

The information that the Minority staff has gathered about the Compliance Division was compared to official pronouncements which the Department of Commerce has made about the Division -- in testimony before Congress and in annual reports to Congress. In this regard, sources included, but were not limited to, 1) the testimony of William V. Skidmore, Director of the Office of Export Administration, before the Subcommittee on International Economic Policy and Trade of the House Committee on Foreign Affairs, on March 26, 1982; 2) the Export Administration Annual Report for Fiscal Year 1980, submitted to the Speaker of the House and the President of the Senate in February of 1981; and 3) the Export Administration Annual Report for Fiscal Year 1981 submitted to the House and Senate in February of 1982.

Mr. Chairman, I request that these three documents be received as exhibits to these hearings.

The investigation, which lasted more than one year, resulted in a series of preliminary findings, which are now submitted to Subcommittee Members for their consideration. It is our recommendation that subsequent witnesses to these hearings from the law enforcement and national security fields be asked to comment on the Minority staff's preliminary findings.

1. Past Departmental Statements To Congress

In the staff inquiry we found that the Commerce Department has overstated the effectiveness of the Compliance Division to the Congress. Whether through deliberate action or through inadvertence, the Commerce Department has portrayed the Compliance Division as if the Division were competently organized and adequately staffed to enforce the Export Administration Act export controls provisions. By contrast, our investigation found that the Compliance Division is not effective. It is an understaffed and poorly equipped and, in certain instances, undertrained and unqualified investigative and intelligence unit.

In his testimony before the House Subcommittee, Skidmore said that Commerce Department officials "regard the enforcement program as an integral part of the export control system," and that his Department's policy was to "marshal our limited resources to exact maximum compliance with the law."

It is useful to note Mr. Skidmore's reference to "limited resources" because the staff also will underscore the limited nature of the Commerce Department's commitment to enforcing export controls. Moreover, the staff inquiry concluded that the Department's commitment to export controls enforcement is so limited, in fact, that it is impossible to expect "maximum compliance with the law." It is optimistic to expect very much compliance at all.

In his testimony, Mr. Skidmore described the Facilitation or Inspection Branch of the Compliance Division as being "staffed by inspectors, export control specialists and document examiners." Then he added:

> Inspectors examine cargo about to be exported from the United States. If a suspected violation is identified, the shipment is detained until our export control specialists can make a determination about the legality of the export. If there is no violation, the goods are released. Generally, those shipments found to be in violation of the law are seized by the U. S. Customs Service at our request. This Branch also reviews Shipper's Export Declarations forwarded to the Compliance Division from the Bureau of the Census. All illegal exports detected by the Facilitation Branch are referred to the Intelligence Branch for evaluation to determine whether further investigation is necessary.

Our staff investigation revealed the number of inspectors for the entire nation is five or six — and five of them are located at the John F. Kennedy International Airport in New York. On a rotating basis, one of the five inspectors is on travel much of the time, trying to conduct inspections for the rest of the nation. Some airports and seaports never are visited by Commerce Department inspectors in the course of a year. Other exit ports are visited one week a year. A sixth inspector is in the Washington, D. C. area.

The Compliance Division's five inspectors are grades 5, 7 and 9.

In fiscal year 1980, according to the Export Administration's annual report to Congress, the Compliance Division reviewed 190,484 Shipper's Export Declarations, or SEDs. The next year, according to the FY 81 report to Congress, the number of SEDs reviewed increased to 230,154. These figures need to be seen in perspective. The Department could have pointed out that about 9 million SEDs are filed a year. That means that, while Commerce Department inspectors reviewed 230,154 SEDs in the reporting period, they did not review about 8.7 million more.

Nor is it apparent the manner in which the SEDs were reviewed. Mr. Skidmore testified about the SEDs being forwarded to the Compliance Division from the Census Bureau. SEDs that arrive at Commerce through that route are at least one month old; it takes that long for Census tabulators to key the data from the SEDs into computers. With information from the SEDs being at least a month old, it is likely that most shipments already have departed and been taken custody of by the ultimate consignee overseas.

Conversely, the Chief of the Inspection Branch told the Subcommittee staff that SEDs are reviewed by his inspectors at the airports and ports. His explanation is more in keeping with this language from the FY '81 annual report to the Congress:

> . . . the Compliance Division reviewed 230,154 Shipper's Export Declarations and identified 10,649 apparent discrepancies requiring further inquiry or inspection; 10,365 of these resulted in the physical examination of export cargo.

If the SEDs are reviewed after they are referred to Commerce from the Census Bureau, it is very unlikely that any of the reviews could have resulted in physical examination of cargo. By the time the SEDs arrive at Commerce, most of the shipments will have reached their destinations. The report to Congress leads the reader to understand that the review of the SEDs led directly to the discovery of discrepancies and that discovery led to the physical examination of the cargo.

Mr. Skidmore's description of the Intelligence Branch of the Compliance Division was as follows in his House testimony:

> The Intelligence Branch is staffed with criminal investigators, intelligence reporting officers and other support personnel who develop and maintain intelligence information regarding possible export control violations. Branch personnel review all incoming allegations, voluntary disclosures and referrals from the Facilitation Branch to determine whether referral to the Investigations Branch is warranted.

The testimony suggests a much larger operation than actually exists. The Intelligence Branch has a Branch Chief, a Deputy Branch Chief, two fulltime professionals and one detailee from the Drug Enforcement Administration.

The Intelligence Branch Chief, who is unique among the three Branch chiefs because of his considerable background in law enforcement, told the staff in a pre-hearing interview that his office is so overwhelmed with its workload and so understaffed that it is impossible for him to provide the kind of intelligence analysis needed for the Division's national security - law enforcement - mission.

The Intelligence Branch is supposed to be able to process and assess sensitive information. Yet the Branch has no secured telephone. None of its professionals has a clearance higher than top secret.

Intelligence Branch personnel often are bogged down in relatively insignificant assignments and do not have the time to collate and synthesize information in an effort to anticipate violations. For example, the Bruchhausen case, one of the most important technology diversion investigations ever conducted — and one which will be discussed in detail later in this statement — was investigated for the first time in an active manner by the Commerce Department in 1980. But the existence of the network of companies in the U. S. and Western Europe was brought to the attention of the intelligence Branch two years before in the form of two anonymous letters. The Intelligence Branch did not see to it that the serious allegations in the anonymous letters were checked out.

In his testimony before the House Committee, Mr. Skidmore went on to describe the Investigations Branch of the Compliance Division. He said that it—

> . . . is also staffed with criminal investigators and conducts full-scale investigations into alleged violations. If it determines that a violation has occurred, but does not find the elements of a criminal offense, either a charging letter is recommended or a warning letter is issued to the alleged violator, depending on the circumstances. If we believe the elements of a criminal offense are present, and our Office of General Counsel concurs, we refer the case to the Department of Justice for prosecution. (emphasis added)

Mr. Skidmore's use of the adjective full-scale to describe investigations suggests a substantive effort. However, the Subcommittee staff was informed by the Chief of the Investigations Branch and by a former Director of the Compliance Division that a full-scale investigation can be a phone call or a letter. In its use of the term full-scale with reference to investigations in the two reports to Congress and Mr. Skidmore's testimony before the House Committee, no definition was given to further explain more precisely what is meant by full-scale.

Carrying the concept of full-scale investigation a step further, both the FY '80 and FY '81 reports to Congress speak of "full field investigations." In 1980, Compliance Division Special Agents conducted 61 full field investigations; and in 1981, an undisclosed number of full field inquiries were made, according to the two reports to Congress. The Branch has about eight investigators. With such limited resources at its disposal, the Compliance Division would be very hard pressed to conduct 61 full field investigations in a 12-month period. The Chief of the Investigations Branch told the Subcommittee staff that 61 full field investigations might not have been the meaning that the report to Congress intended to convey and that there might have been a misunderstanding due to poorly constructed writing in the report.

The exact language from the report was as follows:

> At the beginning of the reporting period, 193 preliminary inquiries were pending, and 139 more were initiated. Further investigation was not warranted in 50 instances; in 61 others, sufficient information was developed to justify full field investigations. (emphasis added)

In his testimony before the House Subcommittee, Mr. Skidmore also noted:

> A principal focus of the Investigations Branch is preventive enforcement. We try to thwart illegal transactions before they occur to avoid possible irreversible harm to national security. (emphasis added)

Our investigation revealed that preventive enforcement is far removed from the realistic objectives of the Investigations Branch. The Branch has about eight Special Agents, some formally trained in traditional law enforcement, some untrained. Most of their work they do on the telephone or by mail. There is some travel but the bulk of the work is done in the Washington headquarters of the Commerce Department. Investigative support is provided by a three-man field office in New York. In law enforcement, the term "preventive enforcement" suggests something quite different than an 8-member Investigations Branch that does most of its work from the office. Preventive enforcement means sending agents into the field, staying in close and frequent contact with the many segments of the affected community. Preventive enforcement is aggressive police work. Equally important, preventive enforcement means having an imaginative and resourceful intelligence capability as well. The Compliance Division has none of these. Nor does it practice anything even approaching preventive enforcement.

The official pronouncements of the Commerce Department reports to Congress and Congressional testimony are sharply different from the views expressed by experienced law enforcement personnel who are familiar with the operations of the Compliance Division. In pre-hearing interviews, one Special Agent currently employed in the Compliance Division had served for more than 20 years as an Army criminal investigator and has well established credentials as an investigator. He said the Compliance Division is "totally ineffective" in preventing dual-use technology from being shipped to the Soviet Union and Warsaw Pact nations. He said the Kremlin's spy organization, the KGB, could not have organized the Compliance Division in a way more beneficial to Soviet interests. This agent's view was not contradicted by persons in the law enforcement and national security field. Unfortunately, it was virtually impossible to persuade these persons to speak for attribution.

As will be noted later in this statement, the result of this reluctance to criticize constructively the Compliance Division in public session leads to the current situation in which the only evaluation the Congress hears is from the Commerce Department, which houses the Division and which is less likely to make a candid and forthright evaluation of the shortcomings of one of its own components. For that reason, it seemed important to the Minority staff that Congress be informed of the widespread dissatisfaction that exists in the Executive branch concerning the Compliance Division and the principal reasons for that dissatisfaction.

2. Commerce Principal Objective Is Trade Promotion, Not Regulation

The Department of Commerce has as its major focus the promotion of domestic and international trade. It is the finding of the Minority staff, based on interviews with officials of the Department and other agencies, that Commerce is not comfortable with the task of limiting the sale of anything, whether it is dual-use technology or some other commodity.

As a result, the Commerce Department has devoted insufficient resources to the Compliance Division. In 1967, for example, the Intelligence Branch of the Division had six or seven professional analysts. Today -- 15 years later -- the Intelligence Branch has two analysts and one detailee from another agency. This statistic was given the Subcommittee staff by the man in charge of the Intelligence Branch, who is deeply troubled by it. The Department of Commerce, therefore,

has reduced its commitment of resources in the intelligence field at the very time when the problem of technology diversions has become more pressing for the country.

The Minority staff is not the only entity that has questioned the depth of the Commerce Department's commitment to regulating technology transfers. In introducing legislation to create an Office of Strategic Trade, Senator Jake Garn of Utah said in Senate remarks on April 24, 1980 that the Commerce Department can be criticized for its work as "lead" agency in combatting diversions. Senator Garn said the Commerce Department had a "trade promotion bias" that prevented it from effectively protecting the country's national security interests. The Commerce Department has shown itself to be preoccupied with the goal of more and more trade with the Soviets to such an extent that the Department has become blind to national security considerations stemming from the sale of certain kinds of high technology data and machinery, Senator Garn said.

The result of the Commerce Department's inadequacies in controlling diversions has been an historic erosion in American technological pre-eminence, Senator Garn said, adding:

> What remains of our once vaunted military superiority, on which our national security increasingly depends, is in part being whittled away through a wide variety of technology transfer mechanisms. It is well documented that technology which the Soviet Union cannot develop will be bought from the West, and technology which the Soviets cannot buy will be stolen.

Mr. Chairman, I request that Senator Garn's bill, his floor remarks in introducing it and a May 8, 1980 "Dear Colleague" letter be sent to other Senators regarding the bill be received as exhibits to these hearings.

3. Commerce Department Has Limited Law Enforcement Tradition

The Commerce Department has limited tradition and limited expertise in traditional law enforcement. Yet the Compliance Division is perceived and described by the Department as being a law enforcement organization. Its personnel include Special Agents, whose titles alone suggest law enforcement assignments. The Special Agents are classified as Series 1811 federal criminal investigators.

The Compliance Division asserts its "lead" role in enforcing export controls for the entire government. The Division undertakes exercises requiring specialized law enforcement skills and capabilities such as the conduct of surveillances of suspected export controls violators.

But, because of its lack of tradition and expertise in law enforcement, the Commerce Department does not require that its Special Agents meet established standards of formal training. "On the job" training is common at the Commerce Department; yet there is no requirement that newcomers to the investigative ranks undergo formal training in the enforcement of export controls or in the most fundamental aspects of police work.

It may be a valid procedure to prepare new Special Agents by giving them "on the job" training. But the question must be asked: from whom are the new agents receiving their "on the job" training? If the training is provided by agents who themselves are marginally qualified, how valuable is the instruction?

The Agent's Manual is a basic instructional document in most law enforcement organizations. Each agent is given a copy of the Agent's Manual and is expected to study it and be fully and currently informed about it. The Agent's Manual describes proper procedures for the agent in every aspect of his professional life -- on points ranging from proper dress to the opening and closing of cases to the writing of reports of investigation.

We asked for a copy of the Compliance Division's Agent's Manual. Its status is not clear. We asked the Acting Director of the Division if we could see it. He gave us a bulky, loose-leaf binder and explained that it was the only such document in the building. We did not think that it was suitable for distribution to and retention by his Special Agents for frequent referral and updating; he concurred.

Another executive of the Division, asked if there was an Agent's Manual, described it as "a semblance of an Agent's Manual."

The absence of a comprehensive, compact and readily available Agent's Manual is reflective of a procedurally uncertain law enforcement environment in the Compliance Division.

The Chief of the Investigations Branch described the Compliance Division to us as a "non-traditional law enforcement organization." Our staff inquiry concurs in that judgment. In more traditional law enforcement organizations, each investigator must meet certain standards of investigative experience and training; and each investigator is supposed to be thoroughly versed in procedures as spelled out in an Agent's Manual.

The Acting Director of the Compliance Division acknowledged that there were problems in the operations of the Division. He said the problems could be

corrected but that such a process took time. Elaborating on this point that the government is slow to change, the Acting Director, a veteran of 25 years in federal service, said the Compliance Division was organized more than 30 years ago at a time when the challenge of export controls was not as great as it is today. But, he said, as export controls became more of an urgent problem to the United States in recent years, the Compliance Division had tended to remain in its previous configuration, making it inadequately equipped for the current technologically competitive world scene. We asked the Acting Director if the nation could afford to wait while the Commerce Department and its Compliance Division adjusted to new challenges in export controls. He had no answer to that query but he did say it was a valid question.

Executives in the Compliance Division have had insufficient law enforcement background and training to be supervising investigators on how to proceed in their inquiries. (By traditional criminal law enforcement training, the Subcommittee Minority staff means that the adequately trained official has been instructed formally on 1) collection and preservation of evidence; 2) interview techniques, including the handling of witnesses and confidential sources; 3) arrest procedures, including techniques used in searches, hand-cuffing and transportation of persons in custody; 4) criminal statutes; 5) issuance of, and training in, the use of firearms on a continuing basis; 6) courtroom procedures, trial preparation and testifying; and 7) surveillance techniques, including the use of electronic and photographic equipment. In addition, most federal criminal law enforcement agencies have specialized training courses in that area of the law they are responsible for enforcing. Refresher courses and programs aimed at keeping personnel informed of new developments in the law and enforcement also are offered.) The Director of the Compliance Division from 1963 to 1979 was a former Customs Appraiser in Chicago with limited experience and limited formal training in law enforcement before he got the job. He told the Minority staff that he did not believe experience or formal training were required for law enforcement work.

He was replaced in the office of Director of the Compliance Division by a person who also had limited traditional law enforcement experience. At this time, the position of Director of the Division is formally vacant. It is being filled on a parttime basis by William V. Skidmore, whose permanent position is Director of Anti-Boycott Compliance. Mr. Skidmore has limited traditional law enforcement experience.

The former Director of the Compliance Division told the Minority staff that on several occasions from 1979 through the first quarter of 1982 she recommended to senior officers of the Commerce Department that steps be taken to increase the effectiveness and numerical strength of the Division. The Department rejected many of her recommendations, she said.

4. Five-man Inspection Staff Is Too Small To Cover Entire Nation

Compliance Division inspectors have limited resources at airports and seaports to detect the export of controlled high technology commodities. The Chief of the Facilitation (Inspections) Branch told the Subcommittee staff that the number of inspectors -- five or six -- was insufficient. Most of the work they do is performed at the John F. Kennedy International Airport in New York.

The former Director of the Division informed the Minority staff that several of the inspectors were parttime employees, working about 32 hours a week and that they put in some overtime to compensate for their shorter work time.

Compliance Division inspectors are not authorized to search and seize suspected cargo. They must rely on U. S. Customs Service personnel. Similarly, unlike Customs agents and inspectors who have kindred and formalized working relationships with customs employees throughout many parts of the world, Commerce inspectors have no counterparts on any foreign soil.

5. Compliance Division Special Agents Not Required To Undergo Formal Training

Compliance Division Special Agents working in the Investigations Branch are not required to have any formal training in investigative techniques, law enforcement or the Export Administration Act. The approximately eight professional members -- the Special Agents -- of the Investigations Branch have varying degrees of law enforcement background. Some have extensive law enforcement background. Others have limited background in law enforcement. One Special Agent's previous job experience was secretarial.

The Chief of the Investigations Branch acknowledged that the Special Agents in the Compliance Division were not required to attend law enforcement training schools and that, while such educational programs were encouraged, the Special Agents had not attended them recently. What training in law enforcement the Compliance Division Special Agents had, he said, was what they had obtained before joining the Compliance Division. The Chief of the Investigations Branch

who had served for about two years as Acting Deputy Director of the Division, himself had come to the Division with no law enforcement training whatsoever, except for the fact that he is a lawyer.

As an introduction to their work in the Compliance Division, the Investigations Branch Chief said, newcomers were expected to read the Export Administration Act and were then encouraged to engage in frequent conversations with other more experienced agents to learn what they needed to know. He said major emphasis was placed on "on the job" training.

6. Size of Investigations Branch Backlog Is In Doubt

Most of the investigative work of the Investigations Branch is done in the office. Agents are expected to conduct inquiry on the telephone and by mail. The most frequent response to allegations of violations of the Export Administration Act is to send the alleged violator a letter of warning. In its FY '81 report to Congress, for example, the Commerce Department summed up the Compliance Division's work this way:

> The Compliance Division of the Office of Export Administration completed 258 full-scale investigations during October 1980 through September 1981. Of these, 33 cases were referred to the Department's Office of General Counsel for initiation of administrative proceedings; 145 cases resulted in warning letters to the parties involved for various violations considered not serious enough to warrant criminal or administrative proceedings; in three instances, educational advice was given to the firms; and 77 investigations were closed after a determination of no violation or insufficient evidence. In addition to the foregoing, three cases were referred to the Department of Justice for possible prosecution of criminal violations. The Division had 153 cases pending at the beginning of the period, of which 258 have been assigned to investigators, and had 311 cases pending at the close of the period.

The reference to 311 cases pending at the close of the period possibly would indicate that a backlog of 311 cases existed. However, it was not possible for the Subcommittee staff to determine the actual size of the backlog.

The Chief of the Investigations Branch said he was not sure how large the backlog was. The previous Director of the Division said the backlog was possibly as large as 300 or 400. The new Acting Director said he thought it was about 200 cases. However, he added that it had been the Division's policy in recent years not to close many cases for fear the Department would be criticized for closing out cases prematurely; this policy would lead to the conclusion that the backlog was bigger than it actually was, he said.

The staff inquiry concluded that a backlog of 200 or 300 or 400 with an investigative staff of eight agents seemed to be inordinately large. So many cases hovering over a relatively small investigative staff could create pressure on Special Agents to close cases without sufficient inquiry.

7. Intelligence Branch Has Backlog Of 600 'Matters'

The Intelligence Branch also has a significant backlog of unfinished business. When the Minority staff interviewed the Chief of the Intelligence Branch in March of 1982, he said he had a backlog of about 600 cases. He said that by the end of the calendar year, he could have a backlog of 1,000 cases.

The Acting Director of the Compliance Division said the backlog in the Intelligence Branch was about 600 but that it was 600 "matters," a large number of which did not qualify as actual cases. Therefore, he said, the backlog was considerably smaller than it might appear.

It is the view of the Subcommittee Minority staff that the backlog -- whether it is 600 "matters" or 600 cases -- is too large and its size has an important bearing on the efficiency of the entire Division. That is because many cases begin in the Intelligence Branch. A serious backlog there can cause delays throughout the system. Large backlogs prevent the entire Compliance Division from moving in a timely fashion against suspected violators.

8. Compliance Division Special Agents Lack Most Law Enforcement Tools

Compliance Division investigators have no authority to search and seize shipments suspected of being in violation of the export controls statute. They may detain cargo; however, as the Chief of the Investigations Branch admitted to the Minority staff, if the persons in possession of the suspected cargo resist having their shipment detained, Compliance Division personnel have no measure of established force to enforce their decision to detain.

For, coupled with their inability to search and seize is Compliance Division Special Agents' lack of authority to make arrests. In addition, Compliance Division agents have no authority to carry firearms and have no mobile communication equipment. Yet they carry out surveillance operations of suspected violators.

Several surveillances have been staffed and directed by Compliance Division personnel not extensively trained in the techniques of surveillance work.

Trained law enforcement personnel have told the Subcommittee staff that surveillance is one of the most difficult of all law enforcement exercises. They said they worked on many of them before they felt confident of themselves in this kind of pursuit; and before they felt they could direct others.

In addition, sending unarmed agents on surveillances is a procedure which some law enforcement officials question. Moreover, to conduct its surveillances, Compliance Division personnel have had to borrow mobile communication equipment from the U. S. Marshals Service and other agencies.

Untrained, unarmed, poorly equipped personnel conducting surveillances under the direction of inexperienced executives is a practice inherently risky. It also demeans and trivilizes the efforts of formally trained, properly equipped law enforcement agents whose surveillance work is performed according to established procedures. It is the finding of the Minority staff that if a surveillance is worth doing, it is worth doing in a professional, procedurally sound manner.

9. One Agent Had Job Of Investigating Grain Embargo Violations

In 1980, the Compliance Division received an assignment of national consequence in addition to its dual-use export controls work. The Division was given the responsibility to investigate violations of the grain embargo called for by President Carter in response to the Soviet Union's invasion of Afghanistan. This responsibility stemmed from language in the Export Administration Act that says it is the policy of the government—

> . . . to restrict the export of goods and technology where necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations . . .

In his letter to the President of the Senate and the Speaker of the House of January 21, 1980 regarding "Shipments of Agriculture Commodities to the Soviet Union," President Carter said the Soviet invasion of Afghanistan "requires a firm and vigorous response from the United States." President Carter went on to say that he had directed the Secretary of Commerce to restrict exports and reexports from the United States to the Soviet Union.

Under the heading of "Enforcement," the President's message added:

> No unusual problem is anticipated in enforcing the control on United States direct sales of agricultural products. With respect to reexports from third countries to the U.S.S.R., the fungible nature of the commodities makes it somewhat difficult to control their destination. The Department of Commerce and

other agencies will watch this situation closely and will take enforcement action in case of violation.

Mr. Chairman, I request that the President's message to the Congress be received as an exhibit.

A former Compliance Division investigator told the Subcommittee Minority staff that he was given the assignment of investigating embargo violations. He said no other agents in the Compliance Division were assigned to assist him.

At several interagency meetings of high level officials working on implementation of the grain embargo, the agent, himself a GS-12, was the sole representative of the Commerce Department. His security clearance was at the secret level and this meant that on some occasions he was not allowed to enter the meetings until issues requiring higher classification were discussed.

The other agencies -- USDA, CIA, State Department, Navy -- felt the matter was important enough to send senior officers while Commerce was represented by a GS-12, he said. The agent said he was embarrassed but was unable to persuade his supervisors that their agency was proceeding improperly by not sending a more senior spokesman.

As for the agent's principal assignment -- the investigation of alleged violations of the grain embargo -- the agent said he did the best he could with the limited resources he had.

The agent said that for the most part, the majority of his investigative work was from the office, as he relied on long distance telephone calls, cables to American embassies overseas and assistance from the Department of Agriculture and the Customs Service.

Not having law enforcement-minded counterparts in foreign nations was a problem for him, the agent said. He found cooperative U. S. embassy personnel on some of his requests for information on grain shipments. But, in other instances, he was met with delayed responses.

I spoke with the Agriculture Department official who was chairman of the high level inter-agency group which monitored the agricultural exports during the grain embargo. He said the group was formed early in 1980 when it became apparent that the Commerce Department was committing insufficient resources to assembling information about compliance and investigating allegations of violations. He said it was his understanding that "one or two" persons were

representing the Commerce Department in this task and that he saw that as "terribly limited" dedication of personnel. He said information assembled by the high level inter-agency group reflected a much broader base than the Commerce Department could have supplied by itself. He said, however, that "the hard core business of proving violations " – that is, the actual investigation – was the responsibility of the Commerce Department. He said members of the inter-agency group he chaired talked openly of the unsatisfactory commitment of resources by the Commerce Department. He said he recalled that the Commerce Department sent representatives to the inter-agency group meetings whose security clearances were not high enough to enable them to be there. He said in certain instances the Commerce Department representative had to wait outside the room until more sensitive issues were discussed.

In addition, the General Accounting Office, in a report of July 27, 1981, entitled "Lessons To Be Learned From Offsetting The Impact Of The Soviet Grain Sales Suspension," said the Compliance Division of the Commerce Department was charged with investigating allegations of illegal grain shipments to the Soviet Union. "At the outset," GAO said, "Commerce did not anticipate taking any other actions to monitor shipments."

However, GAO went on to say, "USDA officials believed that a more comprehensive monitoring program was necessary to ensure that U. S. grain was not being illegally shipped to the Soviet Union." This concern led to the formation of two groups in January of 1980 whose purpose was to provide more information. One group was largely an internal organization within USDA. GAO said the second group was "comprised of policy-level officials from USDA, State Department, CIA, Navy and Commerce," GAO said.

Mr. Chairman, I request that the GAO report of July 27, 1981 be received as an exhibit.

The Minority staff inquiry found that the inadequate response of the Compliance Division in enforcing the grain embargo demonstrates the serious government operations problem in which the most senior officers of the executive branch, from the President on down, shape policy and promulgate directives on the mistaken premise that the affected agencies have the necessary means to turn the policy and directives into reality. President Carter's grain embargo speech might have been received in a different light had he also announced the Commerce Department would assign one man – a GS-12 in the Compliance Division – to investigate alleged violations.

10. Lack Of Harmony Between Compliance Division And Customs Service

A lack of close cooperation existed between the Compliance Division and the U. S. Customs Service. The result was that effective enforcement was reduced. Part of the tension between the two agencies stemmed from the Commerce Department's interpretation of Section 12-C of the Export Administration Act. The Department interpreted the Section in such a way as to preclude sharing proprietary information with other law enforcement organizations. In interviews with Minority staff, Customs personnel complained bitterly about the Commerce Department's interpretation of 12-C. Section 12-C is as follows:

> (c) Confidentiality.--
> (1) Except as otherwise provided by the third sentence of section 8(b)(2) and by section 11(c)(2)(C) of this Act, information obtained under this Act on or before June 30, 1980, which is deemed confidential, including Shippers' Export Declarations, or with reference to which a request for confidential treatment is made by the person furnishing such information, shall be exempt from disclosure under section 552 of title 5, United States Code, and such information shall not be published or disclosed unless the Secretary determines that the withholding thereof is contrary to the national interest. Information obtained under this Act after June 30, 1980, may be withheld only to the extent permitted by statute, except that information obtained for the purpose of consideration of, or concerning, license applications under this Act shall be withheld from public disclosure unless the release of such information is determined by the Secretary to be in the national interest. Enactment of this subsection shall not affect any judicial proceeding commenced under section 552 of title 5, United States Code, to obtain access to boycott reports submitted prior to October 31, 1976, which was pending on May 15, 1979; but such proceeding shall be continued as if this Act had not been enacted.

In Customs and in other offices of the executive branch -- both in law enforcement and in national security affairs -- there is an unwillingness to say anything critical in public about the effectiveness of the Compliance Division. The reluctance to criticize the Compliance Division exists amid a widespread sense throughout affected areas of government that the investigative capabilities of the Compliance Division are inadequate.

The failure not to criticize the Commerce Department ignores the fact that because of the inadequacies of the Compliance Division significant amounts of dual-use technology that contribute to Soviet military strength are being shipped to the Soviet Bloc.

The Minority staff should not be the only entity to make an evaluation of the effectiveness of the Compliance Division. It was our hope that other law

enforcement organizations would come forward and critique the Division in a constructive and professional manner. In this pursuit, we were met with resistance. Working agents and senior officials alike would be candid, while insisting on their anonymity.

The Subcommittee staff did obtain a copy of a memorandum written by a senior Customs Service official who was critical of the Compliance Division's procedures. The memorandum, dated October 30, 1980, was written by William Green, Deputy Assistant Commissioner in the Office of Border Operations. The memorandum was sent to Robert L. Keuch, Associate Deputy Attorney General and Chairman of an Inter-Agency Working Group on Export Control. Green had this to say about the Compliance Division of the Commerce Department:

> . . . . What is particularly significant is Commerce's (OEA/CD) continued action to impede cooperation in investigations even while it states that it wishes to fully participate in all cooperative ventures. Commerce continues to take unilateral and uncoordinated action concerning either joint or Customs initiated investigations by requesting foreign inquiries through various U. S. embassies and consulates without consulting with either Customs Attaches or Headquarters. Such action is causing serious problems. These problems are not limited to hampering instant investigations, but also the compromising of U. S. Customs and foreign government sources, damaging the previously close and long relationships between U. S. Customs and their foreign counterparts, and directly impacting on national security.
>
> These unilateral actions taken by Commerce are not limited to investigations initiated solely by Commerce and being worked only by them; but more importantly, include investigations initiated by Customs and now being either jointly worked by both agencies, or by Customs alone. . . .
>
> While Customs acknowledges that, under the Export Administration Act of 1979, OEA/CD is the agency primarily responsible for administration and enforcement of the Act, OEA/CD is not at this time adequately staffed to enforce the Act. OEA/CD has stated that it is planning to establish foreign offices, together with adequate staffs, and assume those duties related to export control enforcement which the EDO's and Customs Attaches now perform.. Once again, OEA/CD is not adequately staffed to assume these duties and does not have experience concerning the conduct of investigations abroad. OEA/CD is also at a distinct disadvantage in that they have no foreign counterparts with whom they can relate and/or work. They will not have access to Customs mutual assistance agreements on which they can rely to gain access to investigative data and/or other desirable information, nor is it anticipated they will be able to establish such agreements. The U. S. Customs Service is in a much better position to conduct export control investigations and inquiries abroad because we do have foreign counterparts with whom we work and relate; we do have formal and informal agreements with our foreign counterparts; we have established foreign offices with a staff of experienced investigators and have conducted export control investigations and inquiries abroad since at least before 1900....
>
> The only answer is a single-agency concept for all export control enforcement. While not faulting Commerce in its

> attempt to increase its enforcement posture, it should be noted that Customs already has the necessary authority, has a foreign presence that has been in place for at least 80 years, has over 60 domestic offices, has over 500 experienced criminal investigators, and has had experience in export control matters since early in the history of our country. Concerning additional resources, it has been stated that if Customs should assume the entire export control enforcement program it would need approximately 25 additional slots. While this figure may change due to exigencies such as workload, source development, and foreign liaison, it should be noted that any new personnel gained because of the resource increase would not be initially assigned sohisticated critical technlogy cases, but would be assigned to experienced investigators. The new agents would take up the slack caused in lesser areas of the Customs enforcement program.

Mr. Chairman, I request that Mr. Green's memorandum be received as an exhibit.

11. CTC Case Demonstrated Shortcomings In Compliance Division

The many shortcomings of the Compliance Division as a law enforcement organization are apparent in the investigation of a syndicate of businesses, known as the CTC group, owned, controlled or utilized by a West German named Werner J. Bruchhausen. Mr. Chairman, I have prepared a summary of the CTC case which was drawn from information provided the Minority staff by Commerce Department agents, Customs Service agents, the Department of Justice and other sources. It is rather lengthy. I request that it be printed in the hearing record as if read and that I be allowed to give a brief description of what occurred in the CTC case.

From 1977 to 1980, the CTC network of companies in the U. S. and Western Europe bought dual-use technology under false pretenses in the U. S. and then exported it to the Soviet Union and Warsaw Pact.

As will be pointed out in the testimony of Dr. Lara Baker, a computer scientist from the Los Alamos National Laboratory, the CTC syndicate of companies was not buying up high technology equipment at random. They had been given a precise shopping list by the Soviets. As Dr. Baker will point out, the equipment the CTC syndicate bought was for the specific purpose of building and equipping a semi-conductor plant in the Soviet Union. Moreover, a businessman who served briefly as a consultant to the Soviet Union will testify during these hearings that it was apparent to him during a visit to Moscow that such a semi-conductor plant had been built in the U.S.S.R. and the Soviets were in the process of equipping it with American-made machinery.

The existence of the CTC network of companies was first brought to the attention of the authorities in 1977 and 1978 when two anonymous letters were received at the American Consulate in Dusseldorf. The State Department translated the letters into English and referred them to the Compliance Division in the Commerce Department. The Minority staff has established that the letters were received by the Compliance Division in 1978 and that insufficient effort was made to investigate the allegations.

Subsequent to the receipt of the letters, two U. S. producers of dual-use technology reported to the Commerce Department that they were suspicious of the CTC companies. Insufficient inquiry was conducted in response to the first letter.

A Commerce Department Special Agent did interview CTC's principal executive in Los Angeles, a naturalized Russian-born American citizen named Anatoli Maluta, also known as Tony Maluta and Tony Metz. Maluta told the Special Agent from Compliance that he did not know anything about export controls, or the need to have validated export licenses to ship certain controlled commodities. But, Maluta said, because of the agent's interest, he was cancelling the suspicious order.

Maluta's cancellation of the suspect shipment should have triggered increased curiosity in the agent's mind to want to investigate further. But there is no evidence that he did. No further investigation of the CTC network was conducted until a second letter arrived at the Compliance Division, this time from another high technology producer who also voiced suspicions about the CTC companies.

Early in 1980, a second Compliance Division agent, Robert Rice, was assigned to the case and conducted the kind of comprehensive preliminary inquiry that was called for. Rice, the most senior agent in the Division, came upon considerable information indicating widespread violations of export controls.

Rice presented the evidence to the Office of the U. S. Attorney in Los Angeles in March of 1980. A major inquiry was begun by the U. S. Attorney's Office, under the direction of Assistant U. S. Attorney Theodore W. Wu and the U.S. Customs Service. Customs ultimately assigned about 15 agents to the case in California, Texas, New York and Western Europe. Compliance Division Special Agent Rice was the only Commerce Department representative assigned to the case on a regular basis.

Indictments were brought against Bruchhausen and Dietmar Ulrichshofer, both of whom remained in Europe and are fugitives from American justice, and two

Los Angeles accomplices — Maluta and Sabina Dorn Tittel. Maluta and Tittel both were convicted.

The CTC case demonstrated technology diversions of about $10 million and is considered by law enforcement and national security specialists to be one of the most important export control case ever brought to trial.

The inquiry showed that:

1. The Compliance Division did not move quickly to establish the value of the anonymous letters.

2. The Compliance Division did not connect the anonymous letters to the allegations that were reported by two U. S. manufacturers.

3. When Compliance Division Agent Rice turned over the results of his inquiry to Assistant U. S. Attorney Wu in Los Angeles, it was apparent to Wu that considerable expenditures of resources would be needed. Trained investigators would be required to conduct interviews, evaluate shipping documents, surveil suspected violators and carry out other aspects of a traditional law enforcement full-scale, full field investigation. Commerce's contribution to that effort was Agent Rice, a competent investigator in whom Wu had confidence. But he needed more than one agent. He enlisted the assistance of the Customs Service. Later assistance was provided by trained criminal investigators from the Internal Revenue Service.

4. At an early point in the inquiry, it was necessary to seize shipments. Commerce had neither the authority nor the manpower to seize shipments. Customs did it.

5. At another point in the inquiry, it was necessary to search premises of CTC companies and the quarters of certain of his employees in the U. S. and Europe. The Compliance Division had insufficient resources to implement simultaneous search warrants. The Compliance Division had no law enforcement capabilities in Western Europe to work with German Customs in coordinating the searches abroad. Customs executed the warrants in the U. S. and, through its agreements with West German customs, arranged for the execution of the warrants in Germany.

6. To substitute sand for one of CTC's shipments to Moscow, a sizable expenditure of funds was needed. The Compliance Division balked at the shipment substitution strategy and refused to pay the cost of recrating the sand and air freight. Customs officials approved of the substitution and agreed to pay the cost.

7. Extensive overseas coordination, in addition to the search warrants, was called for with West German Customs and other foreign officers. Commerce Department's Compliance Division had no overseas law enforcement contacts. U. S. Customs' contacts were used.

8. Extensive surveillance was necessary. Armed Customs agents and armed Internal Revenue Service criminal investigators and an unarmed Compliance Division Special Agent Rice provided it. Two suspects under surveillance had firearms in the backseat of their car. The firearms were not used. But it was an important law enforcement advantage for the agents on surveillance to be armed as well.

9. Experienced supervisors with law enforcement background and training were needed to direct the inquiry in the field. The Office of the U. S. Attorney for the Central District of California working with supervisorial personnel in the Customs Service, provided the needed direction. Contact with supervisorial personnel in the Compliance Division, who remained in Washington, was made on the telephone and the persons who worked the case in California did not consider such communication to be satisfactory.

10. When the appropriate time came to apprehend Anatoli Maluta and Sabina Dorn Tittel, IRS agents made the arrests. Customs agents, like the trained IRS criminal investigators, are authorized to make arrests. Even had the Compliance Division dispatched sufficient numbers of agents to assist in the inquiry, they could not have arrested the suspects.

It is noteworthy that in its Fiscal Year 1981 report to Congress, under the heading "Criminal Proceedings," the Commerce Department described the CTC inquiry, listed the charges in the indictments, identified certain companies in the CTC network of companies which were denied export privileges and then concluded by taking credit for the case. The report said:

> The order (to deny export privileges) was issued to protect national security and the public interest in view of the facts revealed in the investigation of these parties by the Department.

In fact, the CTC case does not qualify as a Commerce Department investigation. Customs Service agents did most of the work; and executive supervision was provided by Assistant U. S. Attorney Theodore Wu and Kenneth Ingleby, the Chief of the Customs Service Investigations Office in San Pedro.

In participating in the inquiry on a fulltime basis and in conducting himself in a competent, professional manner, Compliance Division Special Agent Robert Rice was handicapped in not being able to do the things Customs agents can do routinely — search and seize suspicious freight, make arrests and carry a weapon. Capable and resourceful as he was, Rice cannot be considered to have been essential to the CTC inquiry. It could have succeeded without him. It could never have succeeded without the Customs Service. Customs contributed necessary manpower and fundamental law enforcement tools. Commerce's contribution was Robert Rice.

After the CTC case was brought to Wu, the Compliance Division played no essential role in the inquiry. That recognition leads to the Minority staff's final finding, which is that the Commerce Department should not have the enforcement function under the Export Administration Act.

It is the finding of the Minority staff that the national security implications of enforcement of the Export Administration Act are too important to be entrusted any longer to the Commerce Department as presently organized.

For three decades the enforcement function has resided in the Commerce Department -- through Administrations controlled by Democrats and Republicans. Three decades is sufficient time to allow reasonably capable officials to perfect the most challenging task. But serious procedural and operational problems still exist in the Compliance Division of Commerce. We find the conclusion inescapable, therefore, that effective enforcement of the Export Administration Act is beyond the institutional capabilities of the Commerce Department. Moreover, from a government operations and executive organizational standpoint, the mere existence of the Compliance Division is an impediment to efficient and effective enforcement of the Act. Understaffed, flagrantly short of resources, the Division cannot do the job effectively; but, by its presence, prevents other components of government from taking on the task.

It is our view that two solutions -- one short term, one long range -- are available. Immediate relief could be found if the Compliance Division were abolished and all its functions placed in the U. S. Customs Service. This action would insure that competent, professional agents, trained in formal, traditional law enforcement procedures, would be assigned to investigate alleged violations of the Export Administration Act; that they would work under the supervision of executives who also would have formal, traditional law enforcement backgrounds;

and, perhaps most important of all, the entire function would exist in a Cabinet-level Department with longtime experience in and commitment to traditional law enforcement. It is the staff's recommendation that Subcommittee Members consider that concept as an immediate solution as these hearings proceed.

In addition, in terms of longer range considerations, it is our recommendation that Subcommittee Members consider the proposal put forward by Senator Garn to create an independent Office of Strategic Trade that, in summary, would absorb the Commerce Department's Office of Export Administration and its components.

Mr. Chairman, that concludes my portion of the staff presentation. I request that the summary of the CTC case be printed at this point in the hearing as if read.

The following summary of the CTC case was written by Fred Asselin of the Subcommittee Minority staff. It is based on information provided by Commerce and Justice Department, U. S. Customs and other sources.

CTC Network Was Formed In 1977

On October 23, 1974, Werner Jurgen Bruchhausen, a 34-year-old West German residing in Los Angeles, incorporated four companies in Southern California for the purpose of buying and selling sophisticated electronic equipment. The firms all used the address of 4676 Admiralty Way in Marina Del Rey. Subsequently, Bruchhausen incoporated eight other entities in Southern California.

Bruchhausen, who was born on November 5, 1939 in Dortmund, West Germany and who listed his home as being D8019 Niederseeon 21 in West Germany, enlisted the aid of two associates in setting up his firms -- Anatolij T. M. Maljuta of 231 Calle Mayor, Redondo Beach, California; and Sabina Dorn Tittel of 30605 Cartier Drive, Rancho Palos Verdes.

Maljuta, who was born in Kharkov, Russia on January 25, 1920, was a naturalized American citizen. He used three aliases -- Anatoli T. M. Maluta, Tony Maluta and Tony Metz. Tittel was born on January 13, 1950 in Gumbsheim, West Germany. Divorced, Tittel was unmarried, as was Bruchhausen. Maluta's wife was named Aida.

Of the four companies Bruchhausen created in 1974, the principal enterprise was CTC California Technology Corporation. From its inception through 1980, CTC utilized 18 other trade styles, 12 of which were incorporated in California. In the four-year period of 1977 to 1980, CTC and its variants, under the direction and supervision of Anatoli Maluta and Sabina Dorn Tittel, purchased high technlogy electronic equipment, peripherals and components valued in excess of $10.5 million. Most of the items they purchased were classified as strategic commodities, controlled for national security purposes and requiring United States export licenses granted by the Departments of State and Commerce.

In the same four-year period, CTC exported from the United States to Germany, the Soviet Union, or the Soviet Bloc more than 300 shipments consisting of strategic commodities. None of the commodities had proper export licenses. The shipments were documented with fraudulent U. S. Shipper's Export

Declarations (SED's). Most of the exports were sent to West Germany consigned to companies controlled by or associated with Werner J. Bruchhausen. From West Germany, most of the commodities were transshipped to Switzerland or Austria or to other intermediate countries and then transported to the USSR or to a Warsaw Pact nation.

The entities located in Southern California that comprised the Bruchhausen or CTC group were as follows:

Interorga International Components and Equipment Sales Organization
4676 Admiralty Way, Marina Del Rey, California
Incorporated: October 23, 1974, file No. 740201
Statement of domestic stock corporation, filed August 31, 1977, file No. 77198790
Chief executive officer: Werner J. Bruchhausen, Marina Del Rey
Secretary: Anatoli Maluta, Marina Del Rey
Chief Executive officer: Anatoli Maluta
Directors: Werner Bruchhausen, Anatoli Maluta, Aida Maluta

Interebdo Ebdo International Inc., dba ADT International Inc.
Post Office Box 9076, Venice, California
4676 Admiralty Way, Marina Del Rey
Incorporated: October 23, 1974, file no. 740203
Statement of domestic stock corporation, filed December 2, 1974, file No. 74180292
Dissolved: February 26, 1979
President: Volker Brandlmeier, Marina Del Rey
Vice President: Barbara Brandlemeier, Marina Del Rey
Secretary/Treasurer: Barbara Brandlmeier
Directors: Herbert Abrams, Marilyn McCumber, Volker Brandlmeier
The name of this corporation was changed to ADT International, Inc., on March 24, 1975, file No. 153552.

CTC California Technology Corp.
4676 Admiralty Way, Marina Del Rey, California
Incorporated: October 23, 1974, file No. 740200
Statement of Domestic Stock Corp., filed December 2, 1974, file No. 74190291
Dissolved: February 26, 1979
President: Volker Brandlmeier, Marina Del Rey, California
Vice President: Barbara Brandlmeier, Marina Del Rey, CA
Secretary/Treasurer: Barbara Brandlmeier
Directors: H. Abrams, Marilyn McCumber, Volker Brandlmeier

MTL Measurements and Test Laboratories, Inc.
4676 Admiralty Way, Marina Del Rey, California
Incorporated: October 23, 1974, file No. 740200
Statement of Domestic Stock Corp., filed December 2, 1974, file No. 74190291
Dissolved: February 26, 1979
President: Volker Brandlmeier, Marina Del Rey, California
Vice President: Barbara Brandlmeier, Marina Del Rey, CA
Secretary/Treasurer: Barbara Brandlmeier
Directors: Herbert Abrams, Marilyn McCumber, Volker Brandlmeier

Electronic Continental Industries, Inc.

4676 Admiralty Way, Marina Del Rey, California
Incorporated: June 30, 1977, file No. 820513
Statement of Domestic Stock filed August 29, 1977, file No. 77186369
Dissolved: February 26, 1979
Chief Executive Officer: Werner Bruchhausen
Secretary/Chief Financial Officer: Anatoli Maluta
Directors: Werner Bruchhausen, Anatoli Maluta, Aida Maluta

Interorga Europe, Inc.
4676 Admiralty Way, Marina Del Rey, California
Incorporated: October 25, 1977, file No. 830539
Statement of Domestic Stock Corp., filed December 29, 1977, file No. 77271373
Dissolved: February 26, 1979
Chief Executive Officer: Werner Bruchhausen, Marina Del Rey, California
Secretary: Anatoli Maluta, Marina Del Rey, California
Chief Financial Officer, Sabina D. Tittel, Marina Del Rey, CA
Directors: Werner Bruchhausen, Anatoli Maluta, Sabina D. Tittel

Atlantic Universal Supply, Inc.
4804 Macafee Road, Torrance, California
dba: AUS, 21515 Hawthorne Boulevard, #646, Torrance, CA
Incorporated: July 3, 1978, file No. 868824
Statement of Domestic Stock Corp., filed November 19, 1979, file No. 79310442
Chief Executive Officer: Tony Maluta, Redondo Beach, CA
Secretary: Sabina D. Tittel, Torrance, California
Chief Financial Officer: Sabina D. Tittel
Directors: Tony Maluta, Sabina Tittel

Consolidated Protection Development Corp.
21515 Hawthorne Boulevard, #646, Torrance, California
Incorporated: July 3, 1978, file No. 868822
Statement of Domestic Stock Corp., filed December 10, 1979, file No. 79324737
Chief Executive Officer: Tony Maluta, Redondo Beach, CA
Secretary: Sabina D. Tittel, Torrance, California
Chief Financial Officer: Sabina D. Tittel
Directors: Tony Maluta, Sabina D. Tittel

American Data Technology Corp.
231 Calle Mayor, Redondo Beach, California (2)
Incorporated: July 12, 1978, file No. 869313
Statement of Domestic Stock Corp. filed: December 10, 1979, file No. 79324736
Chief Executive Officer: Tony Maluta, Redondo Beach, CA
Secretary: Sabina D. Tittel, Torrance, CA
Chief Financial Officer: Sabina D. Tittel
Directors: Tony Maluta, Sabina D. Tittel

Digital Security Corp.
231 Calle Mayor, Redondo Beach, California
Incorporated: May 25, 1979, file No. 931745
Statement of Domestic Stock Corp., filed August 21, 1979, file No. 79231486
Chief Executive Officer: Rainer Hildebrand, Bonn, West Germany
Secretary: Eric Roos, Dusseldorf, West Germany
Chief Financial Officer: Tony Maluta, Redondo Beach, CA
Directors: Rainer Hildebrand, Eric Roos, Tony Maluta, Sabina Tittel

Continental Technology Corp.
21515 Hawthorne Boulevard, #646, Torrance, California
23868 Hawthorne Boulevard, #100, Torrance, California
Incorporated: May 25, 1979, file No. 931746
Statement of Domestic Stock Corp., filed August 21, 1979, file No. 79231485
Chief Executive Officer: Roland Sturm, Munich, West Germany
Secretary: Rainer Hildebrand, Bonn, West Germany
Chief Financial Officer: Tonyt Maluta, Redondo Beach, CA
Directors: Roland Sturm, Rainer Hildebrand, Tony Maluta, Sabina D. Tittel

Universal Digital Corp.
4804 Macafee Road, Torrance, California (3)
1843 Lincoln Blvd., Suite 202, Santa Monita, CA (4)
Incorporated: May 25, 1979, file No. 931741
Chief Executive Officer: Eric Roos, Dusseldorf, West Germany
Secretary: Rainer Hildebrand, Bonn, West Germany
Chief Financial Officer: Sabina Tittel, Torrance, California
Directors: Eric Roos, Rainer Hildebrand, Sabina Tittel, Tony Maluta

CTC Group Used Companies Overseas

In addition to the California-based entities comprising the CTC group, Bruchhausen also controlled or was associated with several other enterprises, including entities in West Germany, Austria and Switzerland.

The CTC group's associates in West Europe included Dietmar Ulrichshofer, Hans-Jurgen Koenig, Sybille Ziogas, and Frank and Karin Nassauer.

Ulrichshofer, born in Austria on May 27, 1940, owned electronics supply companies in Vienna and Bad Reichenhall, West Germany. Koenig, who lived in Bonn, was born on May 12, 1940, and was general manager of electronics supply firms in Dusseldorf, and the West German capital.

The foreign entities utilized or owned by the Bruchhausen group were as follows:

ADT Analog Und Digital Technik
D-8019 Neiderseeon 21, West Germany
Commenced Business: 1978
General Manager: Werner Bruchhausen
Operation: Import, export, distribute and manufacturer electronic building parts and equipment

Elubat Vertriebsgellschaft Fur Elektronik Und Batterien Mbh
Goethestrasse 11, 4000 Dusseldorf, West Germany
Commenced Business: December 30, 1977, under Registry number HRB 595, dated April 7, 1978
Managers: Detlef Lackmann, Werner Bruchhausen
Ownership: ADT Analog and Digital Technik Bauelemente and Gerate-Vertrieb, Gmbg - 50%, Detlef Lackmann - 50%
Operation: Wholesale of electronical elements, batteries and similar articles

Techma Technische Maschinenhandels - Gesellschaft Mbh
Koeingstrasse 10, D-4000 Dusseldorf, West Germany
Commenced Business: February 27, 1978, under Registry Number HRB 13228, dated February 27, 1978
General Manager: Hans-Jurgen Koenig
Ownership: Hans-Jurgen Koenig - 100%
Operation: Distribution, import and export of machine and products of the mechanical engineering, as well as electric devices

Elmasch Vertriebsgesellshaft Fur Produkte Der Electrotechnik Und Des
Maschinenbaues Mgh Bergstrasse 185, 5300 Bonn 1, West Germany
Commenced Business: February 27, 1978, under Registry Number HRB 2478, dated June 19, 1979
General Manager: Hans-Jurgen Koenig
Ownership: Hans-Jurgen Koenig - 90%, Stefan Wagner - 10%
Operation: Distribution, import and export of electrotechnical and mechanical products

Electronic Elektronechnische Bauelmente Handelsgesellshaft Mbh
4951 Ameisasse, 1140 Vienna, Austria
Commenced Business: October 30, 1974, under Registry Number B-9060, dated November 23, 1964
Managers: Dietmar Ulrichshofer, Helmut Hartner
Ownership: Dietmar Ulrichshofer
Operation: Distribution of electronic component parts and apparatus as well as other technical articles, mainly in Eastern Europe (80%)

Ing. Ulrichshofer, Dietmar Vertrieb Electronischer Bauelmente Und Elektronischer Gerate
Baderstrasse 5, 823 Bad Reichenhall, West Germany
Commenced Business: November 1974 under Registry Number HRA 3530, dated 1976
Sole Proprietor: Dietmar Ulrichshofer
Ownership: Dietmar Ulrichshofer
Operation: Wholesale in (5%) import of (20%) and export (75%) electronic components, mainly semiconductors. Exports to European countries.

Solid State Electronics SA
DBA: SSC Solid State Commerz AG, Zurich, Switzerland
Commenced Business: April 26, 1971
Director: Dr. Juraj Tamas Zabratzky
Operation: Trade in products of the electronic industry and related products, take-over of agencies of all kinds, rendering of commercial services of all kinds, acquisition of participations and real property as well as acquisition, registration and exploitation of patent rights of all kinds.

Intra-engineering, GmbH
Goethestrasse 11, D-4000 Dusseldorf, West Germany
Commenced Business: December 30, 1977, under registry HRB 13197
General Manager: Ing. Gerhard Drost
Operation: Development, planning and construction of plants.

Universal Transport GmbH
Cologne, Dusseldorf and Munich, West Germany

Commenced Business: July 19, 1968, under Registry No. HRB 2296, dated July 27, 1978
Operation: Forwarding and transports of all kinds (air, road and water); especially international forwarding for import and export; customs clearance and air freight.

Panalpina AG
Zurich, Switzerland
Commenced Business: 1920
Operation: Freight forwarder to all parts of the world. Wholesale trade with various butcher articles, such as sausage machines, guts, etc. The firm does mainly transit trade, and there is practically no activity in Switzerland.

Copex Air B. V.
Subsidiary of shipping and forwarding "SAFF" B. V.
Schiphol, Metherlands
Commenced Business: January 18, 1977
Managers: G. H. F. Smit, A. M. Hageman
Operation: Air freight forwarding.

1977, 1978 Anonymous Letters Accused CTC Syndicate

In June of 1977 and February of 1978, the United States Consulate in Dusseldorf received anonymous letters alleging that [illegible]ies in the CTC syndicate were violating U. S. export control laws prohibiting the sale and delivery of certain high technology items to the Soviet Union and Warsaw Pact.

Signed "former employee," the June 20, 1977 letter alleged that the CTC group of companies in the United States were falsifying export documents as they shipped commodities from the U. S.; or were routing their cargos to Western European transshipment points through Mexico and South America.

Among the items which "former employee" alleged CTC had exported illegally was an underwater sonar system and accessories with a total value of $200,000. Presently, the letter went on to say, CTC executives were working with Intra-Engineering of Dusseldorf in assemblying for subsequent illegal sale a "complete system for the manufacture of semiconductors, ICs, for an embargoed system, and which will be purchased in the USA and delivered via circumvention of export laws."

The anonymous letter said the CTC group first purchased the high technology equipment through an enterprise in Los Angeles known as "ADT International Interorga & CTC." The European firm that received the products and transshipped them to embargoed nations was identified as "ADT Analog and Digita Technik Bauelemente und Geraete Vertrieb GmbH, Talstrasse, 22, Dusseldorf."

The head of the CTC network was described as being a German citizen who maintained an apartment near Dusseldorf but whose home was in the U. S. in a community called "Merinabay."

The name "Schneider" was signed at the bottom of the February 11, 1978 anonymous letter to the American Consulate in Dusseldorf. Much more detailed in its allegations, Schneider's letter said the CTC syndicate included five firms --ADT International, Interorga and CTC, all of Los Angeles; Solid State Electronics of Locarno, Switzerland; Intra-Engineering of Dusseldorf and Analog and Digitaltechnik of Dusseldorf.

Using the network of six firms, CTC employees were said to arrange for the shipment from the U. S. to West Germany of high technology products. From Germany, Schneider wrote, the products were transshipped to embargoed nations through a Zurich company known as Panalpina, the latter enjoying "a handsome profit from the business."

Schneider described one series of transactions this way. In December of 1970, he said, CTC bought Watkins-Johnson electronic components for $60,000. Schneider said the component was resold for $105,000 and the $45,000 profit "was, according to our observations, never taxed."

Schneider went on to say that in 1976 and 1977 CTC shipped to Horst Jonas in Dusseldorf high technology components that included controlled products manufactured by Tektronic, Hewlett-Packard, RCA and Varian Palo Alto. Schneider also said Horst Jonas sold an IBM high speed printer to an embargoed country late in 1977 through a Stuttgart firm doing business as Datenverarbeitung Klaus Huebner, GmbH.

CTC executives were bringing suit in Dusseldorf to force Horst Jonas to pay for electronic goods shipped to him, Schneider said, adding that CTC had realized great profits from illegal sales of controlled commodities. Schneider said the CTC group had obtained a loan commitment from a bank in Dusseldorf to build a German-based plant, stocked with American equipment, for the manufacture of semiconductors.

Anonymous Letters Were Referred To Commerce Department

The two anonymous letters were referred to the Bureau of East-West Trade in the Department of State. There, the letters were translated into English

and, in April or May of 1978, they were sent to the Compliance Division of the Office of Export Administration in the Department of Commerce. The Compliance Division has the responsibility to enforce the Export Administration Act and to investigate violations. No investigation was initiated as a result of the letters.

Perkin-Elmer Contacted Commerce In 1979

On April 19, 1979, George Hunter, a Special Agent in the Compliance Division of the Office of Export Administration in the U. S. Department of Commerce, was contacted by Robert Markin, director of Administration in the Perkin-Elmer Company of Wilton, Connecticut.

Markin told Hunter that CTC California Technology Corporation of Marina Del Rey had placed a purchase order with Perkin-Elmer on July 7, 1978 for a sophisticated piece of semiconductor testing equipment commercially named "Micralign," valued in excess of $150,000 and requiring a validated export license to be shipped overseas and not licensable for shipment to Soviet Bloc countries.

Markin told Hunter that he had learned that the Soviets were offering several million dollars for the system. It was this information, Markin said, that had prompted him to conduct his own background check into CTC California Technology Corporation. Based on his inquiry, Markin said, he suspected that California Technology Corporation was a "front" company whose intention was to divert the Micralign system to East Bloc countries.

Commerce Interviewed Maluta In 1979

On April 27, 1979, Walter Blackhall, a Special Agent in the Compliance Division at Commerce Department, interviewed Anatoli Maluta in the CTC offices, which were then located at 21515 Hawthorne Boulevard in Torrance, California. Blackhall arranged the interview as a result of information provided by Robert Markin of Perkin-Elmer Company regarding the Micralign system.

Maluta told Blackhall that he had become president of CTC California Technology Corporation in 1978. Maluta said he then renamed the firm Consolidated Protection Development Corporation. Maluta said the founder of the company was Joe (Volker) Brandlemeier.

Maluta said his firm's export business was small and that it specialized in serving as a broker for foreign companies and in locating spare parts and components. Maluta said his company did not export the parts and components, but rather identified for foreign clients those American enterprises that could sell the desired items.

Concerning the Micralign system, Maluta said the order for the equipment had been requested by a salesman for a Dusseldorf firm known as Elubat, GmbH. Maluta said Elubat planned to resell the system in West Germany.

Maluta said his West German purchasing agent did not order commodities by means of formal purchase orders but placed orders by telephone instead.

Blackhall asked Maluta for documentation on the purchase of the Perkin-Elmer Micralign system. Maluta replied that he kept no such records and that he had no notes on his telephone conversations with Elubat representatives. Maluta did have a purchase order, a copy of which he gave Blackhall.

Blackhall asked Maluta if he knew that the Micralign system required a validated export license issued by the Commerce Department and an import certificate from West Germany to export the system from the United States. Maluta replied that he knew little about export regulations. Blackhall then said that because of the possibility of an attempted diversion of the Micralign system, he wanted copies of all documents relative to any license application submitted by Maluta. Maluta replied that because of the Commerce Department's interest in his desire to buy the Micralign system he would cancel the order with Perkin-Elmer.

Maluta Cancelled Micralign Order

Commerce Department Agent George Hunter contacted Elmer-Perkin on May 21, 1979. Hunter was informed that Consolidated Protection Development Corporation, formerly CTC California Technology Corporation, had cancelled its order for the Micralign system.

Fairchild Warned Commerce About CTC In January of 1980

Fairchild Test Systems Group of San Jose, California, wrote to the Commerce Department on January 31, 1980, to express concern about the export activities of Consolidated Protection Development Corporation. As a result of its

concern, Fairchild had decided to hold up delivery of several Fairchild/Xincom semiconductor memory test systems with a total value of $740,000 and ordered by Anatoli Maluta.

Lane Smith, manager of Fairchild's export administration, said in the letter to Commerce that Maluta and Consolidated Protection were very secretive about their activities. Smith went on to say:

> We have sold several Xincom Memory Test Systems to CPCD in the past, but due to very tight security requirements at their manufacturing plants they have not purchased installation or maintenance contracts.
>
> They have supplied us with the proper certifications corresponding to U. S. export regulations (DIB 629 and Purchase Order) but, again, because of very strict security, they refuse to allow Fairchild representatives to physically audit the equipment.

Smith said, however, that two Fairchild executives had met at length with Maluta and concluded that he was not violating export laws. Smith explained:

> I present this information to you in hope that we might rapidly reach a decision as to whether we can conduct business as with a normal domestic customer.
>
> I would appreciate a call if you have any information that would prevent us from shipping our test system to this customer.

A January 15, 1980 letter from Paul Andre Deschenes, senior sales manager of Fairchild in El Segundo, to Richard Noren and Jack Barnes of the Fairchild Test Systems Group in San Jose revealed the extent of the background data Fairchild had obtained on Maluta and his company.

Deschenes said that on the basis of the inquiry and his interview with Maluta he felt Fairchild could no longer justify holding up delivery of the Xincom memory system. He said he had come to this conclusion because of Maluta's assurances that his company was a manufacturer of "perimeter protection systems" used by the air forces of nations comprising the free world and by atomic energy plants and by high technology equipment factories. Deschenes said:

> This suggests that because of its purpose, the Protection System must have a security of at least one order of magnitude greater than that of the installation it is designed to protect.

Deschenes then went on to give the results of his inquiry into Anatoli Maluta's background and character; both, he said, were good. He explained:

> Mr. Tony Maluta is a naturalized United States citizen, who has served with the United States Air Force in Berlin, Frankfurt, Munich and Edwards Air Force Base. He held a top secret clearance file in the military. His military obligation completed, he accepted a position with National Cash Register.

> ...With the unsolicited approval of Mr. Maluta, an investigation was requested through the office of Defense Intelligence in Washington and the Federal Bureau of Investigation in Washington and Los Angeles. I personally met with both agencies to insure the accurate transmittal of information. Upon completion, both agencies reported that from their investigation and information available in their files, they see no reason why Fairchild Test Systems Group should refuse to sell Xincom Systems to Consolidated Protection Development Corporation.

Paul Andre Deschenes added:

> In summary, gentlemen, it appears as though the decision to hold shipment was proper under the then existing circumstances, but with the lack of concrete evidence as pointed out in action 2) (the DIA and FBI checks), it is no longer justifiable. It is my recommendation that a prompt rescheduling of system deliveries to Consolidated Protection Development Corporation is in order.

As further demonstration of his law-abiding intentions, Fairchild officials pointed out, Maluta had been asked to give certification attesting to the fact that he would make end-use application of the Xincom system in accordance with federal laws and regulations. Maluta accommodated Fairchild, asserting in a signed Commerce Department form:

> This is to certify that all the equipment purchased from FTSG (Fairchild Test Systems Group) if ever is resold will be in compliance with all the rules and regulations of the United States Department of Commerce.

Deschenes attached a copy of the certification to his letter to Noren and Barnes.

Watkins-Johnson Told Commerce About CTC In February 1980

In a letter dated February 19, 1980, Phillip Gohr, security manager of the Watkins-Johnson Company of Palo Alto, California, asked the Commerce Department about the Continental Technology Corporation of Torrance. Pointing out that Watkins-Johnson had been doing business with Continental for several yers, Gohr wrote:

> Since they have changed names frequently, we are concerned that there may be a reason. Could you please check on their current name and past identities and advise me by telephone.

Gohr attached to his letter a list of names the firm had used on different dates — January 16, 1975, California Technology Company; September 3, 1975, California Technology Corporation; September 16, 1975, CTC California Technology Corporation; January 20, 1976, California Technology Corporation; December 11,

1978, Consolidated Protection Development; and January 29, 1980, Continental Technology Corporation.

Gohr also quoted from a Dunn & Bradstreet report on January 18, 1980, which, he said, described the Anatoli Maluta firm as being a manufacturer of surveillance equipment for area protection for the Air Force, Army and the Atomic Energy Commission and that the enterprise had sales in the U. S., Europe and Japan.

Commerce Interviewed Gohr In March 1980

Robert Rice, a Special Agent in the Compliance Division of the Commerce Department, interviewed Phillip Gohr on March 3, 1980. Gohr said a Dunn & Bradstreet report of January 18, 1980 raised questions about the end-use of the products Anatoli Maluta bought from Watkins-Johnson. In addition, Gohr said, the firm's many name changes, its undercapitalization, unusual credit arrangements and the highly sophisticated nature of the products it bought raised more questions.

Gohr told Agent Rice that Consolidated Protection Development Corporation -- the name the Malua company was using at the moment -- then had four pending orders with Watkins-Johnson totalling $983,663. The largest order was for a Model WJ 1240 microwave receiving and antenna system valued at about $700,000. Gohr said that the system would be used mainly for communication surveillance.

Gohr said another order was for a Model WJ 940 microwave receiving system valued at $258,000. Gohr said that Anatoli Maluta had indicated that the Model WJ 940 was to be used in an intrusion detection system in Arizona at Fort Huachuca, site of the U. S. Army's Communication Command and an Army intelligence school. Gohr said he doubted that Fort Huachuca needed such a complex system as the Model WJ 940 microwave receiving system. Gohr feared the system might be destined for diversion to a foreign nation.

Commerce Began CTC Inquiry In March 1980

Rice called Fort Huachuca on March 13, 1980 and spoke to John Templeton, assistant chief of staff for intelligence and security in the Army Communications Command. Templeton checked Fort Huachuca records and those

of the nearby U. S. Immigration and Naturalization Service facility, and found that neither Maluta nor his firm had any previous or current contracts for goods or services.

Maluta Ordered Eight Fairchild/Xincom

On March 4, 1980, Special Agent Robert Rice of Commerce interviewed R. Lane Smith of Fairchild in the firm's office in San Jose. Smith said that in August of 1979 Consolidated Protection Development Corporation ordered eight Fairchild/Xincom systems valued at more than $1.3 million. Smith said Maluta had claimed that the machinery was for Maluta's own use in Arizona or in the San Fernando Valley in Los Angeles.

Smith told Rice that Fairchild's records revealed that between 1977 and December 1979 Consolidated Protection Development Corporation, and its predecessor firm, CTC California Technology Corporation, had purchased seven Xincom systems and other semi-conductor testing instruments and accessories, all of which were subject to export control restrictions for national security reasons.

Smith said Anatoli Maluta would not allow Fairchild's salesmen on the company's premises for installation or repair of equipment. Smith said that because he suspected Maluta of exporting the equipment to prohibited destinations he asked Maluta for written certification that, in the event of resale, no laws or regulations would be violated. Sabina Dorn Tittel, Maluta's associate in the CTC organization, signed some of the certification documents. One such declaration was signed by Tittel on December 21, 1978 in a letter to Roy L. Jones, a Fairchild representative in the company's office at 888 North Sepulveda Boulevard in El Segundo. The letter said:

> Dear Roy:
>
> This is to certify that all the equipment purchased from FTSG if ever it is resold will be in compliance with all rules and regulations of the United States Commerce Department.

Tittel signed the letter as "Purchasing Manager" of Consolidated Protection.

Fairchild's Lane Smith told Agent Rice that he asked for the certifications from Maluta and Tittel to release Fairchild from the responsibility of obtaining export licenses if the machinery was resold for foreign use; and to serve the purpose of advising Maluta and his colleagues that the products could not be shipped overseas without export licenses.

Wu Brought Customs Service Into Case

It was at this approximate stage in the investigation that Commerce Special Agent Robert Rice went to the Office of the U. S. Attorney in Los Angeles where he reported on the progress of the Bruchhausen case to Assistant U. S. Attorney Theodore W. Wu, a federal prosecutor who was experienced in technology transfer investigations. At the moment Rice reported on what he knew of the Bruchhausen inquiry, Wu, in fact, was in the process of putting together the government's successful prosecution of Walter Spawr and his Spawr Optical Research Company of Corona, California for having sold high energy laser optics to the Soviet Union.

Rice, who also was involved in the Spawr inquiry, briefed Wu on the CTC network. Wu was of the opinion that the inquiry was potentially too big for Rice to handle alone. When it became apparent that insufficient additional resources could be dedicated to the CTC case by the Commerce Department, Wu and Kenneth Ingleby, Special Agent in Charge of the Customs Investigations Office at Terminal Island, California, worked out an arrangement allowing Customs Service personnel to take part in the investigation. Customs Special Agents assigned to the CTC case at various times and for various lengths of time included Stephen Dodge, Robert Olson, Kelly Wilson, Shelley Altenstadter, Leighton Duffus, James Stanley, Cliff Wilson, James Lindsey, Donald Buynack, Richard Kellogg, Cornelius Lauridsen, Frank Orrantia, Michael Peel, Thomas King, Roger Urbanski, and others. Robert Rice remained on the case and another Commerce agent, Frank Deliberti, assisted on the inquiry for one week.

Maluta Cancelled Fairchild/Xincom Order

Kelly Wilson, a U. S. Customs agent, and Robert Rice interviewed Anatoli Maluta on March 7, 1980. In discussing the orders he had placed with Fairchild, Maluta said the delays had gone on too long. Maluta said he had cancelled the orders.

Seized Documents Revealed CTC Plans

Documents seized in May of 1980 by U. S. Customs and German Customs agents revealed that the Xincom machinery was to have been shipped to the Soviet

Union. The documents were seized by Customs in court-authorized searches of businesses of the CTC group in the U. S. and West Germany in May, June and October of 1980.

A telex from Maluta to CTC executives in Dusseldorf dated January 10, 1980 said:

> ....In the morning, FSC Xincom salesman will bring a special form for me to sign. Do not know what is on that form. After that, sales manager and division manager will decide if I get more Xincoms. Estimate 10 days for final answer.

Items listed on a three page, August 9, 1979 "Quotation" seized in the offices of CTC's Techma Technische Maschinenhandels - Gesellschaft in Dusseldorf on May 16, 1980 included reference to a Fairchild/Xincom 5581 memory test system. Under the category of "prices," the document stated: "To be understood CIF Moscow."

Also seized in the raid on Techma was a three page contract of August 9, 1979 between Techma and an entity known as Vsesojuznoje Objedinenije Electroniorgtechnia of 32/34 Smolenskaja Square, Moscow. The contract stiputlated the terms for the sale of a Fairchild/Xincom 5581 memory test system. Sale price was put at $1.5 million and, the contract said, "The prices are understood c.i.f. Moscow." The contract said payment for the goods would be made through the Bank for Foreign Trade of the USSR.

In the raid on Techma, also seized was an August 9, 1979 telex from CTC employees in Dusseldorf to Anatoli Maluta in which four more Fairchild/Xincom memory test systems were ordered.

Another wire seized from Techma — this one dated August 15, 1979 — was from Hans-Jurgen Koenig to a "Mr. Kedrov" of Electronorgtehnika for additional orders of Fairchild/Xincom memory test systems.

In the raid on Techma, a four-page "order acknowledgement" of September 15, 1979 was seized. The document, sent by Techma to Elektronorgtehnika in Moscow, spelled out the compoments that had been sold that constituted the Fairchild/Xincom 5581 memory system.

Maluta Wanted Two HiPox Systems

Agent Rice of the Commerce Department interviewed Robert Chamberlain, director of international marketing operations for Applied Materials,

Inc., of Sunnyvale, California, on March 3, 1980. Chamberlain said Applied Materials was sales representative for Gasonics, Inc., of Mountain View, California. Gasonics manufactured sophisticated "HiPox" high pressure oxidation systems used in semiconductor manufacturing.

Chamberlain said that in February of 1980, Anatoli Maluta, using Continental Technology Corporation purchase orders, tried to buy two HiPox systems with a total value of about $261,000. Chamberlain was suspicious because Maluta refused to provide any information regarding the end-use of the machinery or its intended destination. The purchase orders were dated February 6, 1980. Because he believed Maluta intended to ship the HiPox equipment abroad in violation of federal law, Chamberlain decided to add as a condition of sale an executed end user's certificate.

Accordingly, Brad Beaty, product manager in the marketing division of Applied Materials, wrote to Maluta on February 13, 1980 to request an end-user's certificate. Beaty noted that "the ultimate consignee must be the person who is actually to receive the material for use. A bank, freight forwarder, forwarding agent, or other intermediary is not acceptable as an alternate consignee."

Beaty also requested a copy of the export license for the HiPox systems. He pointed out that the ordered equipment would not be sent to Maluta until the requested certificates were received.

Maluta sent a memorandum dated February 25, 1980 to Monte Toole, president of Gasonics, in which Maluta asserted that the end-user of the HiPox systems would be CTC Continental Technology Corporation of Torrance. Maluta also stipulated that the equipment would not be exported but would be used in manufacturing processes in the United States. Maluta signed as "vice president" of CTC.

On January 9, 1980, in a telex to his CTC superior in Dusseldorf, Maluta said he had had a "long meeting" with a representative of Gasonics and that the man was "very interested" in where the HiPox systems would be used. He added, "May even have a Perkin Elmer problem here. Get plenty for this."

In the same telex, Maluta made reference to "Uli," a nickname for Dietmar Ulrichshofer, who owned electronics distributing businesses in Vienna, Austria and Bad Reichenhall, West Germany, and purchased electronic equipment from the CTC group for sale to the Soviets, the Soviet Bloc and other nations.

On March 3, 1980, Agent Rice interviewed Monte Toole, president of Gasonics. Toole said Maluta refused to give him any information about the destination of the two HiPox systems or their intended end-use. Maluta would only sayd that the systems were to be used in a top security installation at Fort Huachuca, Arizona.

Hans Witten Was CTC Frieght Forwarder

On March 6, 1980, Agent Rice interviewed Hans Witten, vice president of Kamino International Transport, Inc., an international air freight forwarder located at 613 South Hindry Avenue in Inglewood, California. Witten said he had known Maluta and Tittel since 1978 and that Kamino International had served as freight forwarder for Maluta's multi-named businesses on many occasions.

Witten had documents in connection with 19 international shipments Maluta had instigated from November of 1979 to February of 1980. Maluta purchased the shipped goods in the United States through Continental Technology Corporation and Consolidated Protection Development Corporation and exported under the names of Universal Digital Corporation and Atlantic Universal Supply, Inc. Of the 19 shipments, 16 were exported to West Germany and three to India. None of the shipments to West Germany were made with a validated export license. All shipments to India were made with validated export license issued by the United States.

Commerce Asked Customs For Help In CTC Case

On March 20, 1980, Sharon Connelly, Director of the Compliance Division of the Office of Export Administration in the Department of Commerce, asked the U. S. Customs Service for help in the CTC investigation. Surveillance needed to be performed on a CTC entity and its employees and a search warrant might have to be served. Commerce Department investigators did not have the resources or authority to utilize these law enforcement tools.

In her letter to Kenneth Ingleby, Special Agent in Charge of Customs investigations office at Terminal Island, California, Connelly said:

> During the week of March 24, it is anticipated that Special Agents Frank Deliberti and Robert Rice of my staff will be in Los Angeles on an investigation of potential violations of

the Export Administration Act by Consolidated Protection Development Corporation, 21515 Hawthorne Boulevard, Torrance, California. Agents Deliberti and Rice will be conducting a surveillance of a freight shipment expected to be exported from Los Angeles to an unknown destination in the latter part of that week. We expect that the surveillance will culminate in a seizure of the equipment, and various interviews, with the possibility of the service of a search warrant on the subject firm.

It is possible that assistance from your office will be required, at lest insofar as the anticipated seizure of the equipment is concerned. Due to the tentative nature of the expected events, we are unable at this time to request assistance for a specific date, but it is anticipated that March 26 and 27 are the dates that assistance will most likely be requested, if required.

Thank you for your cooperation in this matter. I will have Agents Deliberti and Rice contact you as soon as they arrive in Los Angeles.

Cal Comp Shipment Was Stored Wtih HiPox

On March 23, 1980, Rice and Customs Agent Stephen Dodge interviewed Hans Witten. Witten said the Gasonics HiPox system cosigned to Continental Technology Corporation in care of Kamino International had been delivered earlier in the day. Witten said he was storing another shipment belonging to Maluta. The second shipment was from California Computer Products of Anaheim, California, an enterprise referred to as CalComp. Witten said he was holding both shipments pending the arrival of shipping instructions from Maluta and Sabina Tittel.

Gasonics Delivered CTC Two More HiPox

On March 25, 1980, Rice again interviewed Monte Toole of Gasonics in the firm's offices in Mountain View. Toole said that on that very day Maluta had accepted delivery of the two HiPox systems. Toole said Maluta told him that Maluta's plant in the San Fernando Valley had recently suffered fire damage and he was unable to use the HiPox systems in that facility. However, Maluta said he would take possession of the systems and store them at Kamino International in Inglewood or use them at a facility he maintained in Arizona.

Agents Inspected CalComp, HiPox Shipments

On April 1, 1980, Agents Dodge and Rice returned to Inglewood and met again with Hans Witten, who showed them the HiPox and CalComp shipments.

Witten explained that earlier in the day he had called Sabina Tittel and asked her if the CalComp shipment required an export license. Tittel had replied that she did not know, but that she would find out from Maluta.

Fort Huachuca Was Termed CalComp Destination

On April 2, 1980, Agent Rice interviewed Richard Kempster, a CalComp sales representative. Kempster said that on January 21, 1980, Anatoli Maluta had placed an order for a $90,360 CalComp Model 7000 high performance computerized drafting system. Kempster said Maluta told him that Continental Technology Corporation intended to use the system to design semiconductor devices used in electronic security systems manufactured by Kamino, Inc., of Inglewood, and that the system would later be sent to Fort Huachuca, Arizona.

True Destination Of CalComp Was Germany

On April 2, 1980, Witten informed Customs Agent Stephen Dodge that the CalComp shipment was to be forwarded to Techma Technische Maschinenhandels - Gesselschaft, GmbH, Dusseldorf, West Germany. Witten said the shipper's letter of instruction, invoices and U. S. Shipper's Export Declarations (SED's) submitted to Kamino by Continental Technology Corporation described the CalComp systems as "meters" valued at $14,035.64. The documentation indicated that the exporter was Universal Digital Corporation of 4804 Macafee Road in Torrance. The SED's were signed by "S. Dorn," Dorn being Sabina Tittel's maiden name.

W-J Receiver Reportedly Was Shipped To Germany

Rice interviewed R. G. Orman on April 7, 1980. Orman, district sales manager for the Watkins-Johnson Company in El Segundo, said he had known Anatoli Maluta for about five years and had conducted a substantial amount of business with him. Orman said Maluta had once told him that one of the Watkins-Johnson radio receiver systems he had bought had been shipped to his contact in West Germany.

Orman showed Rice two Watkins-Johnson internal reports in which Maluta was quoted as having said that a recent order from his firm would be assembled in Arizona and then shipped to an unidentified facility in Alaska.

HiPox Systems Reportedly For Car Bumpers

On April 11, 1980, Witten told Agent Rice that he had spoken to Anatoli Maluta. Witten advised Maluta that the CalComp and HiPox shipments required export licenses. Maluta indicated he would obtain export licenses for them. Maluta also said the HiPox systems were to be used for tasks such as the metal plating of car bumpers.

Documents Show CTC Undervalued Shipments

On April 24, 1980, Hans Witten turned over to Customs Agent Dodge shipping documents which Continental Technology Corporation had submitted in connection with the CalComp and HiPox systems.

Regarding the CalComp Model 7000, there were two shipper's letters of instruction. They revealed that the exporter was Universal Digital Corporation of 1843 Lincoln Boulevard, suite 202, Santa Monica. The agent was Kamino International. The ultimate consignee was Techma GmbH of Dusseldorf. The freight forwarder was Universal Transport of Dusseldorf. The country of ultimate destination was West Germany. The CalComp machinery was described as being typesetting parts and tables. Signator for Universal Digital was "T. Metz," an alias used by Maluta. Declared customs value was listed as a total of $4,091.16.

The two invoices for the CalComp shipment gave Universal Digital's address as 4804 Macafee Road, Torrance. They indicated that the destination was Techma GmbH of Dusseldorf, that the total value of the shipment was $4,090.64 and were signed by "T. Metz" and "M. Maynard" and initialed "ST." Marcia Maynard was a clerical employee who worked for Maluta. ST stood for Sabina Tittel.

The shipper's letters of instruction were carbon copies of shipper's export declarations (SED's), certification required of all exports. Searches were made at Customs Services files at the John F. Kennedy International Airport in New York in March of 1980 -- the site and time the CalComp shipments left the U. S. -- and no copies of the SED's were found.

Customs Service estimates concerning the CalComp shipments were that the exporter -- Universal Digital Corporation, also known as Continental Technology Corporation -- had underestimated the total value by more than $86,000.

Regarding the HiPox shipment, the two shipper's export declarations indicated Universal Digital of Santa Monica was the exporter, Kamino International of Inglewood the agent and the ultimate destination was Dietmar Ulrichshofer's electronics business in Bad Reichenhall, West Germany. The products were described as furnaces with a declared total customs value of $3,445. The HiPox invoices listed the exporter as Universal Digital of Torrance and gave a customs value of $3,444.85. The SED's were signed by "M. Maynard" and initialed by "ST." The shipments were undervalued in the amount of $259,129.81.

CalComp System Shipped To Dusseldorf

On May 1, 1980, the CalComp shipment was forwarded from Los Angeles to the JFK International Airport in New York on American Airlines flight No. 842. In New York, the shipment was transferred to Lufthansa flight No. 461 scheduled to depart for Dusseldorf on May 4. The CalComp shipment was allowed to be exported, although German and U. S. Customs authorities tracked it. On May 7, German Customs Agent Ulrich Schulz, working with U. S. Customs Agent Roger Urbanski, identified the CalComp shipment as being in the Dusseldorf airport marked for forwarding to Zurich by Universal Transport, a freight forwarder based in Dusseldorf. A new consignee, Panalpina A. G., had been stipulated on the shipping documents. Panalpina is a freight forwarder with offices at the Zurich airport.

Sand Substituted For HiPox Systems

Meanwhile, in the U. S., the HiPox shipment was delivered to the Los Angeles International Airport on May 5. Shipping instructions called for the cargo to be loaded aboard a Lufthansa flight for Munich. However, Customs authorities, working with Assistant United States Attorney Theodore W. Wu, and with Commerce Department Agent Rice, established that the shipment was in violation of the Export Administration Act. Wu, after advising the Department of Commerce's Compliance Division of his operational intent, directed U. S. Customs to seize the HiPox machinery and substitute two similar looking crates that contained sand.

The cost of air freight and substituting the sand shipment was estimated to be about $10,000. Officials of the Compliance Division of the Commerce Department in Washington opposed the shipment substitution concept and refused to put up the money. Ingleby and Wu arrived at a solution in which the Customs Service paid for the sand substitution, the cost of which eventually amounted to considerably less than the original estimate.

Fake HiPox Shipment Scheduled For Moscow

The fake HiPox shipment was flown to Munich. On May 23, it was shipped by truck to Vienna under authority of a freight forwarder named Spediton Poseidon. Roger Urbanski, a U. S. Customs agent assigned to the American embassy in Bonn, went to Vienna where Austrian Customs officials told him that Poseidon had booked passage for the HiPox systems aboard a KLM Royal Dutch Airline, flight No. 940, from Vienna to Amsterdam. In Amsterdam, the cargo was to be transferred to Aeroflot flight No. 702 for Moscow, departing on July 7. In scheduling these flights, Poseidon was representing Electronic Elektrotechnische Bauelemente GmbH of Vienna, a firm owned and managed by Dietmar Ulrichshofer. Scheduled to receive the shipment in Russia was an entity known as Mashpriborintorg of Moscow, a Soviet state purchasing agency.

Dietmar Ulrichshofer Discovered Crates of Sand

On the evening of June 3, Dietmar Ulrichshofer went to the Vienna storage area where the cargo was being held prior to its shipment to Amsterdam and then Moscow. Unaware that the two crates contained not HiPox systems but sand, Ulrichshofer opened one of them to insert an operating manual which had been forwarded to him earlier. He discovered that the shipment had been substituted. At 1:10 AM on June 4, Ulrichshofer cancelled the shipment to Amsterdam.

German Customs Seized CalComp Shipment

German Customs agents seized the CalComp shipment on May 16, 1980 as it was stored in a staging area at the airport in Dusseldorf. A court-authorized

search of Techma offices in Dusseldorf revealed documentation proving that the cargo was destined for Moscow where Elektronorgtehnika was to have received delivery.

Information Showed Ties to Ulrichshofer

In late May of 1981, U. S. Customs Agent Roger Urbanski developed information indicating that Dietmar Ulrichshofer, through his Vienna firm, Electronic Elektrotechnische Bauelemente GmbH, had ordered the HiPox systems from a CTC entity in Dusseldorf.

In early June of 1981, Ulrich Schulz of German Customs, U. S. Customs Agents Stephen Dodge and Roger Urbanski and Commerce Agent Robert Rice developed information indicating that Ulrichshofer's firm in Bad Reichenhall was a purchasing agent for Electronic of Vienna, which represented various firms in the Soviet Union and the Warsaw Pact nations. Ulrichshofer reportedly bought electrical equipment from the CTC syndicate and CTC reportedly was able to supply equipment which was very difficult to obtain from anyone else.

Ulrichshofer reportedly sold and delivered Watkins-Johnson microwave receiving systems and associated parts and accessories to the Yugoslavian Defense Ministry. CTC California Technology Corporation purchase orders revealed that Watkins-Johnson 940 series equipment was exported from the U. S. consigned to Dietmar Ulrichshofer in November of 1977, February of 1978 and February, April and October of 1979. All the shipments were in violation of the Arms Export Control Act.

Ulrichshofer reportedly sold and delivered three Fairchild/Xincom 5581 memory test systems to the firm Tungsram of Budapest, Hungary. CTC purchase orders revealed that Fairchild/Xincom 5581 memory test systems were shipped to Ulrichshofer by California Technology Corporation in May of 1978 and May and July of 1979.

Ulrichshofer reportedly received a Watkins-Johnson TN-600 WJ 940 tuner for the Watkins-Johnson 940 microwave receiving system from Mashpriborintorg in Moscow in late 1979. The equipment had broken down and the Russians wanted it repaired. Ulrichshofer reportedly turned the tuner over to Bruchhausen's ADT company in Dusseldorf. The tuner was shipped back to the U. S. for repair and was seized on October 22, 1980 by U. S. Customs agents at Computer Peripherals Industries in Chatsworth, a suburb of Los Angeles.

Sales To Dr. Guenther Forgber

German Customs Agent Ulrich Schulz and U. S. Customs Agent Roger Urbanski developed information on June 23, 1981 indicating that the Watkins-Johnson 940 microwave receiving systems had not been sold to the Yugoslav Defense Ministry but directly to Mashpinborintorg in Moscow. It was reported that only one of the Fairchild/Xincom memory test systems was sold to Tungsram of Hungary and three had been sold to Dr. Guenther Forgber of East Germany.

Schulz and Urbanski obtained documentation from Ulrichshofer's sales of American manufactured electronic equipment to Soviet and Soviet Bloc customers including the sale to Dr. Guenther Forgber of Narda microwave amplifiers and power dividers and a Fairchild automatic testing system and Xincom manuals; and to Mashpinborintorg of Moscow of Watkins-Johnson 940 microwave receiving systems, manuals and tuners.

Koenig Described Work In CTC Syndicate

On June 6 and 12, 1981, Hans-Juergen Koenig was interviewed in the U. S. Embassy in Bonn, West Germany by Stephen Dodge of the U. S. Customs Service, Robert Rice of Commerce and Theodore Wu, an Assistant U. S. Attorney in Los Angeles.

Koenig, reciting his recollections in fluent English, said that he first went to work for the CTC group of companies in June of 1977, serving as general manager of Analog and Digital Technik, or ADT, of Dusseldorf.

Koenig said ADT's sales were largely electrical components to West German firms but one department of the enterprise, managed by Sybille Ziogas, was devoted exclusively to the sale of electronic equipment to the Soviet Union. Ziogas worked in ADT from August of 1977 until late 1978 when she joined another CTC entity.

His tour at ADT lasted six months, Koenig said. While he was not trained in technical matters, Koenig did learn the technical side of the business and how the CTC enterprises operated. Koenig came to realize that ADT had two principal interests -- sales to West German firms, and sales to the Soviet Union.

CTC executives explained to Koenig that all sales by ADT to the Soviet Union were made through Electronorgtechnika, also known at Elorg, the Soviet

state purchasing agency for electrical components, test equipment for components and computers. Koenig said he learned while working for ADT that the CTC group bought most of the electrical components and computers for the Soviet Union from the United States. Koenig said CTC was managed by Tony Maluta, a Russian born American who spoke English, German and Russian and who had technical experience and knowledge of high technology equipment. Maluta was assisted by Sabina Dorn Tittel, a German woman whom Koenig met for the first time in Dusseldorf in 1977 shortly after he joined ADT.

It was the opinion of CTC executives in Germany that ADT's sales of American manufactured high technology to the Soviet Union did not violate German laws because the goods never formally entered West Germany but instead were only "in-transit" -- or passing through -- in route to Switzerland and then on to the U.S.S.R., Koenig said. They felt they were breaking no law when they shipped high technology freight through West Germany and on to the Soviet Union with no German export licenses.

But Koenig doubted this legal interpretation, pointing out that export licenses were required for freight shipped "in-transit" through West Germany and that it was apparant that West German authorities never knew about CTC's sales to the Soviets.

West German executives of CTC also held the legal opinion that Tony Maluta's shipments out of the U. S. did not require American export licenses because Maluta declared the shipments in a deceptive way, describing them in deliberately vague terms such as "electricals." Because their destination was West Germany, CTC's shipments were undetected.

However, Koenig said, CTC officials knew that if they had listed the Soviets as recipients of the goods, export licenses would have been refused. Koenig said Tony Maluta declared Fairchild/Xincom computer equipment as being "electricals" when he knew the machinery was more sophisticated than that. Because of Maluta's "deceptive methods," Koenig said, he believed that Maluta recognized the legal requirement for proper export licenses was being circumvented.

While he was learning ADT procedures, Koenig said, he had differences with management over how the firm should be run. The differences led to Koenig's quitting ADT. However, he remained on good terms with ADT. In fact, company officials put up 50,000 Deutschemarks of their own money to enable Koenig to

establish another enterprise, Elmasch, GmbH. The founding of Elmasch enabled Koenig to put into practice an idea he had of selling electrical and computer components to the Warsaw Pact nations. Koenig explained how and why Elmasch came into being:

> By early 1978, I was knowledgeable of ADT's methods of doing business with the Soviet Union. During this period, I discussed...my ideas about doing business with the other Eastern Bloc nations. As part of my attempts to establish business contacts with the Soviet Bloc customers after the establishment of Elmasch, I attended a trade fair in Hannover, West Germany, in April, 1978. At that time, I anticipated selling electrical components and semiconductors to my customers, but I learned that certain electric components were very easy for Soviet Bloc customers to obtain from West Germany and Austria. I determined that....the price for such components was relatively low and their sale to Eastern Europe was not profitable. In about June, 1978, I obtained from Bulgaria an inquiry for U. S. ball-bonding , die-bonding and etching equipment used in semiconductor manufacturing, and this inquiry became an official order in September, 1978. This inquiry was sent by me in Bulgaria to ADT then to Maluta at CTC.... Later on, less than a week after my return from Bulgaria, ...I talked with Tony (Maluta) about this inquiry by telephone from ADT's office, using a telephone loud speaker.

While Koenig was in the process of setting up Elmasch, GmbH, he established another business, Techma, GmbH, to take over ADT's transactions with the Soviet Union. ADT officials wanted to have no further sales to the Soviets. Koenig was listed as Techma's general manager but Sybille Ziogas, who had supervised ADT's Soviet sales, took on the same assignment with the new entity.

CTC executives held a party in April or May of 1978 near Dusseldorf which was attended by about 20 persons, including Maluta and Koenig. Koenig and Maluta were told to get to know each other and to be on good terms.

Koenig discussed an order he had received from Czechoslovakia for Intel 2708 integrated circuits and an Intel microcomputer develoment system model MDS231. Maluta's judgement was that Koenig was on the right track in planning to use Elmasch, GmbH, as a vehicle to supply Eastern Bloc orders. Maluta told Koenig to accept orders from Warsaw Pact nations and to transmit them directly to him at CTC in California. Maluta said there would be "no problem" with CTC delivering U. S. machinery to Elmasch.

Koenig said he frequently heard CTC officials talking long distance with Maluta. They talked about the availability of machinery and prices. It was obvious what they were talking about, Koenig said. CTC executives in Germany were afraid their telephones were monitored and were careful not to mention Soviet Bloc customers by name.

Koenig remembered one telephone conversation between one CTC executive and Maluta that he overheard on the loud speaker. The two men discussed a possible order from Bulgaria which Koenig knew about. But neither man referred to Bulgaria or the prospective buyer by name.

The circuitous nature of the telephone conversations did not prevent Maluta from knowing what was happening, Koenig said. Maluta knew that all the orders from Elmasch were from Eastern Bloc nations.

The Soviets' invasion of Afghanistan in late 1979 triggered new U. S. government assurances that the flow of high technology to the Soviet Bloc would be made more difficult. The grain embargo was imposed and, Koenig said, there were indications that illegal shippers like Maluta were likely to face stronger U. S. export controls.

To prepare for such an eventuality, the CTC group called a meeting with Koenig and Maluta for London in February of 1980. Maluta said a tightening of export controls might be attempted but that they would not succeed, Koenig recalled. Moreover, Maluta added that he had noted no increase in efforts by the U. S. government. In short, Maluta declared, there was no need to devise a new method for shipping high technology out of the U. S. because no new safeguards had been set up. But, Maluta did say that a Commerce Department agent had visited him, a recollection by Maluta which was doubted by both Koenig and other CTC representatives. They believed Maluta was exaggerating the "dangers involved in ordering U. S. goods" as a ploy to get the CTC syndicate to pay him more money, Koenig said.

Horst Jonas, a customer of CTC, was suspected by the West German national police (Bundes kriminal amt or BKA) of having illegal dealings with the Soviet Bloc. The BKA interviewed CTC executives about Jonas. The encounter troubled them to such an extent that they moved ADT to new quarters in Dusseldorf in 1977 and then moved the company offices to Munich in 1979, Koenig said. Jonas was arrested and imprisoned for 18 months by German authorities for alleged espionage activities.

Referring to his contention that Tony Maluta was well aware of the activities of the West German businesses in the CTC syndicate, Koenig recalled a conversation he had during the London meeting with Maluta. He told Maluta that Bulgaria was Elmasch's biggest customer. To conceal the true destination of the Bulgarian shipments, Elmasch gave them the order code of 7200. Maluta knew all

7200 codes were for Bulgarian customers, Koenig said. Similarly, Maluta also knew that Techma, GmbH, was selling to the Soviet Union, Koenig said. He added:

> I am of the opinion that Maluta knew all orders from Elmasch and Techma were for Eastern European and Soviet customers, except for a very small portion of Techma orders for Zabel, a West German firm. My opinion is based on the fact that I told Maluta in May 1978 that Elmasch was set up specifically to do business with Eastern Europe other than the U.S.S.R., and Maluta had to know Techma was selling primarily to the U.S.S.R. because it followed ADT in the Soviet business, and simply was a change of name for business with the Soviet Union already being conducted by ADT.

Early in 1980 CTC executives began to suspect that Maluta and his assistant, Sabina Dorn Tittel, were cheating them, charging them exorbitant prices for U. S. equipment.

On a Monday morning in May, Werner J. Bruchhausen and Koenig made an unexpected visit on CTC in Los Angeles. Their arrival caused tension between Bruchhausen and Maluta. Later that day the two men quarreled. When Maluta left the offices, Bruchhausen and Koenig searched the files and found evidence that Maluta was overcharging his employer 10 to 20 percent. Bruchhausen fired Maluta and Sabina Tittel.

Maluta's pay, Koenig said, had been $2,000 to $3,000 a month but he was given another $25,000 a month by charging the CTC entities through a fictitious advertising account which CTC executives had agreed to. The CTC executives set aside another $150,000 to be used by Maluta should he be arrested and face big legal fees. Suspicions that Maluta was stealing from CTC were well founded and Koenig estimated that Maluta embezzled about $800,000 from CTC entities.

Koenig recalled his first meeting with Sabina Dorn Tittel, saying he met her in August of 1977 while she was on vacation in Dusseldorf. He said Tittel may not have known about ADT's Soviet sales at the time but that it was his "common sense assumption that Maluta must have told her at some time."

Koenig Listed Communist Customers

In his interview with U. S. government authorities, Koenig gave detailed information about the sales and deliveries of equipment to Soviet, Soviet Bloc and Communist Chinese customers. The customers included:

-- China National Foreign Transportation Co. of Mainland China.

— Electronic-Export Import; and Veb Carl Zeiss Jena (Import Kontor Viw) of East Germany.

- Unitra Foreign Trade Enterprise; and Metronex of Poland.
- Kovo Aubenhandelsunt-Ernehmen of Yugoslavia.
- Tungsram of Hungary.
- Isotimpex; and Inco, Industrial-Ernehmen of Bulgaria.
- Technoimportexport, of Romania.

Ilona Seibert Recalled Maluta's Employ

Ilona Seibert, who worked for Maluta from June of 1978 to February of 1979, told Customs Agent Shelley Altenstadter and Commerce Agent Robert Rice that CTC bought equipment under the name of California Technology Corporation and exported it through the company known as Interorga. Later, she said, purchases were made through Consolidated Protection Corporation and Atlantic Universal Supply, Inc. did the exporting.

The use of different enterprises to buy and export was a ruse to enable the CTC companies to prevent vendors from readily figuring out the fact that their goods were being shipped abroad, Seibert said. She also noted that duplicate or double invoices were prepared by CTC entities but she never asked why.

Marsha Maynard Kept Books For CTC

Similar information was provided to Customs Agents Stephen Dodge and Shelley Altenstadter by Marsha Maynard, a CTC secretary. Maynard, who had jointed the CTC entities in July of 1979, did clerical work and kept the books for Continental Technology Corporation and Universal Digital Corporation.

Maynard, recalling that the CTC entities kept three sets of books, said equipment was bought by Consolidated Protection Development Corporation and Continental Technology Corporation and was exported by Atlantic Universal Supply, Inc. and Universal Digital Corporation.

It was explained to her by Sabina Tittel that the CTC group of firms used differently named firms to buy and export to prevent vendors from realizing that the products they sold Maluta were being shipped overseas, Maynard said. Maluta and Tittel both told Maynard that if any vendor asked where the equipment was to be used, she was to say it would be shipped to a facility in Arizona. Maluta and Tittel both admitted to her that the Arizona plant did not exist, Maynard said,

adding that her instructions also included hiding all documents referring to Universal Digital whenever a vendor visited the CTC office.

Two sets of invoices were maintained, Maynard said, explaining that one set gave accurate dollar values and product descriptions and the second set carried false data.

Scott McKay Was CTC Shipping Clerk

Scott McKay, a shipping clerk at CTC from October of 1978 to October of 1979, told Customs Agent Altenstadter that he prepared duplicate commerical invoices, one listing the actual value and description of the shipped commodities and the second stating false values. McKay said one invoice was mailed to the CTC group in Dusseldorf, the other accompanied the exported item on its journey, but he could not remember which went where.

Sharon Engelman Was CTC Receptionist

Sharon Engelman was a receptionist at CTC from February through July of 1979. She told Customs Agents Altenstadter and Duffus that about once a week CTC offices in Dusseldorf sent by wire transfer about $100,000 to the CTC entities in California.

U. S. Customs Searches CTC Quarters

Shortly after Anatoli Maluta and Sabina Dorn Tittel were fired in early May of 1980, the investigation into the activities of the CTC entities heated up. The U. S. Customs Service, acting upon court-authorized warrants, on May 19, 1980 searched the premises at:

--Continental Technology Corporation, Suite 100, 23868 Hawthorne Boulevard, Torrance.

--Sabina Tittel's residence at 30605 Cartier Drive, Rancho Palos Verdes.

--Universal Digital Corporation, Suite 202, 1843 Lincoln Boulevard, Santa Monica.

--Continental Technology Corporation, Suite 646, 21515 Hawthorne Boulevard, Torrance.

--Sabina Tittel's former residence at 4804 Macafee Road, Torrance.

--Werner J. Bruchhausen's safe deposit box in the Bank of America branch at 21615 Hawthorne Boulevard, Torrance.

On May 20, a court-authorized search was conducted by U. S. Customs agents on a safe deposit box assigned to Consolidated Protection Development Corporation in a Torrance Bank of America branch.

On May 30, U. S. Customs agents made a court-authorized search of Sabina Tittel's home at 30605 Cartier Drive in Rancho Palos Verdes.

The final court-authorized search in California occurred on October 2, 1980 when Customs agents seized documents from the Computer Peripherals Industries, 10836 Bothwell Road, Chatsworth.

German Customs Made Additional Searches

Beginning on May 16, 1980 and continuing through October 8, 1980, German Customs agents, using court-authorized warrants, searched the premises of Techma, GmbH of Dusseldorf, West Germany; Elmasch GmbH of Bonn; the residence of Hans-Juergen Koenig in Bonn; ADT Analog and Digital Technik, Neiderseeon; the resiuence of ADT accountant Ursula Tinte in Dortmund; Ing. Ulrichshofer, GmbH, Bad Reichenhall; Dema Computertechnik, GmbH, Munich; and the residence of Frank and Karin Nassauer in Bad Homburg.

Detlef Lackmann Represented CTC

Customs Agent Stepten Dodge interviewed Darice Garrett, an employee of California Technology Corporation on June 3, 1980. Garrett said Detlef Lackmann, a CTC representative from Dusseldorf, had flown to the United States from Germany to begin disposing of equipment still held by the CTC group of companies.

Dodge and Commerce Agent Robert Rice located Lackmann on June 4 and interviewed him in his room at the Plush Horse Inn in Redondo Beach. They interviewed him again on June 6 in the U. S. Customs house at Terminal Island.

Lackmann, explaining that he was an officer of Elubat, GmbH, and an employee of ADT, said there was no doubt that the CTC companies sold products of U. S. origin to the Soviet Union and might also do the same for Bulgaria. He

said CTC had good contacts in the Soviet Union. He said he was paid $5,000 to make this trip to the U. S. and that its purpose was to sell or ship what remained of the CTC inventory.

Soviets Return Component For Repair

In July of 1977, California Technology Corporation placed a purchase order with the manufacturer for $66,000 in components for very sophisticated machinery with direct military application. All of the components ordered were Munitions List items and cannot be legally exported without approval from the U. S. Department of State. CTC received the equipment. In September 1977, under the company name of Interorga International Components and Sales Organization, CTC exported the shipment to West Germany.

Three years went by. One of the components had worn out and was in need of repair. It was sent to the manufacturer plant for maintenance.

On June 16 and 23, 1981, in West Germany, Stephen Dodge of Customs, Robert Rice of Commerce and Theodore W. Wu, Assistant U. S. Attorney in Los Angeles, developed information indicating that the machinery had been sold originally to Mashpriborintorg of Moscow. The information was that the Russians sent the disabled component back to ADT of Dusseldorf for repair.

A telex from CTC executives in Dusseldorf to Anatoli Maluta, dated February 27, 1980, was seized by U. S. Customs agents in the raid on CTC offices. The telex said the component would be returned to the U. S. for repair and that a "friend" would receive the repaired equipment and would then turn it over to Maluta.

Grand Jury Indicted Bruchhausen And Associates

On August 19, 1981, a federal grand jury in Los Angeles handed down a 60-count indictment against Werner J. Bruchhausen, Dietmar Ulrichshofer, Anatoli Maluta and Sabina Dorn Tittel in connection with charges that they conspired to export more than $8 million in controlled high technology products to the Soviet Union and Soviet Bloc countries. Maluta and Tittel were also charged with tax evasion. Hans-Juergen Koenig was named as an unindicted co-conspirator.

The indictment cited specific high technology systems and components which the group allegedly had exported from the U. S. illegally including:

--Watkins-Johnson Model MF 100/WJ 940 main frame microwave receiver system.

--Fairchild Systems Technology Xincom Parallel Operation Memory Test Systems, Model 5581.

--Data General Corporation Model Eclipse S/230 computer systems.

--Watkins-Johnson Company Model TN-600 microwave tuner.

--Fairchild Xincom Systems Model 5580 Basic Test System.

--Memorex Corporation Disk Drive System.

--Intel Corporation Single Board Computers.

--Intel Corporation and Motorola, Inc., microcircuits.

--Tamarack Scientific Company Model 142 Contact Printer.

--Intel Corporation Microcomputer Development Systems.

--Intel Corporation microcircuits.

--Analog Devices, Inc., microcircuits.

--Watkins-Johnson Company Model WJ 8640 Manpack Receiver with five tuning heads and battery chargers.

The indictment alleged that Bruchhausen, Ulrichshofer, Maluta and Dorn conspired to export various high technology commodities from the U. S. to West Germany and elsewhere without export licenses.

Maluta, Bruchhausen and Ulrichshofer were alleged to have exported electronic communications systems, computer components and other commodities with knowledge that they would be used for the benefit of the Soviet Union or Eastern Bloc countries.

As early as 1977, the indictment alleged, Maluta and Tittel received purchase orders for electronics commodities from Bruchhausen and Ulrichshofer and procured the commodities from U. S. manufacturers for shipment abroad.

Maluta and Tittel were accused of 13 counts of illegally exporting to West Germany. Maluta was charged in 23 other counts with exporting various commodities with knowledge they would benefit the Soviets.

Maluta and Tittel were accused of filing false Shipper's Export Declarations (SEDs) and other false documents submitted to the U. S. Customs Service. Maluta and Tittel were also charged in nine counts with various income tax violations involving hundreds of thousands of dollars.

In addition, Maluta was charged with perjury, having allegedly lied to the grand jury on June 7, 1980.

Bruchhausen and Ulrichshofer were both outside the United States when the indictment came down. Maluta and Tittel were apprehended by agents of the Internal Revenue Service in Palm Desert, California on August 19. Bail for each of them was set at $800,000. The IRS had joined the investigation in April 1981 at the request of Assistant U. S. Attorney Theodore Wu.

Maluta and Tittel were in a car when arrested and had three pistols in the back seat. They did not resist arrest, although one of them seemed to be reaching into the back seat just before they surrendered. Tittel's attorney told reporters that Tittel owned a condominium in Palm Desert and sometimes went shooting in the desert.

Disposition of Maluta and Tittel Cases

Anatoli Maluta was found guilty of conspiracy, filing export documents containing false statements, unlawful exportation of Munitions List items, exporting without a license, tax evasion, subscribing to a false tax return and exporting without a license to countries barred because of national security considerations. Sabina Dorn Tittel pled guilty to making false statements, exporting without a license, tax evasion and subscribing to a false tax return.

In his sentencing memorandum submitted to the court, Assistant U. S. Attorney Wu, who prosecuted the case, said the export offenses committed by Maluta and Tittel involved more than three years of "continuous and deliberately designed, and systematically executed criminal conduct of a serious nature."

Wu said Maluta and Tittel variously were guilty of exporting goods in violation of the Export Administration Act, the Commodity Control List of the Export Administration Regulations, the International Traffic in Arms Regulations and the Arms Export Control Act.

Wu went on to say:

> There is no doubt that both Maluta and Tittel at the time of the commission of the offenses knew exactly what they were doing was contrary to law, e.g., that the exports were knowingly effected without obtaining the necessary licenses; that the contents of the shipments were falsely described and undervalued, and that the defendants' income obtained from the illegal export operation were falsely stated to evade income tax.

Maluta was aware that certain of the goods they arranged to be exported would and did go to the Soviet Union, Wu said, adding that what motivated Maluta and Tittel was greed and that their desire for fortune was quickly satisfied. Maluta, for example, was able to buy in 1979 alone $185,000 in gold and silver coins. According to an affidavit given by Robert A. Lyon, an officer of Jonathon's Coin, Inc., of Inglewood, Maluta made 17 cash purchases of coins in the months of February, March, April, May, June and August during 1979 for a total of $190,358.66. His purchases, all of which were made in cash, included one for $79,974, another for $20,000 and a third for $19,987.

From 1978 through April of 1979, Tittel acquired a single family dwelling in Torrance, California for $92,000, with a down payment of $19,400; a condominium in Palm Desert for $125,995, with a down payment of $49,345; a single family residence in New Cuyama for $33,000, with a down payment of $15,700; a single family residence in Rancho Palos Verdes for $295,000, with a down payment of $198,400; and in 1979 a new Mercedes-Benz 450 SLC automobile for $41,595.56, for which she paid $10,500 in cash and $31,095.56 with a cashier's check.

Wu added:

> To the defendants, it was not enough to get rich quickly through the unlawful export operation; they were driven to do more -- evade income tax. That was greed upon greed. Also, it is clearly apparent that the defendants, especially Maluta, had to know that the high technology products exported by them illegally and the laws they breached implicated the national security interest of this country. The defendants purposefully ignored the risk of running afoul of the law and the risk of compromising controlled U.S.-origin technology to governments whose interests are inconsistent with those of the United States.

Considering the seriousness of their crimes, Wu said, it was his recommendation to the court that Maluta receive a prison term of six to eight years and a fine of at least $100,000.

As for Tittel, Wu said, she told the court that she entered into the illegal export scheme because she was in love with Maluta and, therefore, under his influence and control. But Wu did not believe her love for Maluta excused her conduct, as he explained:

> While she may well have been "in love" with Maluta and thus susceptible to his persuasion, the government contends that Tittel was more "in love" with the glowing prospect of a quick rise to affluence....

Acknowledging that Tittel's responsibility for the exporting conspiracy was somewhat less than was Maluta's, Wu's recommendation was that she receive a prison term of three to four years and a fine of $100,000; along with a five-year probation term to begin on her release from prison.

Maluta, who appealed his conviction on the grounds that he was the victim of selective prosecution by the government, is still involved in the appellate process at this time.

Tittel received a two-year prison sentence and was fined $25,000. She is incarcerated at the Federal Correctional Institute in Pleasanton, California. She has filed a motion to reduce sentence which the court has taken under consideration.

STAFF STATEMENT OF
GLENN W. FRY, INVESTIGATOR
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE

MAY 5, 1982

The Commerce Department's ineffective response to the challenge of technology transfer is an illustrative example of the failure of the Government, in general, to organize itself effectively to remedy this national security problem.

We have learned of the shortcomings in the Commerce Department's efforts to investigate violations of the Export Administration Act thereby causing a serious deficiency in its ability to enforce the statute and its regulations. The law enforcement effort, although critical, is only a part of the overall effort to prevent the harmful flow of U. S. technology. Even if the law enforcement operation were professionally administered with sufficient resources its effectiveness would continue to suffer due in part to deficiencies within other executive branch agencies.

The Commerce Department is mandated to administer and enforce the Export Administration Act; however, matters concerning this act which involve national security interests require the consultation of the Department of Defense and the Intelligence Community as well as Commerce. Ineffective control of the transfer of U. S. technology and the enforcement of export laws will prevail if the Department of Defense and the Intelligence Community continue to provide less than their best efforts to support this national security mission. Despite several previous Congressional investigations and hearings conducted on these matters, dating back to 1974, the responsible executive branch agencies continue to have difficulty in organizing an effective operation.

Technology transfer can occur through the illegal export of controlled or embargoed commodities; however, it can also occur, with equal damage, because of inadequate control and protection of critical information and through ineffective handling of legitimate export licensing cases. The Minority staff has made preliminary findings that the technology transfer programs of the Department of Defense and the Intelligence Community contain basic deficiencies which impair the Government's overall effort to control the flow of critical American technology.

The following are areas within the Defense Department's program that demand attention and ultimate resolution if the Government intends to control the flow of U. S. technology:

(1) The Freedom of Information Act is a legal tactic available to U. S. citizens, foreigners and even Soviet surrogates to obtain critical "dual use" technology. "Dual use" technology, which can be used commercially and militarily, is not excluded from FOIA requests. There is no protection or means to control the harmful transfer of technology that does not fall within the exclusions prescribed by the FOIA.

(2) There have been instances where classified information has been prematurely declassified in accordance with an automatic declassification schedule. In other instances, critical technologies which have military significance are never classified. In either case, the end result is that such information, although not readily distributed, becomes available to anyone. In effect, if the specifications of a grenade launcher were not classified then such information would be available to anyone. There is no effective system to accurately determine whether information should be classified, declassified or remain classified.

The Department of Defense's Offices of Research and Engineering and International Security Policy are responsible for the review of export licensing requests for national security interests. Presently, Defense reviews predominantly those export cases involving the Soviet Union or Warsaw Pact nations. There is very little review of "free world" license requests except for cases involving very advanced computer technology. The program presently administered within the Department of Defense suffers from several fundamental deficiencies.

(3) On August 26, 1977, the Secretary of Defense issued an "interim" policy statement for the export control of U. S. technology. Today in 1982, there has yet to be any follow-up to this "interim" policy. This is representative of the weak overall priority afforded the technology transfer issue throughout our Government. Sources within Defense have indicated that there is ambiguity regarding which DOD office has overall accountability for technology transfer decisions. There is apparent confusion as to who has overall accountability on the issue of transfer of technology between the offices of the Deputy Under Secretary of Defense for Research and Engineering and the Deputy Under Secretary of International Security Policy. Sources have stated that this confusion has caused

95-929 O - 82 - 28

unnecessary and costly delays in the resolution of export license reviews, resulting in the export of various technologies that are potentially not in the best interests of our national security. On May 19, 1979, the Deputy Secretary of Defense issued a directive delineating specific areas of responsibility within the Department of Defense. Defense Research and Engineering was designated as the responsible office for technological matters and processing and coordination of export requests. It was also designated to serve as the DOD focal point on all aspects of export technology, including COCOM, with the Department of State and other Federal agencies. International Security Affairs (later renamed International Security Policy) will be responsible for policy and political considerations. It stated that disagreements should be recorded and referred to the Deputy Secretary for resolution. Sources within Defense have explained that, to date, neither office has overall accountability. There are instances when DR&E makes final decisions and instances when ISP makes them; however, there is inadequate coordination or communication between the two offices.

(4) The Office of Defense Research and Engineering does not have an adequate number of permanent staff specialists to effectively conduct its technology transfer mission. Temporary personnel have been assigned to this office; however, there is an annual turnover. Consequently, much valuable time and resources are continually used to train and familiarize new personnel rather than attend to its primary responsibilities.

(5) Military and Department of Defense Research laboratories who are tasked by DR&E to review licensing cases lack a charter delineating export control or technology transfer responsibilities. There is also no specific funding for this type of operation. Consequently, technology transfer issues are not a priority and do not receive appropriate attention.

(6) There is no adequate data base of information available to all participants in the technology transfer program within our Government. This deficiency is analogous to prosecutors working without the benefit of a legal library. There has to be a centralized repository of information that maintains available data relevant to the decisions to grant exports.

Presently, there are data bases within various agencies; however, they have not been consolidated and there is little coordination between agencies on available information. Much of what is known about technology transfer lies solely on the reliance of corporate memory. In a sense, the present system lends itself to

the cliche that "the right hand doesn't know what the left hand is doing." One DOD research lab could review an export license case and raise no objection to its ultimate export. Another DOD lab might receive a similar case and deny the export based on information it independently had at its disposal. A mechanism is needed to consolidate all available data so that all participants are aware of relevant information.

(7) The Department of Defense does not review a sufficient number of "free world" export license cases. Exports to free world nations many times are improperly or illegally reexported or diverted to East Bloc nations. This has been demonstrated by recent export violations involving nations such as Switzerland and West Germany that were used as conduits for the illegal re-export of high technology commodities to the Soviet Union. The U. S. trades with many nations such as India and Pakistan who have open trade policies with the Soviet Union. To blindly export critical technologies to nations such as those without the benefit of the DOD's review could run the risk of having U. S. technologies end up in the U.S.S.R.

(8) Defense Research and Engineering has not devoted sufficient resources to the program which reviews foreign technical visitor programs. DR&E is responsible for determining militarily critical technology that requires export control. This effort is being done in concert with U. S. industry. In this light DR&E has devoted tremendous resources to the development and understanding of new dual use technologies; however, there is not an adequate operation within DR&E to assess what areas visitors are concerned with and what technology is obtained by these visitors. Therefore, due to this inadequate oversight, DR&E has little control over the potential loss of U. S. technology. Consequently, there is no way to assess what critical technologies have been obtained by our adversaries thereby making it virtually impossible for the Intelligence Community to determine how the loss impacts on our national security.

The effective control of critical dual use technology is largely dependent on the proper gathering, dissemination, analysis and use of intelligence. It is the view of the Minority staff that the Soviets, in many cases, are precise about what technology and equipment they want from the United States. It follows then, that if the U. S. can determine what the Soviets desire, where they are deficient, what they need and what direction their technological efforts are aimed, we are in an improved position to prevent them from obtaining our technology which may meet

their needs. At the very least the U. S. could create delays in the Soviets' efforts which will impede their progress and maintain our lead time in critical areas of technology. Testimony will be given which describes the Soviets as having an enormous, systematic and organized effort to obtain U. S. and other Western technology. The U. S., however, does not have a mechanism equal to the Soviets' task. There has been no overall coordinated, systematic and organized program in the U. S. to effectively prevent loss of our technology to the Soviets.

Intelligence is the key to anticipating the technology on the Soviets' "shopping list." U. S. law enforcement authorities can mount effective enforcement strategy directed towards illegal exports when they are apprised of what the Soviets are looking for. DOD and Commerce representatives who review export licensing cases would be in a better position to render proper decisions based on national security interests if they had the most available intelligence. But, after reviewing information obtained from law enforcement and technology specialists in the executive branch, the Minority staff has reached the preliminary finding that the U. S. intelligence effort regarding export controls is insufficient. Coordination among affected agencies is inadequate. Commitment of needed resources is lacking. The intelligence community is not organized to use information to block prohibited diversions.

Specifically, the Minority staff found the following deficiencies within the intelligence operations of the technology transfer control effort:

(1) The Export Administration Act mandated Commerce to determine the foreign availability of critical dual-use technologies. The foreign availability of technologies is an important ingredient in the decision making process for granting or denying export licenses. However, authorities within the executive branch assert that current foreign availability determinations are not adequate.

(2) The Intelligence Community has not been utilized sufficiently by either Commerce or the Department of Defense. Sources within the Intelligence Community state that they have virtually no communication with Commerce's Compliance Division regarding ongoing investigations of export violations. One representative of the Intelligence Community indicated that there is little feedback from Commerce regarding the intelligence information it provides. The information is submitted to Commerce's Office of Intelligence Operations and it is not known whether it is disseminated to the Compliance Division or other Divisions as well. Conversely, the Compliance Division rarely seeks the expertise of the Intelligence Community regarding investigations.

Moreover, once the intelligence apparatus is strengthened, then methods should be devised that enable sensitive information to be sanitized and passed on to law enforcement personnel in a form that will assist them. Several experienced law enforcement investigators pointed out that frequently intelligence on technology transfers has such a high classification that many agents working export controls cases cannot see it.

It is the view of government experts in law enforcement and science and engineering that until the intelligence capability is upgraded, law enforcement will suffer.

(3) Defense Research and Engineering tasks the Defense Intelligence Agency to conduct "end user" investigations. Essentially, DIA is to determine whether the end user of an export is not a national security risk. DIA performs this task as a support function to DR&E -- its license review procedures. Historically, DIA has been utilized infrequently in this capacity. Within the last 18 months DIA has been tasked more frequently; however, it does not have sufficient resources to conduct end user determinations that are necessary.

(4) There is no mechanism or organized program which conducts follow-up investigations of foreign exports or re-exports of U. S. technology. In fact, there is no adequate system to accurately determine what has been exported, re-exported, where it is used, and how it is used. There is no way to accurately determine the adverse impact to the U. S. of that dual use technology that has been obtained by our adversaries. Officials working in the technology field are troubled by the fact that our government has difficulty determining a current assessment of the "state of the art" of American technology. Given such a fact, the difficulty in assessing what technology has been lost and its impact on U. S. national security seems almost insolvable given the current resources and policy.

In summary, the U. S. Government, at present, has no high level interagency task force or entity comprised of senior cabinet level officials addressing the problem of export control and technology transfer. All past and current efforts along this line have been done by lower echelon Government officials who can merely make recommendations rather than needed changes.

Department of Justice

STATEMENT

OF

THEODORE STEWART GREENBERG
ASSISTANT UNITED STATES ATTORNEY
EASTERN DISTRICT OF VIRGINIA

BEFORE

THE

COMMITTEE ON GOVERNMENTAL AFFAIRS
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE

CONCERNING

TECHNOLOGY TRANSFER
AND
UNITED STATES v. MARC ANDRE DeGEYTER

ON

MAY 5, 1982

TABLE OF CONTENTS

		Page
I.	SUMMARY	1
II.	STATEMENT OF FACTS	2
	A. The Cast	2
	B. The Approach	3
	C. The Offer	4
	D. The Ante Raised	5
	E. The F.B.I. Interviews	7
	F. Discovered - The Approach Changes - DeGeyter and the Arab Shiek	9
	G. Summary of District Court Proceedings	11
EXHIBIT	1. Copy of $500,000 check	13
	2. Complaint (New York)	14
	3. Search Warrant Inventory	16
	4. Complaint (EDVA)	19
	5. Indictment	21
	6. Motion of the U.S. to Hold a Bail Justification Hearing	23
	7. Motion of the U.S. to Increase Bail and to Hold a Bail Justification Hearing	26
	8. Plea Agreement	28
	9. Information	30
	10. Sentencing Memorandum	31
	10A. Judgment and Probation/Commitment Order	34
	11. Proposed Commerce Letter	35
	12. $10,000 Civil Penalty	36

I. SUMMARY

On May 22, 1979, the Federal Bureau of Investigation received information from John Maguire, President, Software, A.G., Reston, Virginia, regarding the attempted bribery of one of his employees by Marc Andre De Geyter, a Belgian national, who stated that he was acting on behalf of the Russian Government. DeGeyter wanted to steal Software's trade secret, the ADABAS source code.

An FBI investigation, which included the use of an undercover agent and consensual monitoring, resulted in DeGeyter's arrest at John F. Kennedy International Airport on May 18, 1980, when DeGeyter gave an undercover agent a check for $500,000.

The investigation was monitored primarily by the Internal Security Section of the Department of Justice. Prosecution of the case was directed jointly by the United States Attorney's Office for the Eastern District of Virginia, and the Internal Security Section. 1/

The investigation was orginially conducted as a foreign counter-intelligence operation and then as a criminal investigation. DeGeyter was indicted on June 9, 1980, for violating Title 18, United States Code, Section 1952(a)(3), interstate and foreign travel in aid of a rackeetering enterprise, i.e., commercial bribery, in violation of the laws of the State of New York and the commonwealth of Virginia. DeGeyter was permitted to plead guilty to misdemeanor violations of the Export Administration Act and the Virginia Commercial Bribery Statute, because of significant governmental interests. After incarceration in Alexandria and FCI, Petersburg, Virginia, DeGeyter was permitted to voluntarily depart the United States.

1/ Then Deputy Section Chief John Martin and Department Attorney George Matava handled the case on behalf of the Internal Security Section.

II. STATEMENT OF FACTS

A. The Cast

1. ADABAS (Adaptable Data Base System), a data base management system. The source code is deemed to be a trade secret worth approximately $10,000,000. It would not be sold in the normal course of Software's business; and, in any event it would require a vote of the Directors to before it could be sold. It was maintained in a safe in the corporate offices and only selected individuals had access to it.

2. James Addis, Salesman, Software, A.G.

3. Special Agent Robert H. Bates, Federal Bureau of Investigation

4. Marc Andre DeGeyter - Following is a description of DeGeyter obtained through interview and observation:

Full Name:	Marc Andre DeGeyter
Other names used:	Marc A. DeGeyter and Marc De Geyter
Birthdate:	February 6, 1949, Tielt, Belgium White male, 5'10", 185 lbs., curly brown hair, receding in front and bald on top, sideburns, ruddy complexion, protruding stomach.
Nationality:	Belgium
Residence:	St. Huberstuslaan 15, Schilde, Belgium 2232
Marital Status:	Married, three children
Passport:	Holds Belgium passport number N147192; issued B-1 visa in Brussels, Belgium for travel to U.S.
Alien Registration:	P147192
Language:	Speaks and understands German, English and Russian

Corporations: President, Commercial Engineering and Sales Agency (CESA), Rue de Geneve, Box 7, Brussels, Belgium 1140, Telephone (02) 242-3660; President, TVS, Broadcast Systems Division, Rue de Geneve 10, Box 7, Brussels, Belgium 1140, Telephone (02) 242-3660; President, afrabel (Africa-Belgium), Rue de Geneve 10, Box 7, Brussels, Belgium 1140, Telephone (02) 242-3600; Managing Director, Softelectronics, Bodegemstreet 82-A, 1000 Brussels, Belgium, Telephone (02) 513-2692; In-Mark Associates (International Marketing Associates, a joint venture) Irvine, California; Inutec (joint venture) Laguna Beach, California.

5. Special Agent Timothy B. Klund, Federal Bureau of Investigation

6. John Norris Maguire, President, Software, A.G. of North America, Reston, Virginia

7. Charles Metheny, Chairman, CENTC, Inc., Reston, Virginia.

8. TECHMASHIMPORT - principal address USSR, Moscow. Registered in the United States by Amtorg Trading Corporation, N.Y.C., N.Y. Techmashimport is a USSR foreign trade corporation which imports equipment and machines for the chemical and oil-refining industry, for the production of basic chemical products, for organic synthesis, for the manufacture of chemical fibres and plastics, synthetic rubbers, rubber, and rubber goods, dyestuffs, lacquers, and paints, plant protection means as well as equipment for the manufacturing of plastic goods, refrigerating. A Registration Statement was filed with the Department of Justice on April 1, 1974.

B. The Approach

Sometime during the week of May 14-18, 1979, Marc Andre DeGeyter (hereafter DeGeyter) contacted James M. Addis, salesman for Software AG of North America, Inc. (Hereafter Software), Reston, Virginia which wholesales an adaptable data base management system (ADABAS), at Addis' residence in Reston, Virginia. DeGeyter told Addis that he had a business proposition to discuss. They met at the Reston Sheraton, Virginia on May 18, 1979.

DeGeyter identified himself as President, Commercial Engineering and Sales Agency, Brussels, Belgium. At this meeting, DeGeyter indicated that the Russian Government had retained him to obtain the "source code" (the mathematical formula behind a computer program) to Software's adaptable data base and computer programming technology, ADABAS, and offered Addis $150,000 for it. DeGeyter stated that he would give the money to Addis in $100 bills, or set up a Swiss bank account. Addis told DeGeyter that he would have to discuss this offer with Software's President, John Maguire. DeGeyter then said he would be in Los Angeles and New York City until May 25, at which time he would call Addis from New York.

DeGeyter called Addis at home on May 24, 1979. Addis told DeGeyter that he had spoken with John N. Maguire, 2/

2/ Maguire reported DeGeyter to the FBI on May 22, 1979 and agreed to cooperate in an investigation of DeGeyter.

President, major shareholder 3/ and one of the three directors of Software, concerning DeGeyter's offer and related to him that Maguire wanted to speak with DeGeyter. DeGeyter then stated that he would call Addis during May 28-30 to arrange for a meeting with Maguire. DeGeyter called on the 29th, but no meeting was scheduled.

C. The Offer

On June 20, Maguire called DeGeyter in Brussels. Maguire expressed interest in talking with DeGeyter and made some tentative arrangements to meet. DeGeyter called Maguire on July 18 and 20 from Missouri.

On July 20, DeGeyter flew from St. Louis, Missouri to National Airport, Arlington, Virginia, where he met with Maguire. DeGeyter indicated that the Soviets were interested in obtaining the source code and that he would purchase it for $150,000. In discussing the method of payment DeGeyter said, "Want a check in Zurich? You got it. Its yours. I couldn't care less. I'm not involved." Later in the conversation, he stated, "It's a one-time shot. No paper, no contract. Nothing." It was absolutely clear that DeGeyter wanted Maguire to steal the source code from his own company.

DeGeyter called Maguire from Brussels on August 7 to work out details of the transfer.

Maguire expressed concerns that the source code would be obtained by him competitors. DeGeyter assured him it was going to Russia, and nowhere else.

DeGeyter wanted Maguire to travel to Brussels where DeGeyter would have the source code authenticated. Thereafter, payment was to be made in Zurich, Switzerland. Maguire said that he wanted to be paid in cash in the United States. DeGeyter was hesitant about traveling with large sums of money because of customs searches.

3/ Maguire and his immediate family own approximately 82% of Software's stock.

During this conversation, Maguire asked, "Do you know about export licenses and everything? What if you get caught with that source code?" DeGeyter responded, "I don't think there should be any problem in that. I would then take the whole responsibility for that. You are not supposed to know where it goes to and what I'm going to do with it."

On August 27, Maguire called DeGeyter in Brussels and told him that he (Maguire) was losing interest in their initial deal. Maguire expressed nervousness about dealing with a Swiss Bank. DeGeyter then indicated that he was considering raising his offer to $200,000.

On September 5, DeGeyter called Maguire from Brussels. Maguire again expressed uneasiness about the deal. DeGeyter responded that he was ready to pay a higher price for the information. Arrangements were made for DeGeyter to call Maguire from New York City on September 12.

D. The Ante Raised

DeGeyter called Maguire on September 12 from New York City and offered to pay $250,000 for the source code. The money was to be placed in a Swiss bank account, or the title to an equivalent amount of real estate in California was to be placed in Maguire's name. DeGeyter indicated that he wanted to avoid bringing that much money into the United States. Maguire again stated that he wanted cash paid directly to him. DeGeyter replied that he would probably terminate the deal.

On October 1, DeGeyter telephoned Maguire and indicated that the Soviets had authorized additional payments, and that he would contact Maguire when he arrived in New York City.

On October 2, DeGeyter called Maguire from Reston, Virginia and arranged for a meeting.

On October 3, the two met for breakfast at the Sheraton Motel, Reston, Virginia. DeGeyter said that he flew in from London for the meeing. DeGeyter told Maguire that he had been authorized by the Soviets, to offer $450,000 and that

Maguire could negotiate through Techmashimport, a company owned by the Soviet Government, and responsible for negotiating contracts for importing technology to Russia. DeGeyter commented that Techmashimport is represented through the trade arm of the Soviet Embassy.

Maguire asked DeGeyter during this conversation whether he felt that exporting software technology without an export license from the Commerce or State Departments was illegal. DeGeyter replied that it was not. Maguire said that he would have to contact the State Department to verify this information. DeGeyter responded that it was not necessary; that the transaction could be ligitimatized on paper by Maguire's licensing one of DeGeyter's California corporations to use the source code.

Maguire again brought up the question of the payment for the information, noting that he was still wary about Swiss bank accounts and land transactions. DeGeyter said that he was unable to have the source code verified in the United States because a Soviet computer expert would test the source code in Brussels. He said that after the source code was authenticated, he and Maguire could fly to Switzerland, where they would put the source code on a Swissair flight to Moscow. DeGeyter claimed he only wanted the information for Tachmashimport.

DeGeyter insisted on handling this transaction either by way of a Swiss bank account, selling the license to one of his United States firms, or handling the matter through a Soviet company, which would take 45 days. Maguire re-emphasized he would not travel to Brussels, nor deal with a Swiss bank account. DeGeyter remarked he was taking all of the risks and did not want to go to jail. He further noted that if the deal was not completed, his business ventures in Belgium with the Soviet Government would suffer millions of dollars in lost business during the next five to ten years. He commented that if he could not get the required information, then the Soviets would assign another businessman or agent to obtain the technology. DeGeyter said he would contact Maguire on October 11, 1980.

On October 5 DeGeyter called Maguire from Belgium and told him that the offer of $450,000 was final. Maguire rejected the offer because DeGeyter was not willing to pay in cash.

E. The F.B.I Interviews

On February 4, 1980, the F.B.I. interviewed DeGeyter at the Sheraton Hotel in New York City. DeGeyter was told that he was being interviewed regarding allegations that he was acting in the United States as an agent of the Soviet Union without registering with the Attorney General. DeGeyter replied that he was unaware of the regulations.

During this interview, DeGeyter mentioned that he was formerly employed at Memorex Corporation in Stuttgart, Germany. He noted that during his tenure at Memorex, he was head of program engineering. He dealt with representatives of the Soviet Union, who expressed an interest in updating their computer technology. DeGeyter remarked that the Soviet Union was attempting to alter and modify its computer system to make it compatible with the systems in the United States.

DeGeyter remarked that shortly after his resignation from Memorex, he formed his own company, known as Commercial Engineering and Sales Agency (CESA), Reu de Geneve, Box 7, Brussels, Belgium 1140, Telephone (02) 242-3660. He noted that this firm was formed as a public relations organization; intended to act as a go-between in business dealings with other countries.

DeGeyter stated that in or about February, 1979, he was asked by a representative of Techmashimport if he would contact appropriate individuals at Software AG to obtain their source code. He contended that he was not offered any money and assumed that his payment would be a 15% commission he would receive from the seller.

DeGeyter recounted that during the early part of 1979, he contacted Addis and explained to him that he (DeGeyter) was

interested in obtaining software technology for the Soviet Union. DeGeyter stated that Addis introduced him to Maguire who also was informed of the Soviet's interest in Software's source code. Degeyter said he did not offer Maguire any money, but did refer to the 15% commission from the seller when the deal was final. DeGeyter stated that his offer to Software was still open, although he flet that Softwar was becoming disinterested.

DeGeyter said he had been asked by Maguire how he (DeGeyter) would export this information to the Soviet Union.

DeGeyter said that he told Maguire that Maguire would have to handle any problems arising out of obtaining an export license.

DeGeyter was reinterviewed by F.B.I. agents on the following day. During this interview, he elaborrated further on his negotiations with Software. He stated that he had received a $450,000 letter of credit from Techmashimport, Ministry of Foreign Trade, Moscow, Russia, in February, 1979, to be utilized in contracting for the purchase of the source code from Software.

DeGeyter said that he had been in contact with Maguire to whom he offered an introductory price of $150,000. DeGeyter said he later offered $250,000 and made a final offer of $450,000 two months prior to the interview. He stated that he had notified authorities at Techmashimport that the deal with Maguire was still open and that he was fervently negotiating a sale.

DeGeyter said that he left the method of payment to the satisfaction of Maguire; however, he suggested to Maguire that the money could be placed in a bank account in Switzerland to be obtained by Maguire when the deal was finalized. DeGeyter told Maguire that Maguire could travel to Brussels, Belgium where the source code would be authenticated by an experienced individual. An unidentified company in Brussels was to be utilized for authenticating the Software's source code. If it were found to be legitimate, it would be placed in an envelope and mailed to appropriate representatives of the Soviet Union. Maguire would be given some type of guarantee that the formula would not be duplicated and sold to his competitors in the United States.

DeGeyter said that Maguire questioned him as to the proper procedures for exporting the formula out of the United States. DeGeyter answered that this matter should be handled by Maguire. Maguire told DeGeyter that he knew someone at the Department of State whom he could contact regarding this matter.

DeGeyter said that he was advised by Soviet authorities 4/ that he could offer up to $450,000 to Software for the source code and if he could obtain the item at a lower price, DeGeyter could pocket the difference.

F. Discovered - The Approach Changes - DeGeyter and the Arab Shiek

On February 6, DeGeyter called Charles Matheny, Chairman of the Board of CENTEC, Reston, Virginia and told him that he was flying into National Airport on the following day. 5/

Matheny picked up DeGeyter at National Airport on February 7 and brought him to a hotel in Reston. At the hotel DeGeyter told Matheny that he wanted to discuss a deal involving an Arab bank which was headed by a Saudi Arabian shiek. He stated that the bank intended to implement a large scale computer system to handle its business and that he had agreed to assist the bank in that effort in return for free billing for one of DeGeyter's businesses. He then said that the bank wanted to put together a team of computer experts to monitor the implementation and specifically wanted an expert from Software. DeGeyter agreed to pay Matheny a finders fee of $25,000 in cash upon finding such an individual. DeGeyter then stated that the individual had to know everything about Software's system and that the individual had to be ready to bring as much of the system as possible, preferably the source code. At the close of the conversation, DeGeyter told Matheny that he was to keep a low profile and not let it be known that he (Matheny) was looking for anyone. In particular, DeGeyter told Matheny not to talk to Maguire or Addis about the arrangements.

4/ DeGeyter specifically mentioned contacts with two Soviets from Techmashimport.

5/ Matheny immediately contacted the F.B.I. and agreed to cooperate in the investigation.

On February 21, DeGyeter called Matheny and said that the Arabs were putting pressure on him to recruit an employee from Software and that he would contact Matheny later for his decision. During the next month DeGeyter inquired as to Matheny's progress in obtaining an employee from Software. Matheny stated that he had recruited an individual but that this individual wanted "front money."

On April 16th, Timothy B. Klund, an F.B.I. agent who was acting in an undercover capacity, but using his real name, posed an employee of Software and met with DeGeyter at the Holiday Inn in Rosslyn, Virginia. 6/ DeGeyter made in clear to Klund that he wanted him to steal the source code. Klund said that he would lose his job and face criminal charges if he were discovered. DeGeyter offered Klund a position in his company.

On April 18, Klund met DeGeyter at National Airport. On this occasion DeGeyter offered Klund $250,000 for the source code. Klund indicated he wanted $500,000 and that he would not travel overseas. DeGeyter said that he would contact the intermediary, Matheny, with a final price on April 25th.

On April 24th, DeGeyter contacted Matheny and told him that he was purchasing a ticket for Klund to use in traveling overseas.

On May 15th, DeGeyter again called Matheny and said that he would travel to New York and have a check for Klund. Matheny reiterated that Klund wanted cash.

On May 16th, DeGeyter called Matheny and said that he was bringing $500,000 in cash and would meet Klund at J.F.K. International Airport on May 18th.

The F.B.I. laboratory produced dummy computer tapes for Klund to pass to DeGeyter.

On May 18th, DeGeyter arrived at J.F.K. International Airport from Brussels, Belgium. Klund gave DeGeyter the dummy

---

6/ DeGeyter called Software sometime prior to this meeting to verify the fact that Klund was employed there.

95-929 O - 82 - 29

tapes and DeGeyter gave Klund the check for $500,000. 7/

Exhibit 1. DeGeyter was arrested by the F.B.I.

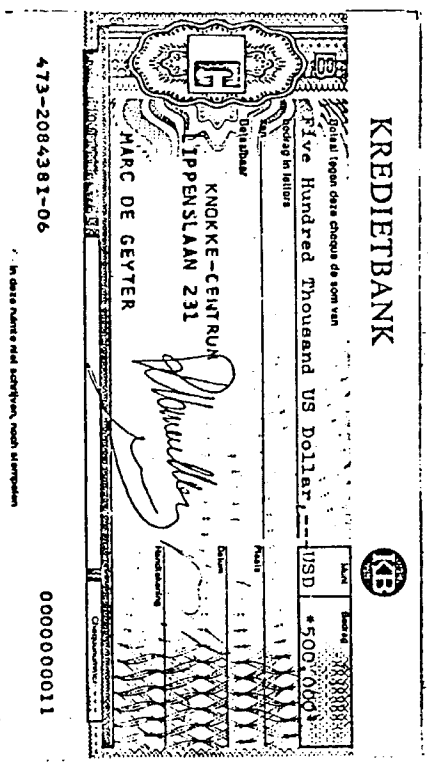
G. Summary of District Court Proceedings

Date	Summary
1980	
May 19	Complaint filed in EDNY (18 U.S.C. §1952(a)(3)). Rule 5 (Fed.R.Crim.P.) hearing. Bail set at $500,000. Exhibit 2.
May 21	Search warrant for DeGeyter's briefcase issued.
May 22	Search warrant executed. Briefcase searched. Exhibit 3. DeGeyter interviewed by FBI.
June 5	DeGeyter arrested in NY on EDVA Complaint (18 U.S.C. §1952(a)(3)). Exhibit 4. $500,000 surety bond.
June 6	Preliminary Hearing - EDNY
June 9	DeGeyter indicted in EDVA - 8 counts 1952(a)(3) -bond set at $500,000 surety. Bench warrant issued. Exhibit 5.
June 9 thru June 16	DeGeyter removed to EDVA.
June 16	DeGeyter arraigned on Indictment. Bond reduced to $100,000 (cash or surety) over objection of U.S. Special conditions set. Motions 6/26/80 -- Trial set for 7/22/80.
June 16	Bail hearing - U.S. motion to hold bond hearing re sources of money denied. Exhibit 6.
	U.S. gets informant information that DeGeyter has stated he is KGB agent and wants to raise bail money to flee U.S.
June 20	$100,000 check tendered to Clerk. U.S. motion to increase bail and hold a bail justification hearing filed. Exhibit 7. Bond hearing stayed until June 23, 1980.
June 23	Bail hearing - DeGeyter released on $100,000 bond. Cashier's check deposited.
July 7	Plea agreement signed (Exhibit 8) - DeGeyter pleads guilty to 2 count Information. Exhibit 9.
August 1	Sentencing Memorandum filed (Exhibit 10). DeGeyter sentenced. Four months Count 1; $500 fine on Count 2. Exhibit 10A. Export denial letter served on DeGeyter. Exhibit 11.

7/ Subsequent investigation determined that DeGeyter only had $800 in his account.

Date	Summary
1980	
October 17	DeGeyter released from FCI, Petersburg, VA to INS detainer.
October 17 thru October 24	DeGeyter allowed to voluntarily depart U.S. by INS.
December 24	$10,000 civil penalty finally assessed against DeGeyter by Dept. of Commerce per plea agreement. Penalty paid. Exhibit 12.
1982	
As of April 22	No final action on Department of Commerce Denial Letter of August), 1980.

EXHIBIT NO. 1


KREDIETBANK

Five Hundred Thousand US Dollar,--

USD *500,000,--

KNOKKE-CENTRUM
IPPENSLAAN 231

MARC DE GEYTER

473-20843 91-06

0000000011

EVIDENCE
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C.

EVIDENCE
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C.

EVIDENCE
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C.

EXHIBIT 2

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA

- against -

MARC ANDRE DeGEYTER,

Defendant.

- - - - - - - - - - - - - - - - - - X

COMPLAINT

Title 18, U.S.C. §1952

EASTERN DISTRICT OF NEW YORK, SS:

JIM WADE ISOM, being duly sworn, deposes and says that he is a Special Agent of The Federal Bureau of Investigation, duly appointed according to law and acting as such.

On or about the 18th day of May, 1980, within the Eastern District of New York and elsewhere, the defendant MARC ANDRE DeGEYTER did knowingly and willfully travel in foreign commerce with the intent to promote, manage, establish, carry on and to facilitate the promotion, management, establishment and carrying on of an unlawful activity, to wit: commercial bribery, in violation of the New York Penal Law §180.00 (McKinney 1975), and thereafter did knowingly and willfully attempt to commit commercial bribery in violation of said statute. (Title 18, United States Code, Section 1952(a)(3).

The source of your deponent's information and the grounds for his belief are a conversation with a Special Agent of the Federal Bureau of Investigation (hereinafter "unnamed Agent") wherein your deponent was advised as follows:

1. In or about the month of April, 1980, the defendant MARC ANDRE DeGEYTER engaged in several meetings with the unnamed Agent, wherein the Agent represented himself to be an employee of Software A.G. of North America, Inc., a software computer firm located in Reston, Virginia.

2. At the aforementioned meetings, the defendant MARC ANDRE DeGEYTER claimed that he represented a foreign conglomerate and stated that he wanted to obtain the source code for a computer data base system entitled "ADABAS". The unnamed Agent informed the defendant that the "ADABAS" source code was a trade secret of Software A.G. of North America, Inc., that the source code was not for sale and that the unnamed Agent would have to steal the source code from its owner, Software A.G., in order to deliver it to the defendant.

3. Thereafter, the defendant MARC ANDRE DeGEYTER agreed to pay the unnamed Agent $500,000 for the "ADABAS" source code.

4. On or about May 18, 1980, the defendant flew to John F. Kennedy International Airport, Queens, New York from Brussels, Belgium.

5. Pursuant to a pre-arranged plan, the defendant MARC ANDRE DeGEYTER met the unnamed Agent at a location in the International Arrivals Building, and delivered a check in the sum of $500,000 to the unnamed Agent in exchange for two reels of computer tape.

WHEREFORE, your deponent respectfully prays that the above-named defedant MARC ANDRE DeGEYTER be dealt with according to law.

Sworn to before me this
19th day of May 1980

UNITED STATES MAGISTRATE
EASTERN DISTRICT OF NEW YORK

EXHIBIT NO. 3

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/28/80

Pursuant to the issuance of a search warrant by United States Magistrate RUTH V. WASHINGTON, Southern District of New York (SDNY) on May 21, 1980, a search of a black leather briefcase, approximately 17 inches long, 13 inches high and three and one quarter inches deep, bearing a stitched border, black leather handle, brass fixtures and two combination locks, and located in the New York Office (NYO) of the Federal Bureau of Investigation (FBI) was made commencing at 8:30 AM on May 22, 1980, and terminated at 9:50 AM on May 22, 1980. The search was conducted by Special Agents (SAS) JIM WADE ISOM and JEREMIAH W. DOYLE in the NYO of the FBI.

An inventory of the items found in the above described briefcase are attached.

Investigation on 5/22/80 at New York, New York File # 105-167272

by SAS JIM WADE ISOM and JEREMIAH W. DOYLE/JWI/rl Date dictated 5/28/80

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Item 1. One black leather briefcase, approximately 17" long, 13" high and 3-1/4" deep, bearing a stitched border, black leather handle, brass fixtures and two combination locks.

Item 2. One Bag-Guard property ownership tag identifing M. DE GEYTER #M78197 as owner.

Item 3. One green Matallurgimport, Moscow, USSR, telephone book with handwritten names and telephone numbers.

Item 4. One American Express Company book of traveler's checks numbered RC21-499-559 through RC21-499-577 inclusive in denominations of $100 for a total of $1900.

Item 5. One business letter from Roth Western Corporation, Janesville, Wisconsin 53545, dated 11/21/79 to MARC DE GEYTER.

Item 6. One box of business cards for TVS Broadcast Systems Division, Brussels, Belgium, in the name of MARC DE GEYTER, President.

Item 7. One scratch pad of notes approximately 8½" by 11" consisting of three pages and cardboard back.

Item 8. One "Business Week", magazine international edition dated April 14, 1980.

Item 9. One ox-blood leather portfolio with the "Aigner" symbol in the upper right hand corner consisting of the following it s typed and written in various languages:

a. One pad of blank lined paper.

b. One business card in the name of JUVENALIY A. SEZLAKOV, Vice President, Novoexport, Moscow, USSR.

c. One handwritten list consisting of 10 items beginning with "ADABAS" and ending with "ADA BASICS, V. 4. 1".

d. One piece of paper bearing the handwritten name and address of GUNTER CAVALLAR, Sony GMBH Austria, Hauff Gasse 24, 1111 Vienna, Vienna 743636.

e. Two copies of "Consulting Agreement - Radio Production Licensing Program" between radio Semiconductor, Inc., State College, Penna. and MARC DE GEYTER dated 2/7/80.

f. One letter in the French language concerning "Cloudless Trading Company SA, Panama" dated 4/20/79.

g. One letter in the German language concerning "TVS Television and Broadcasting SA, Panama" dated 4/20/79.

h. One document in the German language concerning "TVS Television and Broadcasting SA, Panama" dated 4/20/79.

i. Three sheets of blank stationery bearing the letterhead "S.A. Commercial Engineering & Sales Agency N.V., Brussels, Belgium".

j. One telex dated 7/24/79 to Mr. BOLSJAKOV (dep 7) from MARC.

k. One telex dated 7/30/79 to dep7 (BOLSJAKOV) from MARC.

l. One document in the French language concerning "Cloudless Trading Company SA, Panama" dated 4/20/79.

m. One document captioned "Delivery Acceptance Protocol" between V/O Techmashimport, Moscow, USSR and DE GEYTER dated 4/11/79 at Moscow, USSR.

n. Two 5 page documents in the German language.

o. One sheet of note pad stationery bearing the letterhead "Hotel Metropol, Moscow".

p. One ten page contract No. 46-04/92211-113 between "techmashimport", Moscow, USSR and CESA, Brussels, Belgium dated 2/14/79, in Moscow.

q. One addendum No. 3 to contract 46-04/92211-113 dated 4/14/79.

r. One appendix No. 1 to contract No. 46-04/92211-113 entitled, "Specification of the Equipment."

s. One CESA packing list for contract #46-04/91122-113 concerning 3 pcs item LEO 8800 in the amount of $250,000 U.S. dollars dated April 9, 1979 at Brussels, Belgium addressed to Techmashimport, Moscow.

t. One credit document dated March 19, 1979 issued by Swiss Volksbank, Zurich, Switzerland in the amount of $450,000 U.S. dollars covering contract 46-04/91122-113.

u. One two page handwritten accounting worksheet.

v. One sheet on stationery bearing the letterhead "Roland Swreles" Rue Puccini, 44 (Boite 5) 1070 Bruxelles", with hand writing in the French language, signed "MARC DE GEYTER", dated March 22, 1979.

w. One page of note paper with handwriting in the French language.

x. One undated seven page T.V.S., Brussels, Belgium proposal number PSD791013 for the Ministry of Information, Government of Iraq, concerning short wave and medium wave radio broadcast systems.

y. One June 30, 1978 balance sheet for Frucodal Holding AG.

z. One one page document in the German language captioned "Orconsult SA", dated August 24, 1979.

aa. One December 31, 1978 balance sheet for "Orconsult SA, Zuerich".

bb. One bank Brussel Lambert document dated 10/19/79.

cc. One Societe Generale de Banque, Bruxellas dated 8/24/79.

dd. One 1976 - 1979 pocket calendar.

Item 10. One photocopy of Belgium Passport number 147192 in the name of MARC JOSEPH ANDRE DE GEYTER with USSR visa K number 841589 issued to MARC DE GEYTER, on 5/9/80 for travel to V/O Techmasimport, Moscow, USSR for the period 5/11/80 - 5/25/80.

Item 11. One brown vinyl check book with Kredietbank bank card in the name of MARC DE GEYTER 4473-2084381-06 08591242 and Kredietbank checks in the name of MARC DE GEYTER, Account Number 472-2084381-06, Check Number 03 through 010 inclusive and Check Number 012 through 024 inclusive.

Item 12. One Kingdom of Belgium Passport Nr 147192, and international certificate of vaccination for MARC DE GEYTER.

Item 13. One green 1980 bound business diary containing handwritten notes.

Item 14. One black spiral bound 1979 daily pocket calendar and personal telephone directory with handwritten names and telephone numbers and 3 sheets of note size paper bearing handwritten notations.

Item 15. One black leather wallet containing:

a. One first National City Bank traveler's check number 81[illegible]2-076-160 in the amount of $20.00.

b. One sheet of paper captioned "English for Beginners".

c. Various blank self-adhesive labels issued by several airlines for modifying issued airline tickets.

Item 16. One "Sharp" electronic calculator model EL-8145 and case.

Item 17. Six color photographs of an RSI, AM-FM radio.

Item 18. One black business card file containing numerous business cards.

Item 19. One 4 page document captioned "Arrestbefehl", dated February 7, 1980.

Item 20. One notepad bearing the letterhead "The Sheraton City Squire Hotel", NY, NY, with a handwritten notation.

Item 21. One pink computer card with a clipping captioned "Liegen", glued to the face.

Item 22. One blank notepad bearing the letterhead "Ritz-Carlton", Montreal, Canada.

Item 23. One 5½ in. by 3½ in. card captioned "Compliments of Benelux Home Diffusion", Brussels with handwritten notations on both sides.

Item 24. One sheet of paper 3½ in. sq. containing handwritten notation beginning "Smoke hot.....".

Item 25. Two blank guarantee cards for a "Philips" Audio-Visual apparatus.

Item 26. One one page document captioned Wahlungsbefehl dated February 20, 1980.

Item 27. One sheet of "Intourist" notepaper containing handwritten notes beginning "Sample of....." ending "814/4666563".

Item 28. Two telexes to Mr. BOLSHAKOV, signed "MARC".

Item 29. One unused "Sabena" airlines ticket number 3213754608 dated April 28, 1976 for travel between Brussels, Hanover, Brussels, issued to DE GEYTER.

Item 30. Three used "Pan-American" airlines tickets numbered 88254020472, 88254020473, and 88254020474 dated March 16, 1978, for travel between Los Angeles, Washington, New York, Brussels, Zurich, Tehran, Athens, Brussels, London, Los Angeles, Washington, Los Angeles, issued to DE GEYTER.

Item 31. One unused "Sabena" airlines ticket number 3431346302, dated June 28, 1978 for travel between Brussels, London, Isle of Man, London, Brussels, issued to DE GEYTER.

Item 32. One open prepaid "Air France" ticket number 3020678553, dtd. November 21, 1978, issued to DE GEYTER for travel anywhere on an Air France air route.

Item 33. One used "Sabena" airlines ticket number 1210734420, dated March 19, 1980 for travel between Brussels, Zurich, Brussels, issued to DE GEYTER.

Item 34. Two "Sabena" airlines tickets numbered 1410446431 and 1410446432, dated April 15, 1980 for travel between New York, Washington, New York, Brussels, Vienna, Moscow, Vienna, Brussels, New York, Washington, issued to DE GEYTER.

Item 35. One yellow "Bic" pen.

EXHIBIT NO. 4

Form A. D. 95 (Rev. 11-1-63) Complaint

United States District Court
FOR THE
EASTERN DISTRICT OF VIRGINIA - Alexandria

UNITED STATES OF AMERICA	Magistrate's Docket No. 80
v	Case No. 270-M
MARC ANDRE DeGEYTER	COMPLAINT for VIOLATION of
	U.S.C. Title 18
	Section 1952(a)(3)

BEFORE _____ (Name of Magistrate) _____ (Address of Magistrate)

The undersigned complainant being duly sworn states:

That on or about April 18, 19 80, at Alexandria, Virginia in the Eastern District of Virginia

(1) MARC ANDRE DeGEYTER

did(1)

knowingly and willfully travel in interstate commerce from New York to the Eastern District of Virginia with intent to promote, manage, establish, carry on and to facilitate the promotion, management, establishment and carrying on of an unlawful activity, to wit: commercial bribery, in violation of § 18.2-444, Code of Virginia, 1950, as amended and thereafter did perform and attempt to perform acts to promote, manage, carry on and facilitate the promotion, management and carrying on of said unlawful activity.

And the complainant states that this complaint is based on

See Attached Sheet.

EXHIBIT NO. 4--Continued

And the complainant further states that he believes that:

are material witnesses in relation to this charge.

Timothy B. Klund
Special Agent, FBI

Sworn to before me, and subscribed in my presence, June 5, 1980.

W. Harris Grimsley

TRUE COPY, TESTE:
W. HARRIS GRIMSLEY,
QUIN SCHLSON
BY:
DEPUTY CLERK

United States v. MARC ANDRE DeGEYTER
Affidavit for Complaint
Page 2

18 U.S.C 1952(a)(3)

The undersigned complainant, being duly sworn, states that: I am a Special Agent of the Federal Bureau of Investigation; and that the information set out hereinafter has been gained from personal investigation and investigation by other Agents of the FBI whose reports I have read.

1. On or about April 16, 1980, while acting in an undercover capacity, I met with MARC ANDRE DeGEYTER at the Rosslyn Holiday Inn in Rosslyn, Virginia. during this meeting, I told the defendant that I was an employee of the Software AG of North America, Inc. (hereinafter Software AG), a software computer firm located in Reston, Virginia.

2. At this meeting MARC ANDRE DeGEYTER claimed that he represented a foreign conglomerate and stated that he wanted to obtain the source code for a computer data base system entitled "ABABAS". I informed DeGeyter that this source code was not for sale, and that I would have to steal it from its owner, Software AG, in order to deliver it to DeGEYTER.

3. On or about April 18, 1980, while again acting in an undercover capacity and posing as an employee of Software AG, I was at Washington National Airport, Arlington, Virginia, where I observed DeGeyter arrive on an Eastern Airlies shuttle flight which I determined had originated in New York.

4. At National Airport DeGeyter offered me $250,000 for the "ABABAS" source code.

5. Based upon FBI reports which I have read, the source code for Software AG's computer data base system entitled "ABABAS" is a trade secret and would not be sold in the ordinary course of business without approval of the Board of Directors of Software AG.

Timothy B. Klund
Special Agent
Federal Bureau of Investigation

Subscribed and Sworn to Before me this 5th day of June, 1980.

W. Harris Grimsley
UNITED STATES MAGISTRATE

EXHIBIT NO. 5

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CR. NO.
	)	
MARC ANDRE DeGEYTER	)	

JUNE 1980 TERM - At Alexandria

COUNT I

THE GRAND JURY CHARGES THAT:

A. At all times material to this Indictment:

1. The defendant, MARC ANDRE DeGEYTER was a citizen of Belgium.

2. Software AG of North America (hereinafter Software) was a Virginia corporation specializing in computer software. Among other products Software marketed the Adaptable Data Base System (hereinafter ADABAS). ADABAS was a data base management system.

3. The ADABAS source code was a trade secret of Software AG. It was the "logic" behind the ADABAS system.

4. From in or about May 1979, through May 18, 1980, the defendant MARC ANDRE DeGEYTER:

a. represented to various individuals that he wanted to obtain the ADABAS source code for Techmashimport, a foreign trade corporation organized under the laws of the Union of Socialist Republics and other foreign interests.

b. DeGeyter offered amounts varying from $150,000 to $500,000 for the ADABAS source code.

B. On or about May 18, 1979, the defendant MARC ANDRE DeGEYTER did travel in interstate commerce from New York to the Eastern District of Virginia with the intent to otherwise promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on of an unlawful activity, said unlawful activity being commercial bribery, in violation of the law of the Commonwealth of Virginia (Section 18.2-444, Code of Virginia, 1950 as amended) and thereafter the defendant MARC ANDRE DeGEYTER did perform and attempt to perform acts to promote, manage, carry on and facilitate the promotion, management and carrying on of said unlawful activity.
(Violation of Title 18, United States Code, Section 1952(a)(3)).

COUNTS II THROUGH VI

THE GRAND JURY FURTHER CHARGES THAT:

A. Paragraphs A1 through A4 of Count I are hereby realleged and incorporated by reference as though set forth in full.

EXHIBIT NO. 5--Continued

B. On or about the dates set forth, the defendant MARC ANDRE DeGEYTER did travel in interstate and foreign commerce as set forth below with the intent to otherwise promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on of an unlawful activity, said unlawful activity being commercial bribery, in violation of the law of the Commonwealth of Virginia (Section 18.2-444, Code of Virginia, 1950 as amended) and thereafter the defendant MARC ANDRE DeGEYTER did perform and attempt to perform acts to promote, manage, carry on and facilitate the promotion, management and carrying on of said unlawful activity.

COUNT	DATE	FROM	TO
II	July 20, 1979	Missouri	Eastern District of Virginia
III	October 2, 1979	United Kingdom	Eastern District of Virginia
IV	February 7, 1980	Pennsylvania	Eastern District of Virginia
V	April 16, 1980	New York	Eastern District of Virginia
VI	April 18, 1980	New York	Eastern District of Virginia

(Violation of Title 18, United States Code, Section 1952(a)(3)).

COUNT VII

A. Paragraphs A1 through A4 of Count I are hereby realleged and incorporated by reference as though set forth in full.

B. On or about May 16, 1980, the defendant MARC ANDRE DeGEYTER did use a facility in interstate and foreign commerce, namely international and interstate telephone facilities from outside the United States of America to the Eastern District of Virginia with the intent to otherwise promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on of an unlawful activity, said unlawful activity being commercial bribery, in violation of the law of the Commonwealth of Virginia (Section 18.2-444, Code of Virginia, 1950 as amended) and thereafter the defendant MARC ANDRE DeGEYTER did perform and attempt to perform acts to promote, manage, carry on and facilitate the promotion, management and carrying on of said unlawful activity. (Violation of Title 18, United States Code, Section 1952(a)(3)).

COUNT VIII

A. Paragraphs A1 through A4 of Count I are hereby realleged and incorporated by reference as though set forth in full.

B. On or about May 18, 1980, the defendant MARC ANDRE DeGEYTER did cause a person to travel in interstate commerce from the Eastern District of Virginia to New York with the intent to

EXHIBIT NO. 5--Continued

otherwise promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on of an unlawful activity, said unlawful activity being commercial bribery, in violation of the New York Penal Law §180.00 (McKinney 1975 as amended) and thereafter the defendant MARC ANDRE DeGEYTER did perform and attempt to perform acts to promote, manage, carry on and facilitate the promotion, management and carrying on of said unlawful activity.

(Violation of Title 18, United States Code, Section 1952(a)(3) and 2).

A TRUE BILL:

FOREMAN

JUSTIN W. WILLIAMS
United States Attorney

By: Theodore S. Greenberg
Assistant United States Attorney

George W. Nadava
Special Assistant United States Attorney

EXHIBIT NO. 6

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL No. 80-00102-A
	)	
MARC ANDRE DeGEYTER	)	

MOTION OF THE UNITED STATES TO HOLD A BAIL JUSTIFICATION HEARING

The United States, by the undersigned attorney, moves this Court to hold a hearing to insure that any bond posted by the defendant, Marc Andre DeGeyter actually assures his subsequent court appearances. See United States v. Nebbia, 357 F.2d 303 (2d Cir. 1966).

DeGeyter was indicted on June 9, 1980 for violating 18 USC §1952(a)(3), by traveling in interstate and foreign commerce to commit commercial bribery. An arrest warrant was issued and the defendant is in the custody of the United States Marshal. A $500,000 surety bond was set on the return of the Indictment.

EXHIBIT NO. 6—Continued

The Fourth Circuit has held, citing Nebbia, supra, that the "purpose of bail is to secure the presence of the defendant at trial." United States v. Kirkman, 416 F.2d 747, 752 (4th Cir. 1970).

DeGeyter is a foreign national with no residence or business property in the United States. The Indictment alleges that DeGeyter was trying to obtain a trade secret from Software AG of North America, a Reston, Virginia corporation), for a Russian foreign trade corporation and other foreign interests. A review of DeGeyter's passport shows extensive foreign travel. At the time of his arrest an unused airline ticket for travel amongst the cities of Moscow, Vienna, Brussels, New York and Washington was found in his briefcase. DeGeyter was arrested when he passed a $500,000 check drawn on a foreign bank to an undercover agent.1/ Thus, any bond posted by the defendant may not assure his appearance at trial, but only indicate the extent of his criminally obtained resources.

In order to establish that money/surety posted to meet the bond in this case will assure the defendant's presence at trial, the United States requests a hearing pursuant to United States v. Nebbia, supra. See also, United States v. Melville, 309 F.Supp. 824 (S.D. N.Y. 1970).

Pursuant to 18 USC §3146(a)(5) this Court has the power to set whatever terms and conditions are necessary to assure the defendant's future court appearance and a judicial inquiry into the adequacy of the origin of the money being posted to secure DeGeyter's release is proper.

WHEREFORE premises considered, the United States requests that the Court direct the Clerk to enter on the bond, that as a condition precedent to DeGeyter's release, a hearing inquiring into the sources of the bail money be held.

Respectfully submitted,

JUSTIN W. WILLIAMS
UNITED STATES ATTORNEY

By: Theodore S. Greenberg
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Motion of the United States to Hold a Bail Justification Hearing ~~was~~ will be hand delivered to David Cutner, Esquire.

Theodore S. Greenberg
Assistant United States Attorney

1/ Subsequent investigation has shown that there was only $800 in the account upon which the check was drawn.

EXHIBIT NO. 6--Continued

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
V.	)	CRIMINAL No. 80-00102-A
	)	
MARC ANDRE DeGEYTER	)	

ORDER

On motion of the United States requesting that this Court hold a bail justification hearing prior to the defendant, DeGeyter, being released from the custody of the United States Marshal to determine that any money/surety filed with the Clerk adequately insure DeGeyter's subsequent court appearances upon the above styled Indictment;

It is this day of June, 1980,

ORDERED that the Clerk enter on the bond, that as a condition precedent to the defendant being released, a hearing be held by this Court to determine if the sources of the money the defendant posts for bond will insure his future appearances in this Court.

Denied

UNITED STATES DISTRICT JUDGE

June 13, 1980

Alexandria, Virginia

Date:

I ask for this:

Theodore S. Greenberg
Assistant United States Attorney

EXHIBIT NO. 7

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.	)	Cr. No. 80-102-A
	)	
MARC ANDRE DeGEYTER	)	

MOTION OF THE UNITED STATES TO INCREASE
BAIL AND TO HOLD A BAIL JUSTIFICATION HEARING

The United States, by the undersigned attorney, moves this court to increase the defendant's bail to $500,000 and to hold a bail justification hearing should he tender the bond.

DeGeyter was arrested in the Eastern District of New York, on May 18, 1980 for violating 18 U.S.C. §1952(a)(3) by traveling in interstate and foreign commerce to commit commercial bribery. The Eastern District of New York set bail at $500,000, cash or surety. On June 9, 1980, a Grand Jury in the Eastern District of Virginia returned an eight count indictment against DeGeyter, charging him with eight violations of 18 U.S.C. §1952(a)(3). Bail was set at $500,000. At arraignment on June 16, 1980, bail was reduced to $100,000, cash or surety with certain special conditions on travel. On June 20, 1980 his attorney tendered a $100,000 cashier's check to the Court to meet bail.

In view of recent information obtained through the FBI, the United States believes that DeGeyter, a foreign national, intends to flee the United States and the jurisdiction of this Court prior to trial. To support its contention, the Government will present an FBI agent who will testify that a reliable confidential informant has provided information indicating that DeGeyter intends to flee after he meets the present $100,000 bond.

Even though the testimony of the FBI agent will be hearsay, it is admissible at a bail hearing.[1/] See United States v. Wind, 527 F.2d 672, 675 (6th Cir. 1975); United States v. Brown, 399 F. Supp. 631 (W.D.Okla. 1975)(state investigative agent permitted to testify regarding information received from reliable informant).

The United States does not intend to reveal the identity of the informant, either by revealing the informant's name or by disclosing sufficient information from which the individual's identity could be deduced because such revelations will probably result in death to the informant and is unnecessary under the circumstances of this hearing.

1/

18 U.S.C. §3146(f) provides that "[i]nformation stated in, or offered in connection with, any order entered pursuant to this section need not conform to the rules pertaining to the admissibility of evidence in a court of law.

95-929 O - 82 - 30

EXHIBIT NO. 7--Continued

United States v. Roviaro, 353 U.S. 53, 60-61 (1953) only requires the disclosure of an informant's identity when such information "is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause." Moreover, the Supreme Court in McCray v. Illinois, 386 U.S. 300, 307 (1967), stated that whether an informant's identity must be compelled depends not only upon the facts of the case, but also upon the stage of the proceedings at which the issue arises. Since the question of the informant's identity is only arising at a bail hearing, it should not be compelled. Cf., United States v. Pomp, 484 F.2d 919, 922-923 (4th Cir. 1973). The "purpose of bail is to secure the presence of the defendant," United States v. Kirkman, 416 F.2d 747, 752 (4th Cir. 1970). Should DeGeyter be permitted to post the $100,000 bond or should his bond be raised[2/] the United States moves this Court for a hearing pursuant to United States v. Nebbia, 357 F.2d 303 (2d Cir. 1966) and United States v. Melville, 309 F.Supp 824(S.D.N.Y. 1970). Both cases permit a judicial inquiry into the origin of the money being posted for bail. See 18 U.S.C. §3146(a)(5). The inquiry is to assure the Court that the "sources of bail...provide the moral responsibility and the proper purposes to assure the defendant's presence." Melville, supra at 828. "[any] demand for anonymity leads to a suggestion that the donor is engaged in something furtive, stealthy [,]...suspect in motive and possibly illegal...[and] does not enhance assurance of the presence of the defendant." Id. at 829.

In this case, the defendant attempted to steal a "trade secret" worth in excess of $10,000,000 and intended to remove it from the United States.

The Government's evidence is very strong and consists, in part, of body recordings and pre and post arrest voluntary statements made to FBI agents. The defendant, a foreign national residing in Belgium has no family or regular business ties to this country.

Respectfully submitted,

JUSTIN W. WILLIAMS
United States Attorney

Theodore S. Greenberg
Assistant United States Attorney

George G. Matava
Special Assistant United States Attorney

2/ Should the Court grant the Government's Motion to Increase Bail, the United States requests that the Court set forth its reasons in writing. 18 U.S.C. §3146(d) and (e).

EXHIBIT NO. 8

United States Attorney
Eastern District of Virginia

117 South Washington Street
Alexandria, Virginia 22314

703/557-9100
FTS/557-9100

July 7, 1980

David Cutner, Esquire
John D. Schmidtlein, Esquire

Re: United States v. Marc Andre DeGeyter
Cr. No. 80-102-A

Gentlemen:

The defendant, Marc Andre DeGeyter is charged in an eight count Indictment with traveling in interstate and foreign commerce with the intent to commit commercial bribery in violation of Title 18, United States Code, Section 1952(a)(3). Trial is set for July 22, 1980.

Confirming our discussions of July 2 and 5, 1980, the United States, by counsel, and the defendant agree to the following:

1. Defendant DeGeyter will plead guilty to one count of violating the Export Administration Act of 1969 (50 U.S.C. App. Supp. 1, Section 2401 et seq., by a violation of the Export Administration Act (15 CFR 387.2) by seeking to export the ADABAS source code ("technical data"; 15 CFR 379.1(a) and (b)(1)(i) and (ii)) from the United States without the required export license (15 CFR 370.3(a); 379.2). The maximum penalty for this offense is one year imprisonment and/or a $25,000 fine (50 U.S.C. App. Supp. 1, Section 2405(A), Export Administration Act of 1969 and 15 CFR 387.1(a)).

2. For knowingly and wilfully violating the Export Administration Act, Marc Andre DeGeyter consents to an administrative imposition of a $10,000 civil penalty by the Secretary of Commerce or his authorized representative pursuant to the provisions of 50 U.S.C. App. Supp. 1, Section 2405(C)(1) and (C)(2)(B) and 15 CFR 387.1(b)(3). DeGeyter agrees to execute any documents necessary to said consent and collection of the $10,000 penalty.

3. Prior to the defendant's sentencing of the offense set forth in paragraph 1 above, the defendant is to deliver to the United States Attorney for the Eastern District of Virginia a cashier's check in the amount of $10,000 made payable to the Treasurer of the United States. This check will be held by the United States Attorney until such time as the Secretary of Commerce or his authorized representative imposes the aforesaid civil penalty. In the event that the Secretary of Commerce declines to impose the aforesaid $10,000 civil penalty, or imposes only a portion thereof, the cashier's check or an appropriate refund will be remitted to the defendant or his authorized representative.

4. The defendant will plead guilty to one count of attempted commercial bribery in violation of Title 18, United States Code, Section 13 assimilating 18.2-444(1); 18.2-27, Code of Virginia (1950, as amended).

EXHIBIT NO. 8--Continued

5. ~~Following~~ At sentencing on the aforesaid counts, the United States will dismiss the pending eight count Indictment and agrees not to further prosecute the defendant for his activities regarding Software AG of North America, Reston, Virginia from May 1979 through May 18, 1980 or any of which are now known to the Government.

Should the defendant seek at any time to withdraw his plea of guilty to the aforesaid counts or should the District Court decline to accept his plea for any reason, this agreement is null and void and the United States will proceed to trial on the eight count Indictment returned June 9, 1980.

The defendant has been released from custody on a $100,000 cash bond with special travel restrictions. The United States has no objection to the continuation of the present bond pending sentencing.

MAD DC JDS TSG

David Cutner, Esquire
John D. Schmidtlein, Esquire
Page Three

At sentencing the United States will take no position as to the sentence to be imposed.

No additional promises, agreements or conditions have been entered into other than those set forth in this letter and none will be entered into unless in writing and signed by all parties.

Very truly yours,

JUSTIN W. WILLIAMS
United States Attorney

By: Theodore S. Greenberg
Assistant United States Attorney

Agreed and consented to:

Marc Andre DeGeyter

David Cutner, Esquire

John D. Schmidtlein, Esquire

EXHIBIT NO. 9

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 80-102-A
	)	
MARC ANDRE DeGEYTER	)	

THE UNITED STATES ATTORNEY CHARGES THAT:

COUNT ONE

On August 7, 1979 in the Eastern District of Virginia and elsewhere, the defendant MARC ANDRE DeGEYTER did knowingly, wilfully and unlawfully counsel, command and induce the doing of an act prohibited by the Export Administration Act and proclamations, orders, rules and regulations issued thereunder, to wit: counseling, commanding and inducing an officer of Software AG to export the ADABAS source code from the United States to Belgium without obtaining a validated export license.
(All in violation of the Export Administration Act of 1969, 50 United States Code App. Supp. 1, Section 2401 et seq. 2405(A); 15 C.F.R. 370.3(a); 379.1(a) and (b)(1)(i) and (ii); 379.2; 387.1(a); 387.2).

COUNT TWO

On April 18, 1980 at Washington National Airport, in the Eastern District of Virginia, within the special maritime and territorial jurisdiction of the United States, the defendant MARC ANDRE DeGEYTER did knowingly, wilfully and unlawfully attempt to offer to an agent, employee and servant a gratuity without the knowledge and consent of the principal, employer and master of such agent, employee and servant with intent to influence his action to the prejudice of his principal's, employer's and master's business, to wit; to purloin the ADABAS source code.
(All in violation of 18 U.S.C. §7(3); 13 assimilating 18.2-444(1) 18.2-27, Code of Virginia (1950 as amended)).

JUSTIN W. WILLIAMS
UNITED STATES ATTORNEY

By: Theodore S. Greenberg
Theodore S. Greenberg
Assistant United States Attorney

EXHIBIT NO. 10

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 80-102-A
	)	
MARC A. DeGEYTER	)	

SENTENCING MEMORANDUM

Sentencing is set for August 1, 1980. On June 9, 1980 the defendant was indicted on eight counts of interstate and foreign travel with the intent to commit commercial bribery, in violation of 18 U.S.C. § 1952(a)(3). On July 7, 1980 DeGeyter entered into a plea agreement with the United States and pled guilty to a two count Information charging violations of the Export Administration Act of 1969 and the Virginia commercial bribery statute.

On July 30, 1980 the United States reviewed the pre-sentence report in this case. The "Official Version" section of the report is incomplete in that the report depicts DeGeyter's actions as merely an attempt to legitimately buy the ADABAS source code. Accordingly, the United States submits the following facts for the Court's consideration:

A. Background

1. Software AG of North America (hereinafter Software) is a Virginia corporation specializing in computer software. Among other products, Software markets the Adaptable Data Base System (hereinafter ADABAS). ADABAS is a data base management system.

2. The ADABAS source code is a trade secret of Software and is worth at least $10 million.

3. The ADABAS source code constitutes "technical data" under the provisions of the Export Administration Act of 1969.

4. Export from the United States of the ADABAS source code is prohibited without a "validated export license" or other authorization granted by the Office of Export Administration, United States Department of Commerce.

5. Export of technical data is defined, in pertinent part, as an actual shipment or transmission of technical data out of the United States or any release of technical data in the United States with the knowledge or intent that the data will be shipped or transmitted from the United States to a foreign country.

EXHIBIT NO. 10--Continued

B. The Information

DeGeyter pled guilty to wilfully commanding and inducing James Maguire, President, Software AG to export the ADABAS source code from the United States to Belgium without obtaining a validated export license.

Beginning in May 1979 DeGeyter started making contacts with Maguire and James Addis (a Software salesman) to get them to sell him the ADABAS source code without the knowledge of the company.

On May 18, 1979, DeGeyter met Addis, offered him $150,000 for the source code in $100 bills or to set up a Swiss bank account. Addis told DeGeyter to talk to Maguire.

DeGeyter contacted Maguire and at their first meeting on July 20, 1979, told Maguire, "It's a one-time shot, no paper, no contract".

During his dealings with Maguire, DeGeyter made it clear that he wanted Maguire to bring the source code to Belgium, where its authenticity could be tested, following which it would be sent to Technashimport, Moscow. This was the substance of the conversation which took place on August 7, 1979 and which forms the basis of Count One.

The following colloquy on August 7, 1979 between Maguire (JM) and DeGeyter (MD) is germane to this offense.

> JM: In general, I say yes, but I got some questions. You know, I'm a little bit nervous. I mentioned some of the concerns before. This source code, my understanding is, that, as far as moving something out of the U.S., you know, it may be an administrative technicality. Do you know about the export licenses and everything? What if you get caught with that source code?
>
> MD: I don't think there should be any problem in that. I would then take the whole responsibility for that. You are not supposed to know where it goes to and what I am going to do with it.
>
> JM: Okay. It's what's, you know, is, is, is there any way they can trace it?
>
> MD: No.
>
> JM: Back to us.
>
> MD: No, no way whatsoever. There's really no way. Nothing, but you know, you have to trust me on that. I'm telling you there's no way.
>
> * * *
>
> MD: Okay, we'll try to head for the last days of August.
>
> JM: Okay.
>
> MD: And be in Brussels. And we do the tests, we fly to Zurich, and you get the money, and that's it.

In or about November 1979, Maguire, who had been cooperating with the FBI broke off contact with DeGeyter.

EXHIBIT NO. 10--Continued

Unable to obtain the source code directly from Maguire, DeGeyter sought to recruit a Software employee through an intermediary in another company. The intermediary contacted the FBI. On April 18, 1980 DeGeyter offered an FBI agent posing as a Software employee $250,000 to purloin the source code. At this time DeGeyter changed the representations he made to Maguire and told the agent that he was trying to obtain the source code for an Arab group. This transaction was charged as Count Two in the Information to which DeGeyter pled guilty.

On May 18, 1980 DeGeyter gave the FBI undercover agent a check for $500,000 in return for the source code which the agent was to have stolen from Software. Following the exchange DeGeyter was arrested.

Respectfully submitted,

JUSTIN W. WILLIAMS
UNITED STATES ATTORNEY

By: Theodore S. Greenberg
Theodore S. Greenberg
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Sentencing Memorandum was hand delivered this 31st day of July, 1980 to John D. Schmidtlein, Esquire, Suite 506, 320 King Street, Alexandria, Virginia 22314.

Theodore S. Greenberg
Theodore S. Greenberg
Assistant United States Attorney

EXHIBIT NO. 10A

United States of America vs.

DEFENDANT: MARC ANDRE DEGEYTER

United States District Court
THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

DOCKET NO. Cr. 80-102-A

JUDGMENT AND PROBATION/COMMITMENT ORDER

COUNSEL: In the presence of the attorney for the government the defendant appeared in person on this date — MONTH 08 DAY 01 YEAR 80

[ ] WITHOUT COUNSEL However, the court advised defendant of right to counsel and asked whether defendant desired to have counsel appointed by the court and the defendant thereupon waived assistance of counsel.

[X] WITH COUNSEL John Schmidtlein, Esq. (Name of counsel)

PLEA: [X] GUILTY, and the court being satisfied that there is a factual basis for the plea, [ ] NOLO CONTENDERE, [ ] NOT GUILTY

FINDING & JUDGMENT: There being a finding of { [ ] NOT GUILTY. Defendant is discharged; [X] GUILTY.

Defendant has been convicted as charged of the offense(s) of
Seeking to export the ADABAS source code without an export license - Export Administration Act of 1969, 50 USC App. Supp. I, Sec. 2401 et seq.; 2405(A); 15 CFR 370.3(a); 379.1(e) and (b)(1)(i) and (ii); 379.1; 387.1(a); 387.2 - Count 1
Attempted commercial bribery - 18 USC 7(3); 13 assimilating 18.2-444(1); 18.2-27, Code of Virginia (1950 as amended) - Count 2

SENTENCE OR PROBATION ORDER: The court asked whether defendant had anything to say why judgment should not be pronounced. Because no sufficient cause to the contrary was shown, or appeared to the court, the court adjudged the defendant guilty as charged and convicted and ordered that the defendant be hereby committed to the custody of the Attorney General or his authorized representative for imprisonment for a period of four (4) months as to Count 1 and a fine of $500.00 shall be imposed as to Count 2. The defendant shall be given credit for time already spent incarcerated on these charges.

SPECIAL CONDITIONS OF PROBATION:

ADDITIONAL CONDITIONS OF PROBATION: In addition to the special conditions of probation imposed above, it is hereby ordered that the general conditions of probation set out on the reverse side of this judgment be imposed. The Court may change the conditions of probation, reduce or extend the period of probation, and at any time during the probation period or within a maximum probation period of five years permitted by law, may issue a warrant and revoke probation for a violation occurring during the probation period.

COMMITMENT RECOMMENDATION: The court orders commitment to the custody of the Attorney General and recommends,

It is ordered that the Clerk deliver a certified copy of this judgment and commitment to the U.S. Marshal or other qualified officer.

CERTIFIED AS A TRUE COPY ON THIS DATE 8-1-80
BY [signature] CLERK / DEPUTY CLERK

SIGNED BY [X] U.S. District Judge [ ] U.S. Magistrate

Date 08-01-80

EXHIBIT NO. 11

Mr. Marc Andre DeGeyter
St. Rijkersteslaan 15
Zottegem, Belgium 9700

Dear Mr. DeGeyter:

The Office of Export Administration, International Trade Administration, U.S. Department of Commerce, hereby charges that you, Marc Andre DeGeyter, have knowingly violated the provisions of Sections 387.2 and 387.3 of the Export Administration Regulations (15 C.F.R. Part 368 et seq. (1979)) (the Regulations), issued pursuant to the Export Administration Act of 1969, as amended (50 U.S.C. app. 2401, et seq. (1976)).

The Office of Export Administration has reason to believe that, during the period from May 18 to November 6, 1979, you counseled and induced an employee of Software AG of North America, Inc., Reston, Virginia, to procure for you U.S.-origin restricted technical data. The procurement attempt was made by you with the intention that the technical data be exported to the U.S.S.R. without applying for and obtaining a validated export license from the Office of Export Administration which you knew or should have known was required.

Accordingly, you are hereby notified that administrative proceedings are instituted against you pursuant to Section 11(c) of the Export Administration Act of 1979 (P.L. 96-72) (to be codified at 50 U.S.C. app. 2401 et seq.) (the Act) and Part 388 of the Regulations (44 F.R. 55857, October 12, 1979) for the purpose of obtaining an Order imposing administrative sanctions including any or all of the following:

Revocation of validated export licenses under Section 388.3(a)(1);

General denial of export privileges under Section 388.3 (a)(2);

Exclusion from practice under Section 388.3(a)(3); and/or

Imposition of a civil penalty under Section 388.3(a)(4).

Copies of Parts 387 and 388 of the Regulations are enclosed.

If you fail to answer the charges contained in this letter within thirty (30) days after service as provided in Section 388.7 of the Regulations, such failure will be treated as a default under Section 388.8.

You are further notified that you are entitled to an agency hearing on the record as provided in Section 388.7 of the Regulations if a written demand therefor is filed with your answer; to be represented by counsel; and under Section 11(g) of the Act, to seek a consent settlement or an appropriate order to be issued against you.

Pursuant to Section 388.22, I am referring this matter to the Hearing Commissioner. Please submit your answer in accordance with Section 388.6, except that it should be addressed to the Hearing Commissioner, International Trade Administration, Room 3805, U.S. Department of Commerce, 14th Street and Constitution Avenue, N.W., Washington, D.C. 20230.

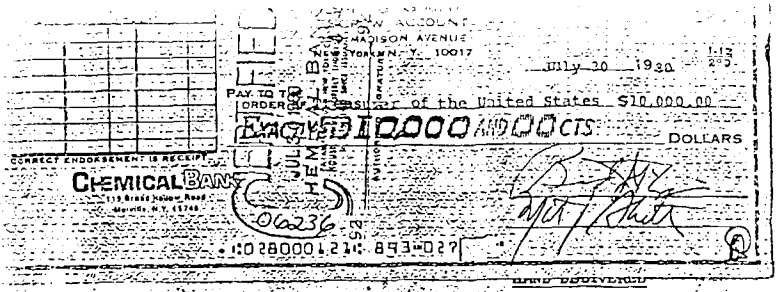
Sincerely,

Kent N. Knowles, Director
Office of Export Administration

Enclosures

cc: Comras/McClelland/Chrono/OEA/Case file 11(75)-20
cp:7/25/80 Wang #8529A

EXHIBIT NO. 12



Thomas C. Barbour, Esquire
Attorney-Advisor
General Counsel of the United States
Department of Commerce
Washington, DC 20230

Re: United States v. DeGeyter
Criminal No. 80-120-A

Dear Mr. Barbour:

I am in receipt of your hand-delivered letter of December 22, 1980, and the attached Order issued in the matter of Marc Andre DeGeyter by Eric L. Hirschhorn, Deputy Assistant Secretary for Export Administration, United States Department of Commerce.

In accordance with your letter and pursuant to the Order of the Deputy Assistant Secretary for Export Administration, I am enclosing herewith a certified check (per Mr. Cutner's July 31, 1980 transmittal letter, a copy of which is attached) in the amount of $10,000 drawn on the escrow account of Shea and Gould, and tendered by counsel for DeGeyter in accordance with the July 7, 1980 plea bargain agreement in United States v. DeGeyter, Criminal No. 80-120-A.

This letter and the attached check are being given to Special Agent Peter Comras, Compliance Division, United States Department of Commerce, for delivery to you.

Sincerely,

JUSTIN W. WILLIAMS
UNITED STATES ATTORNEY

By: Theodore S. Greenberg
Assistant United States Attorney

Enclosure

cc: David A. Cutner, Esquire

GENERAL COUNSEL OF THE
UNITED STATES DEPARTMENT OF COMMERCE
Washington, D.C. 20230

DEC 22 1980 DEC 24 12 16 PM '80

U.S. ATTORNEY'S OFFICE
ALEXANDRIA, VIRGINIA

Theodore S. Greenberg, Esq.
Assistant United States Attorney
Eastern District of Virginia
117 South Washington Street
Alexandria, Virginia 22314

Re: United States v. DeGeyter
Criminal No. 80-120-A

Dear Ted:

Pursuant to our telephone conversation, enclosed is a certified true copy of an Order entered by Eric L. Hirschhorn, Deputy Assistant Secretary for Export Administration, on December 19, 1980, assessing a $10,000 civil penalty against Marc Andre DeGeyter in accordance with the terms of the plea bargaining agreement signed by Mr. DeGeyter and you on July 7, 1980. In accordance with that plea bargaining agreement and the terms of the Order, payment of the $10,000 civil penalty is to be made by transfer of the check provided to your office by Mr. DeGeyter to the Treasury of the United States through the Department of Commerce.

Thank you very much for your assistance in this regard.

Sincerely,

Tom

Thomas C. Barbour
Attorney-Advisor

Enclosure

SHEA & GOULD

330 MADISON AVENUE

NEW YORK, NEW YORK 10017

(212) 661-3200

TELEX 423973

CABLE: HOLMANG

WILLIAM A. SHEA
BRUCE A. BECKER
JAMES J.A. GALLAGHER
BERNARD A. RUDICKI
HAROLD S. LYNTON
JULIAN B. SUSH
EDWIN H. JONES
RALPH L. EVANS
GEORGE DE LIENARD
SHELDON D. CAMMY
WILLIAM A. HAGAN, JR.
DAVID ALTER
KEVIN S. HORATY
WILLIAM C. FINNEGAN, JR.
ALLAN F. TESSLER
NORMAN A. BURSKY
THOMAS E. CONSTANCE
RAYMOND S. HARTMAN
ROBERT W. CLAESSEN
STUART HIRSHFIELD
DANIEL L. CARROLL
EDWARD J. MARTIN
MICHAEL CURLEY
JOSEPH C. GOMARD
EDMUND T. SLUPPLE
WILLIAM R. DUNLOP
PHILIP R. KAHN
LOUIS A. TROST
DAVID A. CUTNER
LEONARD W. WALLSTEIN, JR.
DAVID S. MARCOWITZ

MILTON S. GOULD
BENJAMIN BARTEL
BERNARD D. FISCHMAN
MARTIN I. SHELTON
SEYMOUR M. KLEIN
VINCENT D. MCDONNELL
ALLAN J. PARKER
ROBERT J. RUBEY
IRVING JACOBSON
SAMUEL W. INGRAM, JR.
MICHAEL ROTH
MICHAEL LESCH
LEON P. GOLD
VINCENT W. QUINN, JR.
RONALD H. ALCHESTER
ARNOLD S. JACOBS
IRA PORTEL
LESTER YABBY
JOEL I. PAPERNIK
ROBERT CUSRAS
JOSEPH FERRARO
RICHARD E. HALPERIN
FRANCIS P. POMAR
JOHN J. DUFFY
STRATFORD C. WALLACE
GEORGE T. HUTTON
RICHARD L. SPINOGATTI
ROBERT GOLD
HAROLD A. ASEL
IRA C. LAMBERT
ARTHUR S. KAUFMAN

JESSE CLINKING
FRANK E. BARNETT
MILES F. MCDONALD
SAUL P. STEIT
ARNOLD FORSTER
MAURICE S. DOLPHIN
OF COUNSEL

WASHINGTON, D.C. OFFICE
1037 A STREET, N.W.
WASHINGTON, D.C. 20006
(202) 833-9830
CABLE: HIRGO

WILBUR D. MILLS*
OF COUNSEL

MARIO V. MIRABELLI*
JUDSON A. BOULD*
WILLIAM A. NELSON*
RESIDENT PARTNERS

EUROPEAN OFFICE
47 BERKELEY SQUARE
LONDON W1X 5DB
ENGLAND
01-493-8513
TELEX: 298486

GEORGE E. BOSE*
RESIDENT PARTNER

ALBANY OFFICE
19 WASHINGTON AVENUE
ALBANY, NEW YORK 12210
(518) 449-3120

*NOT ADMITTED IN NEW YORK

July 31, 1980

BY HAND

Theodore S. Greenberg, Esq.
Assistant United States Attorney
United States Attorney's Office
117 South Washington Street
Alexandria, Virginia 22314

Dear Mr. Greenberg:

I have enclosed a certified check drawn on our escrow account and made payable to the Treasurer of the United States in the amount of $10,000. This payment is remitted by Marc DeGeyter in accordance with numbered paragraph 3 of the letter agreement dated July 7, 1980 among yourself, Mr. DeGeyter, myself, and John Schmidtlein.

Pursuant to the above agreement, I understand that your office will hold this check until such time as the Secretary of Commerce imposes a civil penalty against Mr. DeGeyter, which penalty shall in no event exceed $10,000.

Very truly yours,

David A. Cutner

U. S. DEPARTMENT OF COMMERCE

Washington, December 22, 19 80

I HEREBY CERTIFY that the annexed is a true copy of an Order issued in the matter of Marc Andre DeGeyter by Eric L. Hirschhorn, Deputy Assistant Secretary for Export Administration, on December 19, 19[illegible]

Compliance Division, Office of Export Administration
International Trade Administration

Sharon R. Connelly
Director, Compliance Division
(Official title)

RECEIVED
Dec 24 12 15 PM '80
U.S. ATTORNEY'S OFFICE
ALEXANDRIA, VIRGINIA

I HEREBY CERTIFY that Sharon R. Connelly
signed the foregoing certificate, is now, and was at the time of signing Director
Compliance Division
that full faith and credit should be given ~~his~~ her certificate as such.

IN WITNESS WHEREOF, I have hereunto subscribed my name, and caused the seal of the Department of Commerce to be affixed this 22 day of December, one thousand nine hundred and eighty

For the SECRETARY OF COMMERCE:

Tony Stelzer
Certifying Officer

USCOMM-DC 1889-P71

UNITED STATES OF AMERICA
DEPARTMENT OF COMMERCE

In the Matter of)
)
)
MARC ANDRE DEGEYTER)

ORDER

On July 7, 1980, the United States of America, by the United States Attorney for the Eastern District of Virginia, and Marc Andre DeGeyter entered into an agreement which, inter alia, contained the following provisions:

1. Defendant DeGeyter will plead guilty to one count of violating the Export Administration Act of 1969 (50 U.S.C. App. Supp.I, Section 2401 et seq., by counseling and inducing a violation of the Export Administration Act (15 CFR 387.2) by seeking to export the ADABAS source code ("technical data"; 15 CFR 379.1(a) and (b)(1)(i) and (ii) from the United States without the required export license (15 CFR 370.3(a); 379.2). . . .

2. For knowingly and willfully violating the Export Administration Act, Marc Andre DeGeyter consents to an administrative imposition of a $10,000 civil penalty by the Secretary of Commerce or his authorized representative pursuant to the provisions of 50 U.S.C. App. Supp.I, Section 2405(C)(1) and (C)(2)(B) and 15 CFR 387.1(b)(3). DeGeyter agrees to execute any documents necessary to said consent and collection of the $10,000 penalty.

3. Prior to the defendant's sentencing on the offense set forth in paragraph 1 above, the defendant is to deliver to the United States Attorney for the Eastern District of Virginia a cashier's check in the amount of $10,000 made payable to the Treasurer of the United States. This check will be held by the United States Attorney until such time as the Secretary of Commerce or his authorized representative imposes the aforesaid civil penalty. In the event that the Secretary of Commerce declines to impose the aforesaid $10,000 civil penalty, or imposes only a portion thereof, the cashier's check or an appropriate refund will be remitted to the defendant or his authorized representative.

On August 1, 1980, Marc Andre DeGeyter appeared in the United States District Court for the Eastern District of Virginia and entered a plea of guilty to a two count charge filed by the United States Attorney. One of those counts was the violation of the Export Administration Act and implementing Regulations referenced in paragraph 1 quoted above.

ACCORDINGLY, pursuant to the authority delegated to me by the Secretary of Commerce by Department Organization Order 10-3 (45 Fed. Reg. 6141, January 25, 1980), and International Trade Administration Organization and Function Orders 41-1 (45 Fed. Reg. 11862, February 27, 1980) and 41-4, effective August 26, 1980, I hereby find:

1. On August 7, 1979, Marc Andre DeGeyter knowingly, willfully and unlawfully counseled, commanded and induced an officer of Software AG to export the ADABAS source code from the United States to Belgium without obtaining a validated export license, in violation of the Export Administration Act of 1969, 50 U.S.C. app. §2401, et seq. (1976 and Supp.I 1977) and the implementing Regulations, 15 C.F.R. §§370.3(a); 379.1(a) and (b)(1)(i) and (ii); 379.2 and 387.2 (1979); and

2. Marc Andre DeGeyter has consented to an administrative imposition of a $10,000 civil penalty for the violation of the Export Administration Act and the implementing Regulations referenced in paragraph 1 of this finding.

IT IS THEREFORE ORDERED, that Marc Andre DeGeyter, within 20 days of the date of this Order, pay to the Department a civil penalty in the amount of $10,000. Payment of the $10,000 may be made by the Office of the United States Attorney for the Eastern District of Virginia out of funds provided to that Office by Mr. DeGeyter pursuant to the agreement signed by that Office and Mr. DeGeyter on July 7, 1980.

This Order is effective immediately.

Eric L. Hirschhorn
Deputy Assistant Secretary
for Export Administration

Entered this 19th day of December, 1980.

STATEMENT OF
DOUGLAS K. SOUTHARD
DEPUTY DISTRICT ATTORNEY
COUNTY OF SANTA CLARA, CALIFORNIA
BEFORE THE
U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
MAY 5, 1982

Senator Nunn, Members of the Subcommittee and Staff:

My name is Douglas K. Southard. I am a Deputy District Attorney for the County of Santa Clara, California. I have been employed by the District Attorney's Office, the chief prosecuting agency in that county, for a period of five years. Prior to that I practiced general civil law for a period of two years in a small law firm in the county. I am a graduate of Stanford University with a degree in Philosphy, and of Hastings College of the Law, the University of California, having attained a J.D. Degree in 1975. Like many people in law enforcement, I have no technical background in the area of semi-conductor manufacture or electronics in general, but have, of necessity, learned some of the basics of the industry which was necessitated by my involvement in high technology theft prosecutions. In the District Attorney's Office I have been assigned for a period of three and one-half years to felony prosecutions. For the last two years my primary assignment has been high technology thefts, including trade secrets thefts, integrated circuit thefts, electronic equipment thefts and the investigation and prosecution of related criminal conspiracies.

In learning the technical necessities of this area I have been greatly assisted by numerous people in law enforcement and in the industry itself; and particularly, have received training and assistance from Intel Corporation, Signetics Corporation, National Semiconductor, Synertek Corporation, Hewlett-Packard Corporation, and the NBK Corporation.

Investigation agencies with whom I have closely worked investigating and prosecuting these cases primarily have been the organized crime and criminal investigation section of the Santa Clara County Sheriff's Office, the Federal Bureau of Investigation, and the Santa Clara County Police Department, with notable assistance from the Los Angeles and Orange County Sheriff's Departments, United States Customs Service and the Department of Commerce. The preeminent police expert on these matters in our county is Detective Patrick Moore of the Sheriff's Office.

95-929 O - 82 - 31

In the last two years we have investigated literally scores of technology-related theft cases, resulting in numerous convictions, but also, sadly, numerous unsolved thefts or thefts wherein the property was never recovered.

Like you, we in local law enforcement are very concerned with the national security implications of the technology thefts that we have seen. However, as our expertise is in the field of investigating and prosecuting these crimes, and not in the international ramifications thereof, I will limit myself in my comments to the problem as seen by the local investigator and prosecutor and some suggestions as to where law enforcement has to go to help stem the tide.

First, however, I think it would be instructive to explain somewhat the integrated circuit manufacturing process and the history of the industry. I think this will help the Subcommittee understand the sophistication of the technology involved, the sophistication of the manufacturing process, and the areas in which security problems can arise. The focus of my presentation will be on integrated circuits themselves and not upon the finished products into which they are constructed.

Overview Of The Technology

A semiconductor is merely a description of the material from which integrated circuits are made. All integrated circuits, as we know them, are semiconductor integrated circuits. However, all semiconductor circuits are not necessarily integrated circuits. The concept of integration infers that large numbers of transistors or diodes or other electrical elements are combined together to perform a function. Large scale integration ("LSI") is now the norm.

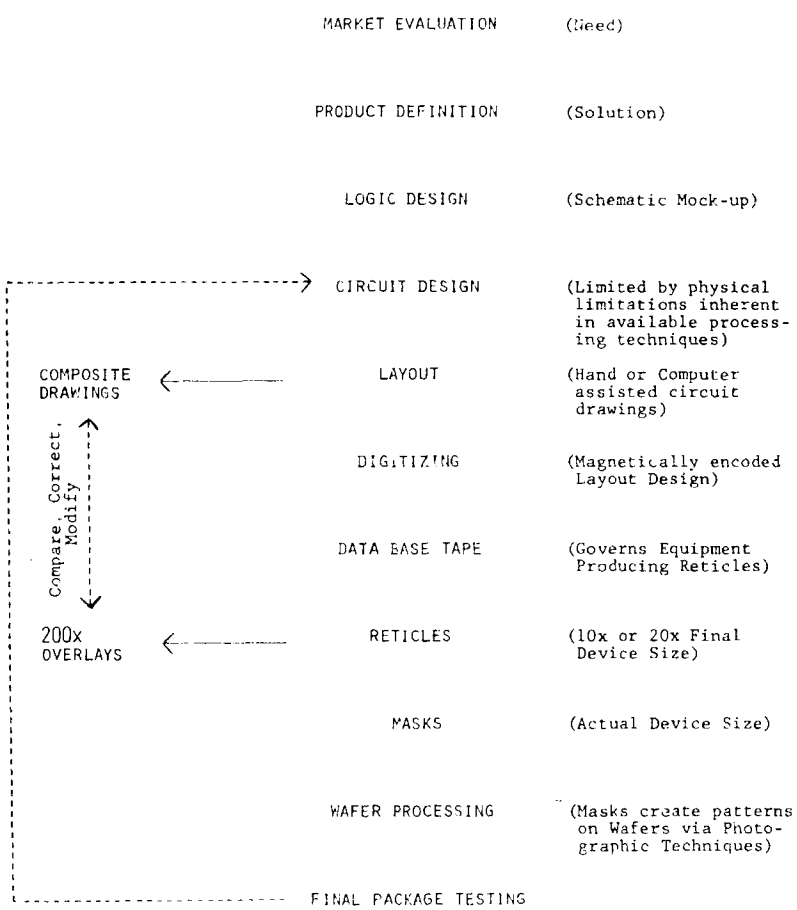
An integrated circuit is nothing more than a super miniaturized electronic circuit constructed on a substrate of silicon crystal. Silicon provides an ideal medium in that it has the electrical properties of both a conductor and an insulator. Like metal, silicon is cold, clammy to the touch, grey and semi-metallic in appearance. Like an insulator, such as glass, silicon is fragile -- it can be broken or chipped much like, for instance, quartz or obsidian. Because of its molecular structure, the addition of certain types of impurities to a pure silicon crystal structure can create free electrons which may alter its electrical properties. By adding these impurities, (such as phosphorus, boron or arsenic), which are often called "dopants" to the pure silicon crystals structure, in measured amounts, and at specific locations, the electrical properties can be altered in different areas of a silicon chip, giving one area an excess of electrons and another area a dearth of

electrons, so that current flow between the two adjacent areas can be induced with the appropriate input. Given these basic compositions, super-sophisticated geometries can be constructed by semiconductor engineers connecting hundreds or thousands of different "doped" areas in a particular fashion to achieve the result desired. These designs are three-dimensional in nature, interconnecting different layers of an integrated circuit device vertically with different areas horizontally. Horizontal and vertical connections are made by alternatively photo-lithographing circuit designs upon the silicon and building up layers in the silicon by exposure to corrosive chemicals which cause the silicon, in effect, to grow.

The net result is a three-dimensional electronic circuit as small as one-quarter inch square or as large as an inch square which may contain anywhere from four thousand to hundreds of thousands of transistors or other electrical devices. For instance, a "2114" type integrated circuit, which is a relatively simple memory device, has the capacity of retaining four thousand bits of information, that is four thousand binary encoded memory units. The memory portion of the chip alone will contain approximately eight thousand transistors and the entire chip ten to twelve thousand transistors. This particular chip is a very basic chip which is quickly becoming outmoded and serves as a building block upon which computer systems or other electrical systems can be constructed.

Design Process

The product flow of a typical integrated circuit device can be graphically summarized as follows:



The market evaluation and product definition stages define the need and the envisaged solution to the problem. This is followed my meticulous design work culminating in a layout either drawn by hand or computer aided design equipment. The resulting design is then "digitized" by translating its physical dimensions and qualities into quantifiable data which are encoded by a computer onto a memory tape, called a data base tape. This tape can then be used, with some intermediate computer language translations, to run special machinery which creates reticles. Reticles are groups of glass plates, one for each layer of the final chip, which have the layer designs very precisely photographed upon them. From the reticles, by use of a step and repeat camera, are made the chromium masks with which the wafers are actually processed. Each mask has scores of circuit layers upon it, each exactly the same. Usually the mask actually contacts the wafer to print the circuit design upon it.

As is indicated on the diagram, constant design re-evaluation goes on, leading to continual upgrading of designs.

Any person who was able to steal or otherwise acquire a data base tape, reticle or mask set for a given product would have tools incorporating the original designer's trade secrets, arrived at only after hundreds of thousands, even millions, of dollars in design effort. With these tools an unscrupulous competitor could undercut the original designer's prices and compete with him almost overnight. Although basically the same data could be obtained by "reverse-engineering" a chip purchased on the open market, such a process is expensive, time consuming, and less precise than stealing the original designs.

Manufacturing Process

The actual manufacture of the integrated cirucit is a very complicated process, which is difficult to understand for someone like myself who is not very well versed in physics and chemistry, but I think we can describe it in such a fashion that you get a feeling for it. I have brought some samples of the items to be discussed to aid in understanding the technology.

First of all, an integrated circuit is a micro-miniature structure comprised of several key materials. The basic material is highly pure, single crystal silicon. The process starts with a single silicon crystal called a seed crystal. The seed crystal, like the yeast in French bread, is sort of the magic ingredient. It is a pure silicon crystal which is dipped into an essentially rotating vat of liquified silicon, and is extracted under a controlled rate so that the molten

silicon material adheres to it and grows upon it. The result of this process is a long sausage-like poly-silicon ingot, with an almost perfectly pure crystal lattice structure, consistent throughout the entire ingot.

The ingot is then sliced into thin round silicon wafers. After the wafers are polished they are subjected to a diffusion and photo-lithography process which imprints the completed circuits upon them. Each wafer, approximately three to four inches in diameter, can be imprinted with hundreds of individual circuits for rectangular chips, each of which is essentially identical to the other.

The diffusion process consists of placing the wafers into furnaces at very high temperatures in different gaseous atmospheres containing the desired dopants. By this method oxide layers are grown on top of the wafers. This is really just a very accelerated and sophisticated "rusting" process such as we are all familiar with. These deposits are called epitaxial growth.

Each diffusion or oxidation step is then followed by a photo-lithography step.

The patterns lithographed upon a wafer are introduced through the use of several successive masks and processed very similarly to the taking and developing of pictures. The process requires a very clean, particle-free environment containing much complex and expensive processing equipment. Patterns on masks are projected into an emulsion film on the wafers from a light source with a machine called a "projection printer." The picture of the mask on the wafer is developed through regular "dark room" developing techniques, the purpose being to delineate areas from which to remove the unwanted portions of the deposited silicon or metal. This is in turn done by use of suitable acid rinses, which etch away unwanted materials. After each acid etch a long rinse in very pure water is necessary.

Under newer processes ion implantation is used instead of or, in conjunction with diffusion. With this method, ions are literally shot into the silicon wafer by an ion beam generator. Laser etching equipment is also now coming into general use.

The process continues in successive layers, sometimes as many as eight or ten layers thick. Although the variables are many, the process is basically the same for each successive layer: diffuse (grow oxides), photo-lithograph the circuit pattern, etch, then repeat. The final layer, called the "metal mask," is an aluminum film which interconnects all the vertical and horizontal geometries

within the design. This is the layer that is most visually apparent when looking at the chip.

All this construction is done in a micro world that approaches the size of bacteria. For instance, a common dimension of a typical circuit "wire," if you can call it that, may be as small as four microns -- that is, four millionths of one inch.

All of this, of course, is done by super sophisticated equipment and trained personnel in highly controlled atmospheric conditions. The designs themselves, and the processes which are used to grow the layers on the chip, are the result of years of design and re-design effort, leading finally to a design which not only is workable but is makable, given the physical and technical limitations of the manufacturing technology of the day.

After the chip manufacture process, the chips are separated from each other by cutting up the wafer with special machines, so that each rectangular individual chip may be encased in a protective housing and connected to the outside world by means of precious metal leads that go to the familiar pins that plug into printed circuit boards. Prior to doing that, of course, there is laborious, painstaking and precise testing process wherein each individual chip is electrically tested for defects. The defective chips are marked and ultimately discarded, usually for later reclamation of precious metals.

The resulting chip is a high-reliability product which will perform in adverse conditions for a substantial period of time without failure. Internally the chip has no wires to come loose, no terminals to corrode, nor any other of the physical attributes of traditional electronics devices which make them susceptible to malfunction. Moreover, the incredible miniaturization achieved makes it possible to literally construct a computer on a chip, and therefore make it available for applications not previously dreamed of.

The variety and types of chips produced in this fashion are limited only by the imagination of the engineers. The two basic types involved are: memory chips, which can be broken down into numerous sub-categories depending upon the type and properties of the memory and the input-output capabilities it has; and micro processors, which are the commonly referred to "computers on a chip." They are central data processing units designed to work in conjunction with other chips (for instance, memory chips) to process information.

The applications of these chips are likewise as diverse as man's imagination. They can be used in everything from digital watches to auto emission

control systems; video games to intercontinental ballistic missile guidance systems; desk top computers to smart bombs and cruise missiles. This technology presents such significant opportunities for the human race, that it may be the most significant advance in technology since the industrial revolution. With it, we are anticipating a quantum leap in man's ability to do tasks that need to be done.

Brief Industry History

The integrated circuit was invented in the late 1950's. Commerically useable integrated circuits, known as "I-C's" in the parlance, were first available in 1961. The technology expanded rapidly and in 1971, a then small Santa Clara company produced an entire computer on a single silicon chip. The computer on a chip, technically called a micro processor or micro computer is revolutionizing the electronics industry. As certain periodicals have recently pointed out the micro-computer chip will have more impact on our society in the next twenty years than any other invention. Already the micro-computer is being used in microwave ovens, refrigerators, electric ranges, cash registers, taxi meters, gas pumps, typewriters, television, computers and military applications. By the end of this decade we may expect that they may be found in virtually every home and business.

The integrated circuit was a uniquely American development. It was first marketed in 1961, and integrated circuits are now already more than a five billion dollar world-wide industry. Only over the last five years or so has foreign competition become substantial factor in the state-of-the-art, leading edge portion of the business. The micro-computer started from nothing in 1971. Recently sales were in the range of half a billion dollars, and are expected to grow at approximately fifty percent annually for the foreseeable future.

Continued development of integrated circuit memory chips has reduced the cost of information storage in computers a hundred fold in the last ten years. In the late twentieth and early twenty-first centuries integrated circuitry will be as basic to an industrial economy as steel in the nineteenth and early twentieth centuries. Leadership in this technology will be vital to any nation that would be a world leader in economic and military power.

In the wake of this new technology has sprung an industry centered in what has come to be known as "Silicon Valley," Santa Clara County, California, which is among the most fast-moving and competitive in the world. Any individual who can build a better electronic mousetrap using this technology has potential

immediate access to great wealth and recognition. Companies spring up over night, based upon one good idea and sometimes die just as quickly when that idea is overcome in the marketplace by new and better ideas. The leading semiconductor manufacturers in the country and in the world are often companies who did not even exist fifteen years ago and have literally gone from a backroom type of operation started in somebody's garage to a billion dollar corporation in the space of ten or fifteen years. Up to now, in my view, the rapid growth of these companies has prevented a proper assessment of their security operations and has caused a substantial lag in public and official appreciation of the national secuirty implications of the new technology.

According to available evidence, in the past five years probably one hundred million dollars or more in electronic technology and product has been stolen in the Santa Clara County area alone. We in law enforcement have only recently, within the last three years, almost stumbled across the problem. At the time we were totally unprepared to deal with it. Now we are beginning to make some headway.

What follows is a summary of some of the cases we have dealt with, the problems we have encountered, and some suggestions aimed at strengthening law enforcement's position.

Silicon Valley Thefts

In recent years increasing press coverage of high technology thefts has gained the headlines across the country, and particularly in Silicon Valley, Santa Clara County, California, where high technology electronics is centered. So what's all the fuss about? In the last five years I would estimate that in excess of a hundred million dollars of technology and products have been stolen, illegally copied or counterfeited from Silicon Valley firms. Most of that theft is by employees. The cases we handle involve technicians, inventory clerks, draftsmen and engineers. Quite commonly, security personnel are also involved. They steal circuit designs, process information, precious metals, and the chips themselves. There is also an increasing propensity to stealing finished goods, such as computer disc drives, and personal computers which have become increasingly smaller in size and therefore more easy to steal.

This is not difficult to do. A complete set of glass reticles, which are essentially production tools incorporating all details of a sophisticated new circuit design, can be taken out of a plant in one's coat pocket. The same would apply to a

computer tape describing all details of the design. When a sophisticated new circuit design may have cost as much as a half million dollars or more to research, develop and engineer through the manufacturing stage, these items become increasingly attractive targets of crime. With these reticles or computer tapes, and available production technology, a competitor could go into direct competition within a few months, undercutting the original firm's price because of less capital investment. Where a company or country has not developed technical expertise to actually design these products effectively from scratch, as is the case in Eastern Europe, the availability by theft of proprietary product designs makes the establishment of semiconductor manufacturing possible where it otherwise might not have been.

The "Gray Market"

The most common problem, however, is much more crude and direct. An employee can take out one thousand high priced, high demand chips selling for as much as one hundred dollars each in his briefcase, the lining of his jacket or in his lunch bag. He may sell them for five to fifty cents on the dollar to one of the numerous fly-by-night independent distributors operating out of low rent office suites, their homes, or even the back of their cars. Usually no questions are asked. Independent brokers are not about to share with their customers the source of their product, as the customer could then go directly to the source and cut the broker out of his percentage.

As often as not the buyer purchasing stolen parts is an otherwise respectable appearing businessman, who either uses his business as a front for criminal activity or just can't pass up the opportunity to make some fast money. In one recent case in Santa Clara County, resulting in a conviction of two persons, an undercover officer offered to sell to a local distributor purportedly stolen Intel memory chips which were then in very high demand. The officer flat out told the defendants that the chips were stolen. After snapping up the parts for $10,000.00 cash, the common method of payment, the defendants the same day shipped the parts via air freight to Werner Bruchhausen, a notorious international chip broker in Germany. Bruchhausen is widely reputed to be a Soviet East German agent, is under indictment by a federal grand jury in Los Angeles, and is currently in the custody of the German federal police. This transaction was in violation of federal export control regulations prohibiting such transactions without prior approval because of the military applications of these products.

Now the principal here was no back-alley crook. He had a fine home in one of the exclusive hillside residential areas in Santa Clara County. He and his beautiful wife drove Mercedes and sent their kids to the best private schools. He was an armed forces veteran and a member of the reserves. He was president of a successful parts distribution firm and all in all a typical American success story. And yet, here he is selling stolen integrated circuits to an internationally known fence. The reason is the same as always, greed. This kind of greed is not unusual in the context within which he worked: Silicon Valley, a prime example of capitalism on the rampage. Everyone wants to become an overnight millionaire and money flows like water, tempting the otherwise honest citizen to scramble fast to get his share of the pie.

Greed has spawned what is often called the "gray market". To understand what the "gray" market is one must understand the hierarchy in electronics commerce. The manufacturers such as Intel, National Semiconductor, Texas Instruments, Signetics, Synertek and others, actually create the technology and design and manufacture the integrated circuits for later use in a variety of electronic equipment. At the end of the line is a customer such as Burroughs, General Electric, Westinghouse, Siemons of Germany, or any of the numerous defense contractors in this country.

In between are the middlemen. At the top of the distribution heirarchy are the so-called franchised distributors. These include such companies as Elmar Electronics, Hamilton-Avenet, and Western Microtechnology, which have continuing written contracts with various manufacturers to represent them and sell their parts in the market place. Major customers deal directly with the manufacturers, but franchised distributors take up the production slack and provide the means to connect supply with the demand by locating the demand. These are reputable firms who prize their business name and deal only in first line products. No evidence of false or fraudulent dealings or dealing in stolen property, by these companies, has ever been brought to my attention.

Down line from the franchise distributors are the so-called independent distributors. They obtain their product either directly from the company which manufactures it when surplusages occur or from franchised distributors or from such other means as might be available. Other means might include, and often do include, purchasing surplus inventory from the end users. Because of the volatile nature of the market, the end user customer will often find itself in a situation

where it has a surplus of parts. It might, for instance, have purchased large numbers of scarce parts which had been allocated to it by the manufacturer as a hedge against a rainy day. It may not have needed the number of parts it had allocated to it, but purchased them anyway to insure that it had a supply so that its production would not be interrupted. Down line if demand fell off the need for this inventory evaporates and the customer finds himself with a "white elephant" inventory, which often he is eager to dispose of quickly for cash. Or a customer might purchase inventory in preparation of a new product introduction and then scrap the product, leaving itself again with a surplus of unneeded parts. These too would be sold in the independent distributor market.

Another source of parts for the independent distributor is used parts. Numerous types of products incorporate printed circuit boards into which the integrated circuits themselves are literally plugged. As customer needs change sometimes the old printed circuit boards are scrapped and new ones with more updated capabilities replace them. Again, surplus parts are now available and are often sold at low rates in the independent broker market. Because of the basic reliability of integrated circuits, used integrated circuits are often quite reusable.

What is created by this system is an "anything goes" marketplace where, especially in times of high demand and short supply, such as occurred in the 1977 to 1980 time frame, speculation runs rampant. It's really no different from pork belly futures. Brokers buy large quantities of parts at fire sale prices, hoping to be able to turn them over quickly if a need is found elsewhere. Numbers of these people made a lot of money doing just this sort of speculation during the parts shortage of 1977 to 1980.

Gray Market Case History: Larry E. Lowery

Larry E. Lowery first came to the attention of law enforcement in January 1978. In that month an employee at Elmar Electronics, a franchised electronics distribution house in Mountain View, California, was cautiously approached by a fellow employee, Paul Hernandez, about the possibility of stealing integrated circuits from Elmar's warehouse. The employee alerted police and cooperated in an undercover investigation. Hernandez was observed to steal one hundred thousand dollars worth of late model circuits and transport them to David Henry Roberts, who in turn delivered them to Larry Lowery's house, where Lowery's wife paid Roberts. Larry Lowery was at the time away in Las Vegas. Roberts and Hernandez were arrested, but due to a series of mis-cues by law

enforcement their cases were dismissed by the courts. Neither would testify against Lowery, and Lowery's wife claimed marital privilege. Lowery, therefore, escaped prosecution.

Through investigation it was learned that Lowery operated a company called L. & M. Electronics in Mountain View, California, and had since mid-1977 successfully solicited electronics thefts, via Roberts, on a continuing basis.

In early 1979 Roberts was again arrested and convicted for two integrated circuit thefts perpetrated by forged invoices written on his employer's account. Again he named Lowery as his instigator and fence, but police were unable to acquire evidence other than Roberts' statement with which to prosecute. It's interesting to note that Roberts' employer was unaware of Roberts' previous criminal activity.

In April 1980, it came to the attention of the Santa Clara County Sheriff's Office Organized Crime Unit that a large quantity of Synertek Corporation's E-prom type circuits, then in high demand, were being offered for sale by a local independent broker. An undercover investigation was initiated which ultimately led to the arrest of Lowery, and the search of his business premises. By now he had changed his business name to Brut Electronics. Over eleven thousand stolen Synertek integrated circuits valued at between one hundred and one hundred and fifty thousand dollars were seized. Search warrants also led to the seizure of his business records and the records of a "paper company" used by Lowery called O.C.S.

Leg work and forensic examination disclosed that the records relating to Lowery's acquisition of the stolen Synertek parts were phoney. Handwriting experts determined all were authored by David Roberts, although they purportedly showed transactions with numerous different companies. Innumerable hearings and motions followed Lowery's arrest. Prior to the preliminary hearing a prosecution witness was lured out of his home, attacked and severely beaten by a total stranger. He was therefore unable to testify at that hearing. On the eve of a jury trial, Roberts, then under subpoena by the prosecution, was murdered execution-style, and his body dumped in a shallow grave in the Santa Cruz mountains.

After six weeks of trial, necessitated by execessive technical testimony, Lowery was convicted on November 2, 1981 of knowingly receiving stolen property. He was allowed to remain free on bail pending his sentencing. On January 18, 1982,

Lowery was sentenced to two years state prison and remanded into custody by the judge.

On Thanksgiving weekend 1981, while Lowery was still free on bail after his conviction, Monolithic Memories, Inc., of Sunnyvale, California suffered a three point four million dollar theft, notwithstanding extensive electronic security measures and twenty-four hour security personnel. The theft was undetected until workers returned from the long Thanksgiving weekend. Many of the circuits taken were reportedly specially designed units with direct military application. In all, about a ton of boxed first line parts were taken, necessitating at least two truck loads to make off with all the booty.

It was quickly determined that this had to be an inside job in that somebody with knowledge of security measures would have to have disconnected, or otherwise rendered inoperative, electronic security measures which included perimeter alarms, closed-circuit television, ultrasonic motion detectors and locked-cage part storage areas. Lie detector tests were given to various security personnel who had worked shifts coinciding with the theft. One security guard, Ronald Washington, notably failed the polygraph test, but was informed that he passed, in hopes he would be put off his guard by that information.

Soon thereafter an acquaintance of Washington's, lured by the $50,000.00 reward offered by MMI, contacted MMI and law enforcement authorities, with information regarding the case. It was learned that Washington had bragged about having participated in the theft and stated that he was using the $7,200.00 payment he had received for his part in the theft to finance his fledgling cocaine sales business.

An undercover operation was initiated wherein an experienced narcotics officer was introduced to Washington and proceeded to purchase cocaine from him on five occasions. During the course of the conversations attendant to those drug purchases, further statements were made by Washington incriminating himself and others. He described the "big man" in the theft operation in such a manner as clearly described Larry Lowery.

After weeks of negotiations with Washington the undercover officer told him that he had a friend who would soon be quitting Synertek, a local integrated circuit manufacturer, and who wanted to make one last killing by stealing parts from his employer before moving east. A sting operation was thereby initiated wherein a half million dollars in stolen Synertek parts were offered to Washington

and Washington's superiors. A purchase date was set up and bait parts were acquired from Synertek for the operation.

On February 24, 1982 the operation went into effect. The plan was to deliver the purportedly stolen parts to Washington and his confederate and to tail them as they delivered them to the broker for whom they were purchasing the parts. The operation was partially successful in that Washington, Abel Urbina and third individual took delivery of the parts, but did not take them immediately to their broker's location. They were monitored in regular telephone communication with the leader of their operation, but waited to have the entire delivery made before taking them to their storage location. Because Synertek was understandably unwilling to risk a half million dollars worth of parts to the undercover operation for fear the thieves might get away with them, the officers were unable to complete the operation according to plan.

The three subjects were arrested and evidence was seized implicating both Larry Lowery and his partner, Larry Kizer. One of the vehicles used by the three young thieves was Larry Lowery's personal Lincoln Continental automobile, registered in his name. The other vehicle, a truck, was owned by a Nevada Electronics company run and owned by Larry Kizer. Subsequent search warrants revealed numerous business documents in Brut's (that is, Lowery's) business premises showing Kizer's relationship to Brut and Lowery. Telephone records were seized, pursuant to warrant, which indicated that at the very time of their arrest the three arrestees were talking to Kizer in Nevada on the pay phone in Santa Clara County. To date, despite extensive efforts by law enforcement, the parts themselves have not been located or recovered. It is feared that they may have already been transported overseas, most likely to a European location.

To date, the trail of investigation is littered with dead bodies, assault, sophisticated thefts, drug sales, and more. Scores of criminal conspirators appear to be involved. It represents the clearest case of consistent, habitual, organized criminal activity aimed at Silicon Valley as yet uncovered. Because of the complexity of the case and the circumstantial nature of the evidence available, it would be a very difficult task to fully prosecute and bring to justice all of the people involved. Undoubtedly it will take years before the investigation is completed and prosecutions culminated.

Gray Market Case History: John Jackson

John Jackson, when he first came to the attention of Santa Clara County law enforcement officials had previously been convicted five times elsewhere of felonies involving theft, forgery and theft by false pretences. He had never been sentenced to state prison for any of these offenses.

In November 1979, around Thanksgiving time, Intel Corporation suffered a theft of approximately one million dollars worth of "2732" E-Prom devices. These were at the time state-of-the-art memory devices in very high demand throughout the world. They were capable of holding thirty-two thousand bits of binary information in the memory and of being erased and re-programmed at will by the user. This combination of memory capacity and flexibility made them a standard memory unit around which such devices as main-line and desk-top computers were built.

After the theft, corporate investigators had no leads as to how the items had been stolen. Shortly thereafter, however, in December 1979, it came to the attention of Intel employees in Europe that a large number of 2732's had surfaced there. Specifically, Siemons AG of West Germany, a huge electronics manufacturer and one of Intel's best customers, had apparently just received a large shipment. At this particular time these particular items were in such short supply, and in such high demand, that Intel was using a rationing system whereby preferred customers were allocated a monthly allotment of parts based on various criteria. Siemons was among Intel's highest allotment consumers, receiving one to two thousand of these parts per month.

Within a short time Siemons began to notice a high failure rate of Intel 2732's it had purchased in a bulk. Siemons contacted Intel to complain. Samples of the questioned chips were sent to Intel in the United States for analysis. Forensic analysis disclosed that the devices in question, had in fact, been counterfeited. Although they were authentic Intel parts, they had been forged with falsified Intel part numbers, logo and markings. The reason for this was that the ten thousand 2732's stolen in the November 1979 theft had not yet been marked. The marking of a device with the logo and part number is the last stage in the final testing and quality assurance process. The parts that had been stolen had not yet reached the final phase and had in fact not finished the testing process. As a result of that, a substantial number, perhaps thirty percent, were parts that would not have passed Intel's strict quality control standards. Thus, in use by Siemon's customers equipment had begun to fail.

After putting some pressure on Siemons, Intel learned the source of parts in question. Siemons, had purchased a bulk lot of approximately ten thousand parts from E.B.V. Corporation of Munich, West Germany. Further pressure was brought to bear on E.B.V. and the admission was made that it had received parts from two sources: Republic of Virginia in Arlington, Virginia, another parts broker, and Mormac, Incorporated of Torrance, California. Until the execution of search warrants on these premises in February 1981, the trail had grown somewhat cold and no further back-tracking could be done.

A break in the case occurred in January 1980 when an anonymous telephone informant informed police that John Henry Jackson lived at a specific location with a house and garage full of stolen integrated circuits. An undercover investigation led to the issuance of a search warrant, the seizure of thousands of stolen integrated circuits, and Mr. Jackson's arrest. However, the case was later dismissed after the judge found the search warrant to have been issued based upon improper evidence.

In the course of investigating the case, however, law enforcement officials contacted employees of Jackson who provided information linking Jackson to improper dealings with integrated circuits.

It was learned that Jackson had been in business as a printed circuit board "stuffing" house and aspiring computer maker, with a parts brokerage business on the side.

Another employee of Jackson's came forward, spurred in part by continuing revelations in the press regarding the seriousness of the stolen chip problem. This individual literally walked into the investigator's offices and plunked down upon their desk an assortment of printing plates which he stated he had used while in Jackson's employ to counterfeit Intel integrated cirucit devices. Further forensic analysis was done comparing the printing plates provided by this informant to the printing on the confirmed stolen parts recovered from Siemons in Europe. The printing plates matched the printing on the stolen devices.

This witness told of having been hired by Jackson for a menial job and being induced by him into participating in his chip marking and marketing operation. In the period of less than a year that he worked for Jackson he had marked tens of thousands of integrated cirucits, primarily Intel 2732's and 2716's. He provided information corroborated by another Jackson employee that Jackson had been doing business in large part with the firm of Mormac in Los Angeles, and

in particular an individual by the name of Patrick Ketcham. Ketcham had previously been convicted in a federal court in Los Angeles in another forgery scheme wherein parts acquired on the open market were falsely represented and documented to meet the stringent military specifications required by the Department of Defense. At the time of the Jackson investigation, Mr. Ketcham was still on probation for that offense.

With the cooperation of this informant the Sheriff's Department and Intel Security set up an undercover operation whereby the informant continued to work for Mr. Jackson, marking with counterfeit markings stolen Intel parts and informing the police of their disposition. After one such counterfeiting session, an associate of Jackson's was arrested in Long Beach, California, attempting to sell the parts to a broker at that location. At that point, in February 1981, law enforcement officers arrested Jackson, Ketcham, and one of Jackson's associates, a former Intel employee. This employee had, according to both informants, been seen to deliver Intel parts to Jackson's business premises on multiple occasions. On one occasion the parts were delivered in the lining of the subject's leather jacket. The subject, in fact, had worked in a area of Intel, a Reliability Testing area, where he had access to the stolen 2732's and stolen 2716's. Intel business records reflected that the subject had signed in on the "off hours" signing sheet on one of the days of the Thanksgiving weekend in which the ten thousand 2732's were stolen.

Concurrent with these arrests, extensive search warrants were prepared and served on Mormac, Space-Age Metals, Jackson's business and home, and on Republic of Virginia, the parts distributor in Arlington, Virgina. No business records were discovered memorializing Jackson's role in any of these transactions. However, the business records of Space-Age, Mormac and Republic clearly indicated that shortly after the theft in November 1979 or early December 1979, Space-Age Metals sold Mormac five thousand Intel 2732's and sold Republic another five thousand 2732's. Mormac and Republic in turn each sold all of those parts to E.B.V. in West Germany, from which they went to Siemons. All of this in the space of approximately one and one-half months after the theft. In one business letter discovered at Space-Age Metals a Republic vice president told a Space-Age official that he was amazed at the quantity and price that was being offered for these parts given the scarcity of the parts in the marketplace, but that he wanted to close the deal and wasn't stupid enough to ask any questions.

The Jackson case is still pending trial. Charges against Patrick Lyle Ketcham were dismissed due to insufficient evidence that he had actual knowledge that the parts received by Mormac were stolen. Although the informant witnesses had initially linked Ketcham directly to receipt of large quantities of integrated circuits, in the relevant time-frame, subsequent investigation proved that Ketcham in fact had received the five thousand parts in November and December of 1979 from Space-Age, not Jackson. In fact, at that particular time Ketcham's relationship with Jackson was strained because Jackson had provided him with so many sub-standard parts. Charges against the president of Mormac, one of Ketcham's associates, were also dismissed for lack of evidence of personal knowledge on his part. Charges against Space-Age Metals or any of its employees or officers were never filed. No direct evidence of whom in that organization was responsible for the acquisition of those parts was ever found.

The Jackson case points out the difficulty of proving knowing receipt of stolen integrated circuits. Although the various business records of the affected companies, mainly Siemons, E.B.V., Republic, Space-Age, and Mormac, indicate transactions amongst them in Intel 2732's during the relevant time-frame, it is impossible to prove which Intel 2732's were actually involved in the transactions. Once the parts actually got to E.B.V., all were incorporated into products which were later sold. Only a handful were actually extracted and preserved by Siemons after defects began to be discovered. Siemons wasn't about to recall all the finished products into which these chips might have been incorporated just to rip them apart to find stolen chips. As a result the web of circumstantial evidence becomes strained. Direct evidence is simply not forthcoming. The records-keeping systems employed by the brokers are not sufficiently specific to be able to trace the particular part. Nor are knowing thieves likely to keep such records.

Finally the cost for such a prosecution would be almost prohibitive for a local jurisdiction. The estimated costs of producing the minimum one dozen witnesses from Europe and the East Coast necesssary to prove the evidentiary chain in the Jackson case is in excess of the entire witness budget for the County of Santa Clara for an entire year. Public safety considerations simply will not allow property crimes prosecutions to take precedence over violent crimes prosecutions.

Modes of Thievery And Problems Of Prosecution

The most common means of theft involve company employees. They are the following types:

(1) Finished Goods Thefts: Usually these are from warehouse or storage areas, although armed robberies and truck hijack thefts have also occurred. Usually the storage area has some sort of security, sometimes including elaborate electronic measures. A determined thief, however, can usually defeat these systems without detection. The common denominator here in the intent to resell the stolen product in the "gray market."

One of the primary difficulties investigators face is the identification of the stolen product. Integrated circuits are fungible goods without clearly traceable identification markings. Usually the devices bear a manufacturers' logo, part number, and bottom-side markings indicating place of manufacture (usually overseas, mostly in Southeast Asia), and a date code. Some manufacturers also mark the parts with lot numbers, identifying a part as being one of a finite group of parts (usually a few thousand) which were processed at a certain place and time.

Lot numbers provide the minimum amount of identification necessary for law enforcement to be able to trace back stolen parts. Some manufacturers have also resorted to the use of chemical taggants in their printing inks, much as the Bureau of Alcohol, Tobacco and Firearms has required of gunpowder manufacturers. Unfortunately, limited experience has shown that these additives can interfere with the electrical functioning of the part.

Another problem is sloppy inventory control. Many of these companies have grown so quickly that proper inventory tracking policies have not been insitituted. Company philosophies emphasizing speedy, inexpensive

production and quick product turnover are not conducive to accurate record keeping. On numerous occasions stolen chips have been recovered and confessions given, when the company involved can't even prove anything is missing! With many products substantial inventory shortages have become so common that the companies have just given up and accepted the losses as normal inventory attrition which is factored into product planning.

Apparent lack of commitment to reasonable security goals also thwarts detection of theft. To many companies the security department is a bastard stepchild which is always well down on the list of priorities. Apparently it is felt that security costs more than it's worth. As a result, many crimes are never detected or, if they are, are not reported. It's interesting to note that a number of the largest companies have, to my knowledge, never reported any integrated circuit thefts. Others report them only when a thief is caught red-handed. Yet companies which have made a substantial commitment to improved security, especially Intel and Signetics Corporations, which have their own full-time corporate investigators (as opposed to just security managers), have regularly reported, investigated, and actively prosecuted thefts. Given the number and seriousness of the thefts that are reported by such companies, one can only conclude that the other companies are either unaware of or do not report their own thefts. One can hardly conclude that a company with tens of thousands of employees suffers no thefts.

The ironies that occur as a result of this lax attitude are worthy of note. On one occasion Sheriff's detectives warned one of the largest manufacturers that, based upon intelligence information, a major theft was planned for a specific date in the near future. The potential thief, a

convicted murderer, was identified. Although the theft was thwarted, the thief was not fired, and reportedly still carries out a thriving cocaine business.

Almost every time we serve a search warrant on a chip black marketeer we find integrated cirucits made by one large manufacturer, without appropriate paperwork accounting for its acquisition. (The situation appears so hopeless we don't even bother to try to determine if it's stolen or not).

At another company, the security manager had evidently been a thorn in the side of management for some time, since he continually decried the lack of funding for the security department, warning that this prevented him from doing his job properly. When a substantial theft occurred, management's response was to effectively disband the security department and decentralize security by transferring those responsibilities to the unit managers of each production unit, thus multiplying the opportunities for corruption.

(2) Unfinished Goods Thefts: Integrated circuits can't be considered finished goods until they have not only gone through the actual manufacturing and assembly process, but also have been thoroughly tested. The testing process is vital to the reliability of the chip, and serves to cull out sub-standard parts (which do not meet the manufacturer's published specifications), and grade those parts which meet or exceed specifications.

Almost all United States semiconductors actually design and fabricate the semiconductor chips themselves in their U. S. facilities. This is a capital and technology intensive enterprise requiring a relatively skilled labor pool. After chip fabrication on the wafers and initial electrical testing, however, the wafers are usually sent to overseas plants. Here they are sorted and fabricated into the actual protective plastic package which contains the chip. The chip is placed in the package and connected by fine aluminum or precious metal wires to the external pins which are ultimately used to plug the device into a printed circuit board.

These operations are relatively labor intensive, and the low wage rates overseas, especially in Southeast Asia, make it cost effective to do this work there.

At this point the fully fabricated but untested devices are shipped back to the United States for final testing, quality assurance work, and then marketing. The industry practice is not to imprint the devices with logo, device type or lot numbers until stateside final quality assurance testing is completed. Thus, any unmarked part is presumptively either a reject or an untested part.

Since there can be an much as a 30% to 40% rejection rate at this stage, especially for the more complicated devices, a good number of bad parts have to be disposed of in some fashion. This is normally done by a reclamation process which involves grinding up the parts in a shredding machine and flushing out the precious metals in an acid bath. Although some companies maintain their own reclamation facilities, most sub-contract this task out to metal reclaimers. Varying degrees of security are used to insure the parts are in fact ground up.

These measures are taken because the manufacturers want to maintain a reputation for quality. One obviously doesn't sell defective products with one's logo on it. Nor would a company normally want to put its unmarked rejects on the market. They could easily have counterfiet markings printed on them, and be sold as good parts. The resulting warranty claims and injury to reputation would be costly. As a result, the manufacturers almost uniformly maintain a policy of not selling unmarked or reject parts. Thus an unmarked part should be presumptively stolen.

If this were in fact the case, law enforcement's job would be easier. Unfortunately, the truth is more complicated. Many parts which do not meet specifications and are therefore technically rejects are useable for lesser tasks, and thus still have value, often above their scrap value. For example, a 16K EPROM (an eraseable, programmable memory with a 16,000 bit memory capacity), may not meet factory specs, yet still have 4,000 or 8,000 bits of usable memory capacity. As such it may not be usable in, say, computer or guidance system applications, but it would be usable in less critical applications, for instance a video game. If cost effective, the company might sell it with special customer markings or no markings at all. In such a case the part could be remarked and fraudulently sold as first grade product. Or, if a company were particularly cash poor at a given time, it (or an unauthorized department head), might be tempted to sell the unmarked parts for the short term benefit involved. This has happened on numerous occasions.

When combined with the fact that many reclaimers fail to destroy rejects because their intact value is worth more than the scrap value, these practices have created a more or less established grey market for unmarked parts (either untested or rejects). Rejects are especially easy targets, since very sloppy inventory control and security practices are used with respect to them. Often they are stored for months in rows of large barrels in various out-of-the-way areas without security protection. The same can be true, to a lesser degree, with untested parts. It's only when the parts are market grade that security becomes serious.

With easy access to unmarked parts, parts counterfeiters can have a relatively easy time of it. John Jackson used stolen or counterfeited printing plates to mark his parts. Larry Lowery stamped his with "generic" device names, not even bothering to put on a logo. With the legal availability of unmarked parts, proving guilty knowledge by one who possesses them is difficult.

All in all, however, the primary problem with the unmarked parts market involves consumer safety, not national security. When defective chips installed in medical equipment, airplanes, microwave devices and the like start failing, people are going to get hurt. Hopefully the problem can be cured before that happens.

Trade Secrets

Trade Secrets thefts pose a potentially more serious security problem than theft of product, since such thefts provide the very means of obtaining the technology upon which to establish an industry and develop competitive expertise. I've heard it authoritatively said that the United States at one time possessed a ten year lead over the Soviet Union in micro-electronics technology, but that that lead has already shrunk to maybe five years, based primarily on the easy access the Soviets have had to our technology. I'm not in a position to attest to the veracity of that proposition, but what I have seen would certainly not negate it.

By its very nature Trade Secret theft is the most difficult to detect and solve. What is taken is generally not a physical thing, but an idea. Original documents, computer tapes, reticles, masks, and technical drawings can be easily copied by any of a number of photographic or electronic means without anything corporeal ever being taken. Hence, it is never missed.

California at least is among the few states that at least have a criminal trade secrets theft statute. It reads as follows:

Penal Code Section 499c

(a) As used in this section:

(1) "Article" means any object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, micro-organism, blueprint or map.

(2) "Representing" means describing, depicting, containing, constituting, reflecting or recording.

(3) "Trade secret" means the whole or any portion or phase of any scientific or technical information, design process, procedure, formula or improvement which is secret and is not generally available to the public, and which gives one who uses it an advantage over competitors who do not know of or use the trade secret: and a trade secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.

(4) "Copy" means any facsimile, replica, photograph or other reproduction of an article, and any note, drawing or sketch made of or from an article.

(5) "Benefit" means gain or advantage, or anything regarded by the beneficiary as gain or advantage, including benefit to any other person or entity in whose welfare he is interested.

(b) Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret, or with an intent to appropriate a trade secret to his own use or to the use of another, does any of the following:

(1) Steals, takes, or carries away any article representing a trade secret.

(2) Fraudulently appropriates any article representing a trade secret entrusted to him.

(3) Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.

(4) Having obtained access to the article through a relationship of trust and confidence, without authority and in breach of the obligations created by such relationship makes or causes to be made, directly from and in the presence of the article, a copy of any article representing a trade secret.

(c) Every person who promises or offers or gives, or conspires to promise or offer to give, to any present or former agent, employee or servant of another a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his present or former principal, employer or master, to any person not authorized by such owner to receive or acquire the same and every person who, being a present or former agent, employee, or servant, solicits, accepts, receives or takes a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his present or former principal, employer or master, or any person not authorized by such owner to receive or acquire the same, is punishable by imprisonment in the state prison, or in a county jail not exceeding one year, or by fine not exceeding five thousand dollars ($5,000), or by both such fine and such imprisonment.

(d) In a prosecution for a violation of this section it shall be no defense that the person so charged, returned or intended to return the article. (Emphasis added)

Subsection (b) thus makes it a crime to take or copy any article containing a trade secret. Subsection (c) makes it a crime to offer a bribe to another to obtain a trade secret.

Note that Section 499c does not prohibit competitors from exploiting trade secret where they honestly gain access to them, such as by analysis of and reverse engineering from a finished, marketed product. The emphasis is on dishonest acquisition. Nor is novelty required. As is explained in the Restatement, Torts (1939), Section 757, Comment "b":

> ...A trade secret may be a device or process which is patentable; but it need not be that. It may be a device or process which is clearly anticipated in the prior art or one which is merely a mechanical improvement that a good mechanic can make. Novelty and invention are not requisite for a trade secret as they are for patentability. These requirements are essential to patentability because a patent protects against unlicensed use of the patented device or process even by one who discovers it properly through independent research. The patent monopoly is a reward to the inventor. But such is not the case with a trade secret. Its protection is not based on a policy of rewarding or otherwise encouraging the development of secret processes or devices. The protection is merely against breach of faith and reprehensible means of learning another's trade secret. For this limited protection it is not appropriate to require also the kind of novelty and invention which is a requisite of patentability.

Unfortunately, very few states have criminal trade secrets theft laws. In an informal survey I did, I discovered that most of the western states where significant semiconductor and defense plants exist have no trade secrets laws. I see this as a serious deficiency.

Trade Secrets Thefts Case History: Peter K. Gopal

Peter K. Gopal first came to the attention of industry security personnel in approximately January 1978. At that time, Intel Corporation learned from an anonymous source that one of its biggest competitors, National Semiconductors Corporation was in possession of a computer data base tape containing the design for a late model Intel microprocessor chip. This chip, the 8085, was a new, original Intel design representing a substantial advancement from previous microprocessor design.

Investigation revealed an individual by the name of James Catanich, an employee of National Semiconductor and their Microprocessor Division. Catanich told investigators that Gopal had directed him to take a untitled data base tape for inspection on National's computer system to see if the data contained in it was, in fact, genuine. Catanich reported that he picked up this tape from one of Gopal's associates and took it to National Semiconductor to view its contents with the use of National computers.

According to Catanich, upon viewing the contents he immediately recognized that the data thereon was proprietary Intel design information and, in a panic, took the tape off the machine and returned the tape to Gopal. However, it appears that in his haste he forgot to erase the data from National Computer's memory banks, and another National employee subsequently discovered the data. That employee thereupon apparently sought to convince his superiors that he could reverse engineer the Intel design, without telling them that he had acquired the original Intel data. After the incident was discovered, the employee was dismissed, as was Catanich. The corporate investigators, who later contacted the police regarding the incident, were unable to directly link the information to Gopal. National cooperated with Intel, returning all information to them. Intel let the matter lie.

Thereafter, in September 1981, one Andrew Moore, an independent manufacturer's representative, indicated in conversations to a National Semiconductor employee that he represented a principal who owned original Intel design information available for sale. The National employee immediately contacted his superiors, who contacted Intel and law enforcement authorities.

An undercover investigation ensued. The National employee, Larry Worth, re-contacted Mr. Moore, and set up a meeting with his principal, who turned out to be Peter K. Gopal. Equipped with a body transmitter-recorder, Mr. Worth and another undercover operator, Tom Dunlap of Intel Corporation, met with Mr. Gopal on numerous occasions. Dunlap posed as a National Semiconductor employee. Dunlap was used, rather than a police officer, because his technical expertise was needed to authenticate the genuineness of the data Gopal proposed to sell. During negotiations, Gopal offered to sell both chip designs and process information for numerous Intel Corporation products. One of the products offered was a highly proprietary state-of-the-art design not yet even marketed by Intel or any other corporation. The purchase price proposed for the entire package was in the millions of dollars. Gopal indicated that he had past and continuing access to proprietary Intel designs via insiders within Intel corporation. He stated that he had already sold his designs in Europe and the customers were quite satisfied with their performance and authenticity.

The undercover operation culminated in late September 1978, with the sale by Gopal to undercover operators of Intel 2114 chip designs. The 2114 is a standard memory chip. Search warrants were prepared and served leading to the

seizure from Gopal's business premises of scores of computer tapes, glass reticles, masks and other design materials for Intel, National, Zilog and other corporations. The value of the items seized ran well into the millions of dollars. Some of the items seized were designs still in the research and development state, which had never been marketed.

Also seized were business and personal records of Gopal's indicating numerous trips to Europe in 1977 and 1978, including trips to the Soviet Union and Poland. Business cards of numerous Soviet consular level and ministry officials dealing in technology exchange and purchase were found. These items can be summarized as follows:

(1) Money exchange certificate, in both Russian and English, signed by Gopal, dated November 28, 1977, showing a transaction wherein Gopal exchanged $100.00 U.S. for 71.48 rubles. From personal experience I know that the maximum amount of foreign currency one can bring into the U.S.S.R. is $100.00. One must exchange it for rubles at the port of entry and then re-exchange the rubles for dollars when you leave. Thus the certificate indicates Gopal entered the U.S.S.R. on November 28, 1977.

(2) Russian coins of various kopek denominations.

(3) Diary entries showing trips to Vienna in August, October, and November 1977, plus airline tags, etc., for Austrian airlines.

(4) Diary entry of November 1977, with the following name and address:
Zdzilaw Przychodzien
Deputy Director
Ministry of Machine Industry
36 Krucza Street
00-921 Warsaw, Poland

(5) Separate personalized business cards of the following persons, listing their address as "Ministry of Electronics Industry," Usieuicha 24/2, Moscow 125315, Tel. 155-49-15:

(a) Alexander I. Rublsov
Dipl. Engineer Semiconductors

(b) Alexander S. Ivanov
Mgr. of Special Technological Equipment Department

(c) Leonid F. Dymov
Chief of Department

(d) Vasily V. Kurdin
Director of Marketing

(e) Gennady V. Verklovenko
Sales Mgr. Semi-conductors

(6) Separate personalized business cards, listing the address as "V/O TEchnoproimport" Moscow C-200, Smolenskaja - Semaya Place 32/32, Tel. 244-33-52":

(a) L. A. Pavlov

Expert (This card bears the pencil-written words "Terms of contract negotiation" in what appears to be Gopal's handwriting.)

(b) Valeric N. Kousnev
Dipl. Engineer

(7) Separate personalized business cards, listing the address as the Soviet Consulate at 2790 Green Street, San Francisco, California (415)972-6642:

(a) Stanislav N. Nosov
Commerical Counsel
U.S.S.R.

(b) Yuriy V. Palov
Vice Counsel, Science, Technology, and Education Exchanges.

Business records seized indicated continuing international transactions between Gopal and Austrian and Swiss firms. The primary Austrian firm, Sacher-Gesellschaft AG, of Vienna, Austria, was headed by Dr. Rudolf Sacher. He was also a one-half shareholder with Gopal in Gopal's business, Semiconductor Systems, International, Inc. Subsequent investigation of the Swiss firms indicated they were probably nothing more than shell corporations, serving as middlemen for the transactions in which they were involved. Efforts to track the course of the transactions past the Swiss firms were fruitless. Gopal has refused to cooperate with the authorities.

The investigation continued after Gopal's arrest. A business associate was located who told authorities that Gopal had bragged of having purchased certain integrated circuit testing equipment and selling it to Poland via one of his Swiss intermediaries. Gopal bragged to him that he had received three times the fair market value of the equipment in cash, and had successfully smuggled the cash back into the United States without interdiction by Customs or Commerce officials. A check of available business records confirmed that Gopal had indeed acquired the equipment in question and had sold it, but its ultimate purchaser could not be determined. My understanding is that the Department of Commerce, after a diligent investigation, concluded that it was unable to prove a violation more serious than a misdemeanor, for which the only penalty was suspension of export licensing privileges. Since Gopal had, by that time, been effectively blackballed from the indsutry, it was felt that such a prosecution would not be worth the effort.

Gopal and his co-cospirators were charged with various state law violations, including conspiracy, bribery to obtain trade secrets, and the and

possession of stolen trade secrets. (It is interesting to note that during one of the tape recorded conversations Gopal had with undercover operatives, he offered Larry Worth, the National employee, ten thousand dollars each for each late model data base tape Worth could smuggle out of National Semiconductor. Based upon these conversations, the bribery count was included.) This prosecution represented one of the first major prosecutions under California's Trade Secret Theft Statute.

That statute, as previously pointed out, is a departure from traditional common law notions of property subject to theft. At common law, property must be physical to be subject to theft. The Trade Secrets Law expands this concept of property by specifically making ideas which qualify as Trade Secrets property for purposes of penal statutes. This statute was designed to fill some of the logical gaps left in the law by existing patent and copyright legislation. It protects ideas which are not patentable nor copyrightable, but which have substantial business value to its owner or competitors. For instance, a semiconductor device, such as a "memory" device would not be patentable because it is not a product of new technology, but merely builds upon existing technology. Under copyright law it would not be copyrightable even though such a design is in large part based upon its designer's creativity. Yet such a design can and increasingly does represent the expenditure by its owner of hundreds of thousands, even millions, of dollars of manpower, time and materials, before a single chip can ever be produced.

After initiation of the Gopal prosecution a novel problem presented itself and led to the suppression of all of the physical evidence against Gopal. While serving the search warrant the police had taken with them technical representatives of Intel and National Semiconductor in order to help identify the numerous items at Gopal's business which might be stolen. The police officer involved, having no technical background, had no idea of what they were looking at, or for. Trained engineers were required merely to identify those items which belonged to the victims. The majority of the items seized were reticles, photographs and tapes. None of them obviously had the word "stolen" on them. Many had the victims' logos and other identifying criteria deleted. Only an expert would be able to identify them.

The trial court ruled that the police had abdicated their responsibiilty of personally conducting the search by using these outsiders and suppressed all the evidence. Thankfully, on the People's appeal, the Appellate Court reversed and reinstated the evidence to the case.

After literally years of motions and other proceedings the case finally came to trial in November 1980. As neither side was comfortable with the prospect of a jury of lay people understanding the complex evidence being presented, both agreed to trial before a judge only. In the six months that followed extensive technical testimony was required to establish the case and to identify the items in Gopal's possession as being copies of originals in the possession of Intel Corporation and the other victims. On one occasion the court had to be recessed to the Computer Facilities room at National Semiconductor Corporation so that computer tapes could be played and displayed to court and council for analysis. Forensic analysis, including comparison of microscopic defects in the stolen reticles verses Intel and Zilog master reticles, consituted key evidence in the case. It was thus proved that the copies in Gopal's possession were directly made from original proprietary design data in the custody of one of Intel's sub-contractors and accessible to an employee who was a friend and part-time employee of Gopal".

Gopal was convicted by the court of six counts of receiving and possessing stolen trade secrets, bribery and conspiracy. He was sentenced to two years, eight months in the state prison in California, but is currently free on bail pending his appeal, which is expected to take at least a year. The transcript of the proceedings has not yet been transcribed, it was so voluminous. Three and one-half years after the offense and one year after the conviction, Mr. Gopal has yet to go to jail. Moore and Catanich, Gopal's co-conspirators, were each convicted by their plea of guilty to one count, one felony count. Each received probation and a substantial fine. The actual thief of the Intel trade secrets had his case dismissed for insufficient evidence, which was purely circumstantial and insufficient to support a reasonable expectation of conviction.

Copyright Protection

The U. S. Copyright Office has maintained a general rule that it will accept and maintain registration for a chip design incorporated into a schematic diagram, mylar sheet, photolothographic reticle or mask, or similar representatives in the nature of scientific or technical drawings. However, chip makers are hesitant to rely solely on registration of these for at least three reasons:

First, the final chip configuration represents the integration of a number of individual "drawings," so that the final product may be different from each individual layout itself. Not only are revisions made, but the total is more than just the sum of its parts.

Secondly, the diagrams, sheets and masks which the Copyright Office will register are not items which are exposed by the chip maker on the market. You can't buy them. When unauthorized duplication does occur, it is usually done by a primarily photographic process of "reverse engineering" from the finished chip, not from the design layout itself. Since the items registered were not in fact copied, it's questionable whether copyright protection applies under Section 113(b) of the Copyright Act. In the past, the Copyright Office has refused to concede that the chip itself is a published version of the drawings, so that while the drawings were protected, the chips were not.

Finally, even if copyright protection is available, proof of infringement poses difficult problems. Those who reverse engineer commonly alter the design cosmetically to disguise its origins from all but expert analysis. For instance, in the Gopal case, where stolen designs were used, naturally all logos and other unique company identifiers were removed. In addition, memory arrays were flip-flopped in a mirror image manner, address and input-output buffers were enlarged, and metal mask circuitry was rearranged in visually different but functionally irrelevant ways. The resulting chip would have been created and sold in plastic protective carriers so that a sample device would have to be purposely dissected and technically analyzed for the offense to be discovered. Once discovered the offender would undoubtedly argue no violation since substantial cosmetic differences existed.

Patent Protection

Although I don't presume any expertise in patent law, I think it's fair to say that the standards of patent protection, whether under state or federal law, are much more severe than those of copyright protection. One must show (1) novelty, (2) uniqueness, and (3) improvement over the prior art, which is not required for copyright purposes.

The standards of novelty and invention are high, and cumbersome to obtain. Although certain basic building blocks of semi-conductor technology, such as the semi-conductor transistor or "gate," are patentable, the patent process is generally not amenable to design advances. Like a novelist using established words and alphabet, the chip designer's genius is in his creative mastery and manipulation of the basic building blocks which enable him to get from a functional point A to a functional point B in the most electrically efficient and mass-producible package he can. Continual revision and redesign is the rule. A design which is state-of-the-

art today may be obselete in the market place next year. The tedious patent process does not fit into such an industry.

Suggested Responses To The Problem

Although the problems outlined are often centered in California, they are becoming increasingly national in scope as the industry spreads out across the country. Most western and eastern seaboard states have an electronics manufacturing industry of some sort. Even relatively isolated states as Idaho and Utah have significant branch manufacturing facilities run by companies based in California. This trend will continue as the industry seeks new locations with relatively cheap labor pools and inexpensive employee housing opportunities. Both of these commodities are becoming extremely scarce in California.

As a result of this, it appears unreasonable to expect local law enforcement agencies to be up to the job of such specialized investigations. Some sort of national or regional approach is necessary. The following is a list or priorities which would address the problem:

(1) Increased Staffing of Investigative Personnel In Export Regulatory Agencies And Amendments Of Their Enabling Legislation

Neither the U. S. Customs Service or the Export Administration Compliance Division of the Department of Commerce is adequately staffed to enforce existing laws regarding export of high technology goods.

The Customs Service's mission is not really even defined to include export activities. Its emphasis has always been monitoring of imports. It is suggested that amendments of applicable law to expand its mission in this area is desirable.

Many of the export laws now on the books provide inadequate penalties to deter criminal conduct. As was mentioned with respect to the Cogal case, an export violation discovered there was only a misdemeanor, for which the only penalty was suspension of export licensing status. A re-evaluation is in order.

(2) Creation Of National Or Regional High-Technology Crimes "Task Force" Or Information Clearinghouse

The Santa Clara County experience suggests that creation of a central intelligence clearinghouse is a mandatory first step toward combatting high tech crime. The "gray market" in particular consists of large numbers of interconnected companies and individuals, whose activities and relationships can only be establsihed by a continual monitoring effort, much like a narcotics bureau. Since these people operate on at least a regional scale, it is impossible for a local agency

95-929 O - 82 - 33

to keep track of them. By a pooling of information into a central intelligence unit, a broader, more complete picture can be constructed. From this vantage point, the major problem can be isolated and addressed.

To date the Santa Clara County Sheriff's Organized Crime Unit is the only such unit in the country that I'm aware of. Despite effective efforts by those in the unit, its staffing level (less than 5 people), is insufficient to deal with the cases arising just in Santa Clara County, much less in the region as a whole.

(3) Mandating Crime Reporting

If a centralized intelligence unit were created, laws making reporting of thefts to such agencies mandatory would be useful in gathering information and assessing patterns of criminal activity. Sanctions for violations need not be criminal sanctions.

(4) Electronics Broker Regulation Legislation

The obvious "choke point" of the gray market is the broker. Without the unscrupulous broker, the thief would have no one to sell to, and thus no reason to steal. If the brokers can be controlled, so can the crime problems. This should be the focus of the investigative efforts. The restrictions imposed need not be much more onerous than those almost everywhere imposed on pawnbrokers. Among the possibilities include the following:

(a) Federal broker licensing statutues: Require all electronics parts brokers to be licensed, conditioned upon identification of all parties holding an interest, disclosure of all current business and inventory locations, agreement to keep full and complete records of all transactions, to follow specified procedures to assure property acquired is not stolen, and to abide by other applicable laws and regulations, on pain of criminal penalties.

(b) Inspection statutes: Enabling designated law enforcement agencies access to brokers inventories and business records to assure compliance with the rules set forth in the licensing regulation. This should specifically include authority to search and seize with probable cause, but without a warrant. Again, this is generally no more severe than current pawnbroker statutes.

(c) Prohibition against possessing, buying or selling unmarked integrated circuits: Or other specified electronic devices, except by the manufacturer or its designated agent for scrapping purposes.

(d) Prohibition against remarking or counterfeiting integrated circuits, etc.

(e) Creation of an evidentiary presumption: That a broker in possession of specified stolen electronics goods has knowledge of its stolen character, unless he can show excercise of reasonable efforts to assure himself it was not.

(5) Enactment Of A Federal Trade Secrets Law With Criminal Penalties

Such a law, patterned on traditional civil law concepts (as was California's criminal statutes), would help fill the gaps in federal patent and copyright laws, and would give law enforcement an additional tool with which to combat espionage. In specific cases, prosecution under such a law might be much more manageable than having to prove actual diversion of classified information to a foreign power. Such a law could be tailored to fit federal subject matter jurisdictional requirements, if necessary, and would lend uniformity to an area which now has only spotty coverage.

Department of Justice

STATEMENT

OF

THEODORE WAI WU
ASSISTANT UNITED STATES ATTORNEY
CRIMINAL DIVISION
CENTRAL DISTRICT OF CALIFORNIA

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE

CONCERNING

UNITED STATES v. EDLER INDUSTRIES, INC., AND VERNON EDLER

UNITED STATES v. SPAWR OPTICAL RESEARCH, INC.,
WALTER J. SPAWR AND FRANCES A. SPAWR

UNITED STATES v. ANATOLI TONY MALUTA AND SABINA D. TITTEL,
SUB NOM, UNITED STATES v. WERNER J. BRUCHHAUSEN
ANATOLI TONY MALUTA, SABINA TITTEL AND DIETMAR ULRICHSHOFER

MAY 5, 1982

Good morning, Mr. Chairman and members of the Subcommittee, my name is THEODORE WAI WU. I am an Assistant United States Attorney of the Criminal Division, Central District of California. I have been investigating and prosecuting illegal exports of Munitions List articles and controlled technology and products since 1976. In this respect I have worked closely with special agents from the U.S. Customs Service and the Compliance Division of the Commerce Department, as well as concerned members of other federal agencies.

My testimony today will focus on the three cases I handled in the area of illegal technology exports.

Mr. Chairman, with your permission I would like to read the salient points of a prepared statement.

I

UNITED STATES v. EDLER INDUSTRIES, INC., AND VERNON EDLER (CENTRAL DISTRICT, CALIFORNIA)

A. The Initiation of the Investigation

The federal investigation into the technology export activities of Edler Industries, Inc. (EII) of Newport Beach, California, was instituted by the U.S. Customs Service in Los Angeles in July 1975. The Office of Munitions Control (OMC) of the U.S. Department of State had asked Customs to investigate whether EII was engaging in illegal export in violation of the International Traffic in Arms Regulations (ITAR) and 22 U.S.C. § 1934, then in effect. Thus in July 1975, pursuant to a search warrant, Customs agents seized numerous corporate records and documents from EII. Subsequently, the matter was referred to the United States Attorney's Office in Los Angeles and was ultimately assigned to me. A number of witnesses were interviewed; they included several former EII technical and non-technical employees, as well as OMC licensing officials and a government solid fuel rocket expert.

B. History of Proceedings

On July 12, 1976, a federal grand jury in Los Angeles returned an indictment against EII, and its president-owner, Vernon Edler, for illegally exporting controlled technical data and assistance to France, in violation of then 22 U.S.C. § 1934, now 22 U.S.C. § 2778(c) [Section 38 of the Arms Export Control Act (AECA)]; the International Traffic in Arms Regulations (ITAR) and 18 U.S.C. § 1001. Two months later, a federal jury found both the corporation and Vernon Edler guilty of exporting, without license, to the Societe Europeenne de Propulsion (SEP) of France, certain technical assistance and data related to the fabrication of graphite and carbon-carbon advanced lightweight material components having missile and aerospace applications. EII

was sentenced to pay a $25,000 fine and Vernon Edler received a two-year prison sentence. The execution of Vernon Edler's prison sentence was suspended, and he was placed on probation for five years on the condition that he serve ten (10) weekends in jail and donate 1200 hours of work to a charitable organization. Thereafter, EII and Vernon Edler appealed their convictions. On appeal, the Ninth Circuit Court of Appeals remanded the case for a new trial, on the basis that the trial court should have permitted EII and Vernon Edler to offer proof that the technical information exported to SEP had non-military uses. The court of appeals opined that evidence concerning non-military applications was relevant to the question "whether a defendant knew or should have known that the recipient of the exported information would use the information to produce or operate Munitions List articles." The appellate court also concluded that EII and Vernon Edler should have been allowed to show a lack of significant relationship between the technical information and Munitions List items. Accordingly, the case was remanded for a new trial.

On February 7, 1979, as a result of a new trial, EII and Vernon Edler were convicted by a federal jury of illegally exporting Munitions List technical data to SEP and they received the identical sentences as those previously imposed by the district court. EII and Vernon Edler again appealed but the appellate court affirmed their convictions. Their subsequent petition for certiorari was denied by the United States Supreme Court.

C. The Exports and Technology Involved in Edler

From as early as 1968 through 1976, Vernon Edler was owner and president of EII, a Newport Beach aerospace engineering firm. He was the decision-maker of the corporation and had close, daily working contacts with its engineers and technicians. EII began as a machine shop and gradually evolved into an aerospace manufacturing and engineering firm engaged in the fabrication of missile and rocket components --

particularly nozzle components for missile and rocket motors. EII had from time to time performed Government defense contracts and worked on rocket motor components for such missiles as the Polaris, Minuteman, Tartar, Hawk and Navy Standard Arms. Sometime during 1968-1969, Vernon Edler applied to OMC for approval for EII to enter into a Tape Wrap technical assistant agreement with a French entity called Societe d'Etude de la Propulsion par Reaction (SEPR) of Paris, France. (Tape Wrapping was then a sophisticated technical process for making components out of lightweight silica preimpregnated material.) Under that agreement, EII would provide SEPR with technical assistance related to the fabrication of tape wrapped components for rocket motors. The application was disapproved and Vernon Edler was informed by OMC that the disapproval was based on foreign policy and national security reasons. Specifically, OMC informed Vernon Edler that "the policy of the United States was not to assist a foreign country in the development of nuclear strategic delivery capabilities," and that the assistance which Edler proposed to provide SEPR was in the "strategic delivery area." Notwithstanding OMC's refusal to grant an export license, EII implemented the Tape Wrap program and provided SEPR with technical data, drawings, job travelers, and conducted critiques with SEPR engineers and technicians from France on tape wrap processes related to the fabrication of nozzle throat inserts and other nozzle components for missiles and rockets. French engineers and technicians from SEPR made technical visits to EII facilities and Vernon Edler sent his manufacturing supervisor to SEPR's missile manufacturing site in Lyon, France, to furnish technical assistance to SEPR. The tape wrap program was completed in 1971. EII-SEPR contacts continued, however.

In January 1974, Vernon Edler sought OMC export license to enter into a Lightweight Technical Assistance Program (LTAP) to provide the Societe Europeenne de Propulsion (SEP) with technical assistance related to lightweight material processing for the production of rocket motor components. According to former EII employees, SEP and SEPR were so related that the technical personnel whom EII dealt with at SEPR under the Tape Wrap agreement were also representatives of SEP. To EII, SEPR and SEP were one and the same. Just five months later in June 1974, EII applied for OMC authorization to export carbon-carbon technology to SEP under a Carbon-Carbon Technical Assistance Program agreement (C/CTAP) which EII, without OMC's knowledge, had already signed with the French. Based on the C/CTAP, EII was now to provide more sophisticated technical know-how that related to the fabrication of carbon-carbon rocket motor components. The technology involved in the production of carbon-carbon material components was a technical upgrade compared to the know-how covered by the earlier LTAP and the Tape Wrap agreement.

While the export license applications for the LTAP and C/CTAP were still pending, an OMC licensing officer informed Vernon Edler that those technical assistance programs were covered by OMC licensing requirements and that EII was not to act on them without "specific written approval" from the State Department. However, unbeknownst to OMC at the time it gave this caution, EII was already well into the performance of the LTAP and C/CTAP. French engineers and technicians from SEP were given detailed technical instructions, job travelers, drawings, data on specific gravity measurement and calculations, configuration analysis, and on-site demonstrations on how to process lightweight silica, carbon and graphite ablative materials for the fabrication of rocket motor components. EII technicians again went to SEP manufacturing sites to observe and critique material fabrication processes for nozzle throats, entrance caps and exit cones. EII

personnel saw those components being qualitatively verified at SEP for quality acceptance. According to one EII engineer, if accepted, those components would be put on the applicable missiles. At another SEP manufacturing facility, an EII engineer observed exit cones of the size and configuration which he associated with the submarine-launch Polaris missile. Another EII engineer saw exit cones at various stages of completion as well as completed nozzle assemblies attached to rocket motors. Indeed, EII personnel demonstrated to French technicians at SEP "techniques" of fabricating hardware "associated with missiles and rockets." As trial testimony showed, EII personnel knew SEP was buying EII technical knowledge to fabricate aerospace products. Under the carbon-carbon agreement, programs which involved carbon/carbon rocket motor components were assigned various female names. For example, there was the "Irene" program which related to exit cones for solid fule rocket motor; "Marcella" which pertained to nozzle throats; and "Nancy" which concerned entrance caps.

According to the trial testimony of one former EII employee, the diameters of the nozzle throats and entrance caps of the "Kathleen" program fit the same "ballpark as a Polaris or Poseidon" submarine-launch ICBM. This witness testified he had no doubt that the carbon/carbon agreement was to give SEP technical know-how and manufacturing techniques to fabricate rocket nozzles and that SEP's attempt to reach "high density" for the carbon/carbon material indicated to him that the technology transferred to the French could only be used for rocket motors.

Throughout the summer of 1974, French engineers continued to receive instructions from EII on "fabrication parameters" and were shown manufacturing techniques for the components under the various "girl" programs. Vernon Edler himself participated in these activities.

In October 1974, OMC informed Vernon Edler that EII's license applications for the LTAP and C/CTAP agreements had been disapproved. Yet, notwithstanding OMC's refusal to grant approval, Vernon Edler continued to export to SEP the controlled technical information.

Two government missile experts testified at trial that the technology EII transferred was significantly and directly related to rocket nozzles for military missiles. According to one U.S. Air Force rocket expert, the data exported by EII "uniquely speak to, without exception, rocket nozzles." Indeed, some of the techniques transferred to SEP were then currently used in a major U.S. missile program, according to an expert from the aerospace industry. Vernon Edler himself admitted to a Customs special agent in my presence that he (Edler) was aware that SEP was involved in missiles and missile components production, and he believed that the technology EII conveyed to SEP would be utilized in that vein.

The Edler case represents the first successful government prosecution of illegal exportation of Munitions List

II

UNITED STATES v. SPAWR OPTICAL RESEARCH, INC.
WALTER J. SPAWR AND FRANCES A. SPAWR,
No. CR 80-789-WMB (C.D. Cal. 1980

A. The Investigation

In February 1978, Compliance Division, Office of Export Administration (OEA), Department of Commerce, received a report of possible interest from a government agency regarding the alleged sale of laser mirrors to the Soviet Union by Spawr Optical Research, Inc., (Spawr Optical), Corona, California, in violation of the Export Administration Act of 1969, as amended. The referring agency gave its approval for Compliance Division to contact the concerned citizen who furnished the information on the alleged violations. OEA licensing officers confirmed that laser mirrors, of the type described in the report, were controlled by the Commerce Department for national security reasons and would not be authorized for export to the Soviet Union. Licensing officers also confirmed that Spawr Optical had applied for authorization to export certain high energy laser mirrors to a research institute in the USSR

in 1976, and that the license application had been rejected for national security reasons. Further research revealed the license application had specified 14 water-cooled laser optics (mirrors) of various diameters valued at approximately $30,800. One week later, a special agent from the Compliance Division and a Customs special agent (from the San Francisco Customs Office) contacted the concerned citizen and two former employees of Spawr Optical, who furnished substantive facts to support the previous report. Based on this information, a federal grand jury subpoena was issued in March 1978, for Spawr Optical corporate records and documents related to the export of laser mirrors.

On March 9, 1978, special agents from Customs and the Commerce Department interviewed Walter J. Spawr and Frances A. Spawr at the company premises and obtained a voluntary, signed statement from Frances Spawr. According to Frances Spawr's statement, she had undervalued several shipments of laser mirrors to a Wolfgang Weber in West Germany at the latter's request. Following the interview, the agents served the grand jury subpoena on Frances Spawr as the company's custodian of records. Investigation then followed.

Subsequently, Special Agent Rice of the Commerce Department Compliance Division, initiated a foreign inquiry through the U.S. Consultate General in Frankfurt, West Germany concerning the disposition of the Spawr laser mirrors exported to Weber. Weber admitted that the mirrors had been transshipped to the Soviet Union and agreed to come to the United States to disclose to the Compliance Division his involvement in the transshipment scheme.

In September 1978, Weber traveled to the United States and was interviewed by special agents of the Compliance Division, at which time Weber disclosed in detail his participation

with Walter Spawr in the transshipment of Spawr laser mirrors to Mashpriborintorg, a state purchasing agency of the Soviet Union. Thereafter, the matter was referred to the United States Attorney's Office in Los Angeles for consideration, and in the spring of 1979, I was assigned to oversee the investigation and, if appropriate, to prosecute the case. Investigation continued and additional witness interviews were conducted by Customs and Compliance Division special agents and myself through the summer of 1980. In August 1980, Compliance Division Special Agent Rice and I went to Switzerland in an attempt to elicit the cooperation of the Swiss Government in our investigation of Spawr Optical and of another export control matter. Representatives of the Swiss Government declined to lend assistance based on their political neutrality and the restrictions of their own business secrecy law.

Investigation and trial evidence disclosed that Spawr Optical held a DOD facility security clearance and had performed contracts on government defense programs. Walter Spawr and the company had performed laser optics polishing work for companies like TRW and Rocketdyne, and government agencies such as Los Alamos Science Laboratory, Redstone Arsenal and Naval Weapons Laboratory. Moreover, Spawr had furnished the Air Force Weapons Laboratory at Kirtland AFB, New Mexico, high energy laser mirrors of the identical specifications as some of the mirrors illegally sold to the Soviet Union.

B. The Indictment

On September 3, 1980, a federal grand jury returned a 15-count indictment against Spawr Optical, and Walter J. and Frances Spawr, charging conspiracy, submission of false statements to the government and illegal exportation of laser mirrors to the Soviet Union.

C. The Exports and the Technology

Witness statements and evidence presented at trial established the following:

In 1974 and 1975, Spawr Optical, led by its president and founder, Walter J. Spawr, sought additional markets for the Spawr laser mirrors in Europe. One of the firms contacted there as a possible sales agent was Oriel GmbH, Darmstadt, West Germany, whose managing director was the previously mentioned Wolfgang Weber. Weber was a young and ambitious entrepeneur with good contacts in the USSR. In early 1975, Weber became Spawr's West German sales representative. Weber testified that he went to Moscow in late 1975 for the purpose of exhibiting Spawr mirrors in the Soviet Union with Walter Spawr's approval. Initial contacts between Weber and representatives of Mashpriborintorg were encouraging to Weber, and he contacted Walter Spawr by telephone in December 1975 to convey the Soviets' interest in him. According to Weber, Spawr was enthusiastic about possible large sales of his laser mirrors to the Soviet Union.

Weber testified that, in about January 1976, he obtained a large order for Spawr Optical water-cooled laser mirrors from Mashpriborintorg. These mirrors of various diameters ranging up to twelve (12) inches, were the finest manufactured by Spawr Optical, which was noted in its field for the superior quality of its mirror surfaces. Weber transmitted the order to Walter Spawr after receiving his approval in January 1976. Almost immediately thereafter, Walter Spawr assigned a production-order number to the Russian order, and work was begun on filling the order. Even though the firm's general manager had over one year earlier warned both Walter and Frances Spawr of the U.S. Department of Commerce requirement for export licenses for such laser mirrors, no export license application was submitted by the firm to the Department of Commerce for export of the mirrors.

The majority of the laser mirrors in the January Russian order were exported to Weber in West Germany in July 1976. Export documents, containing false statements, were executed by the Spawrs to facilitate the shipments and to deceive U.S. authorities as to the value of the contents and shipments, and

thereby to evade scrutiny and export licensing requirements. Weber testified that, after the arrival of the mirrors at Frankfurt Airport, he arranged to forward them to Moscow. Weber subsequently learned from the Russians that they were very pleased with the Spawr mirrors they received, and he communicated the Soviets' satisfaction to Walter Spawr. Weber also testified that he called Walter Spawr on several occasions from Moscow concerning the mirrors for Russia. This was confirmed by the firm's former secretary, who was told of the Moscow calls by Frances Spawr.

In April 1976, Weber received another large order for additional Spawr water-cooled mirrors from Mashpriborintorg. The order included mirrors of various diameters ranging up to 15.74 inches. Weber was told by the Russians that these mirrors would be used by the Lebdev Institute, Moscow, for "laser experimentation." As he had done with the first order, Weber sent the order to Walter Spawr and informed him of the intended customer. According to a former Spawr Optical employee, Frances Spawr told her that the Spawrs believed they should apply for a Commerce export license to cover the larger mirrors in the second order because there was a possibility that the larger mirrors would be detected and stopped by Customs officers. An export license application for 14 of the 29 mirrors odered by the Soviets in April 1976 was sent to the Commerce Department's Office of Export Administration in May 1976. In October 1976, the license application was denied for "national security reasons." The Spawrs were expressly informed by Commerce in writing that

> "these laser mirrors . . . have significant strategic spplications. They have been denied in view of the predominant use with CO_2 lasers which have important applications in the military arena."

Weber testified that, during the period before the license application rejection, he discussed with Walter Spawr what to do if the application was denied. According to Weber, he and Spawr devised a plan to send the mirrors to Switzerland, from where they would be forwarded to the Soviet Union. A

former Spawr Optical secretary testified that Frances Spawr told her that if the Department of Commerce did not approve the license application, they would ship the mirrors to Russia anyway, by way of Switzerland.

After the application was rejected by the Commerce Department, Spawr Optical continued with the fabrication of the mirrors for the second Russian order. Walter Spawr cautioned his employees to no longer refer to the pending order as the "Russian" order as they had formerly done. As part of the conspiracy to export the second order of mirrors to the Soviet Union without licenses and to deceive U.S. export licensing people, Walter Spawr asked Weber to send him an order cancellation on that second Russian order, but to really keep the order open. Testimony and documents obtained at the firm showed that it was Frances Spawr who received from Weber the address of the Swiss freight forwarder used to divert the mirrors to the USSR.

By February 1977, Spawr Optical had completed the second Russian order, and had begun to ship the mirrors to Switzerland in four shipments. In order to avoid scrutiny by U.S. authorities, Frances Spawr, as she had done earlier with another employee, instructed the firm's new secretary to falsify the value of the mirrors on Shipper's Export Declarations. Frances Spawr told her secretary to place on the export declarations the false value of $500 or less per mirror. This was the same tactic used by the Spawrs to effect the July 1976 shipments. The second Russian order had a price tag of about $40,000.

On December 12, 1980, after 13 days of trial which spanned over a five-week period, the Spawrs and their firm were variously convicted by a jury of conspiracy, submission of false statements, and illegal exportation of laser mirrors to the Soviet Union. Frances Spawr was sentenced to five years imprisonment. Her sentence was suspended and she was placed on five years probation. Walter Spawr was sentenced to ten years imprisonment,

with all but six months suspended; he was also placed on five years probation. Both Mr. and Mrs. Spawr were ordered to contribute 500 hours to a charitable organization. The firm was fined $100,000.

The Justice and Commerce Departments and the Customs Service considered the prosecution to be an important milestone in export control enforcement because of the seriousness of the offenses and because of the important laser optics technology made available to the Soviet Union as a result of the unlawful exports. Colonel Bob L. Francis, USAF, Commander of the Air Force Weapons Laboratory, Kirtland AFB, assessed that the mirrors exported by Spawr Optical not only advanced the laser mirror technology in the USSR, an area where the Russians were felt to be deficient, but it also saved the Soviets millions of dollars and nearly one hundred manyears in research and development costs. Even though the commercial value of the mirrors was relatively low (about $60,000), the technological value received by the Soviet Union was significant. According to Colonel Francis:

> "The free world, and especially the United States, has actively pursued the technology investigations of high energy lasers as to their weapons lethality capabilities. In this pursuit it became evident that sophisticated heat exchangers using water cooling of the mirrors substates were very important and necessary elements. This eight-year development effort, of improving and perfecting the heat exchangers on water-cooled laser mirrors, has involved many millions of dollars and nearly a hundred manyears of R&D effort. The illegal sale by Spawr, et al, has now provided the Soviets with over 50 water-cooled high energy laser mirrors as well as the capability to disassemble and back engineer this mirror heat exchanger technology."

95-929 O - 82 - 34

The assessment that the mirrors illegally exported to the Soviet Union had real potential military application paralleled what was evidently known to the Spawrs at the time of the consummation of the offenses. In October-November 1976, the Spawrs had asked of their prospective secretary during an employment interview how the latter felt about working for a company that makes things that might harm people.

In the respect of national security interest, then, the Spawr Optical prosecution was particularly important to the government. It also resulted in the largest fines and longest prison sentences levied for export control offenses up to that time.

It should be noted that the assistance of concerned citizens and cooperative witnesses were crucial to the successful investigation and prosecution of the Spawr Optical case.

III

UNITED STATES v. WERNER J. BRUCHHAUSEN, ANATOLI T. MALUTA, SABINA D. TITTEL, AND DIETMAR ULRICHSHOFER (CENTRAL DISTRICT, CALIFORNIA)

A. The Origin of the Investigation

In March 1980, while conducting the Spawr Optical Research investigation, I was advised by the Compliance Division special agent who was on the Spawr case that he was also concurrently working on another investigation involving possible diversions of controlled high-technology goods to the Soviet Bloc by a Los Angeles firm. He furnished me with the following information:

In January 1980, Fairchild Test Systems Group, San Jose, California, contacted the Compliance Division concerning sales of advanced semi-conductor test instruments to an entity styled Consolidated Protection Development Corporation. Fairchild had previously sold four of the systems to Consolidated Protection and had current orders for eight more systems, valued at about

$1.3 million. In February 1980, Watkins-Johnson Company, Palo Alto, California, and Applied Materials Corporation, Sunnyvale, California, also contacted Compliance Division inquiring about Consolidated Protection and its president, Anatoli Tony Maluta. The Compliance special agent then contacted Fairchild, Applied Materials, and Watkins-Johnson. What emerged from these contacts was information pointing to the possibility that Anatoli ("Tony") Maluta was purchasing U.S.-origin high-technology products for possible diversion to proscribed countries. Maluta's method of operation was consistent with traditional diversion procurement attempts, although it was apparent that Maluta had refined those methods. Further investigation showed that Maluta was purchasing goods under one name and exporting under another. In fact, Maluta, over a three-year period, was determined to have actively used some six trade styles to conceal his activities. Maluta's freight forwarder in Los Angeles confirmed to the special agent that Maluta made only export shipments, contrary to Maluta's assertions to his suppliers that he was purchasing for domestic consumption only. Most of the shipments through the freight forwarder were made to West Germany through Los Angeles International Airport. In addition, records made available to the government indicated Maluta had apparently undervalued and misdescribed the commodities on Shipper's Export Declarations to disguise the nature and value of the goods.

Further leads revealed that Maluta had devised elaborate cover stories to mask his true activities. These cover stories generally followed the line that Maluta was enaged in the manufacture of perimeter protection systems for military installations in Alaska, Arizona, Southern California, or elsewhere in the "Free World." Maluta also falsely represented to his suppliers that his work was classified by the government. These cover stories were apparently designed by Maluta to prevent installation or repair technicians and salesmen from the manufacturers from visiting Maluta's asserted installations, and also to allow Maluta to evade manufacturers' questions about the intended uses and locations of the equipment. Maluta's apparent intent was clear to the investigators: the fewer questions asked, the better.

The Compliance special agent also learned that Maluta was then in the process of purchasing considerable amounts of equipment, including two highly sophisticated Gasonics, Inc., HiPox high-pressure furnaces, valued at about $300,000, used in the manufacture of semi-conductor devices.

B. The Investigation Upgraded

Upon receiving the foregoing information, I advised the Compliance special agent and the Customs special agent on the Spawr case to increase vigilance on monitoring Maluta's activities in addition to working on the Spawr case. In late March 1980, the Gasonics equipment was tracked from the manufacturer in Sunnyvale, California, to the Los Angeles freight forwarder, where it was to be shipped on Maluta's orders. It was held there by the freight forwarder awaiting eventual export to West Germany. Maluta had instructed the freight forwarder to ship the equipment to a consignee in West Germany. We ascertained Maluta had not applied for the necessary export license.

It was readily apparent to me then that the investigation was taking on major importance and scope and that the one or two Commerce Department Compliance agents assigned to the case did not comprise sufficient manpower to handle the investigation. I then requested the Special Agent in Charge of the U. S. Customs Office of Investigation in Los Angeles to enter the investigation and assign additional Customs investigators to the case, which he did.

It was clear that we could not risk the Gasonics furnaces falling into the hands of a Communist Bloc nation because of the strategic nature and the state-of-the art technology of the equipment being readied for export. I also considered it important not only to our potential case against Maluta, but also to our national security interest, to ascertain the final destination of the equipment, which we suspected to be a Bloc nation. For this reason, I, after discussion with the Customs and Commerce agents, requested Customs to prepare a substitute Gasonics shipment containing sand or some other suitable material for a controlled delivery. I also asked Customs

to seize the real high-pressure furnace systems when they were presented for export at Los Angeles International Airport. The substituted crates would then be allowed to be exported in place of the real equipment. It was our considered opinion that if the controlled delivery worked, we would have a good chance of tracing where the equipment was really going.

The substituted shipment was exported in early May 1980 to Vienna via West Germany. Documents showing the ultimate destination of the equipment as Mashpriborintorg, Moscow, USSR via Amsterdam were subsequently recovered by the U. S. Customs Attache Office, Bonn.

Throughout the investigation, there was an efficient and cooperative relationship between working level U. S. Customs investigators, U. S. Commerce Department investigators, the U. S. Justice Department personnel involved in the investigation and prosecution, the U. S. Customs Attache's Office in Bonn, and West German Customs officials in Bonn and Duesseldorf. As you will see, later on, special agents and revenue agents from the Internal Revenue Service entered the investigation with excellent results.

The continuing investigation by U. S. Customs in Bonn and the Duesseldorf West German Customs Office revealed an extensive and complicated web of diverters and firms wittingly and unwittingly providing assistance to the network of Maluta and his West German co-conspirator, Bruchhausen, who procured goods primarily for the Soviet Union. It was also learned that Elmasch GmbH, an additional West German firm in the network was established to procure U.S.-origin technology goods for other Soviet Bloc nations, principally Bulgaria, Poland, East Germany, Czechoslovakia, and Hungary.

By mid-May 1980, search warrants had been obtained to search Maluta's firm, now named Continental Technology Corporation. in Torrance, California, bank deposit boxes and former offices of Maluta's California firms. Warrant searches were also conducted at the residence of Sabina Tittel, who was then suspected of being a part of Maluta's illegal export activities. Voluminous export documents were obtained in the search of Continental Technology which were crucial to the investigation. It was also apparent that many other documents

had been destroyed before the searches. Searches of entities allegedly operated by Bruchhausen in West Germany were also conducted by West German Customs authorities, which resulted in the discovery of significant amounts of incriminating documents.

I arranged for travel to West Germany for one Commerce investigator and one Customs investigator and myself in July and August 1980. On arrival in Bonn, I met with U. S. and West German officials to elicit West German cooperation in our investigation of what was considered to be the most significant and elaborate diversion scheme yet unearthed. After some frank discussions with West German officials, they agreed to allow the Commerce Department investigator and me to work with the West German Customs authorities. U. S. Customs investigators were already authorized by an existing U.S.-German Customs Agreement to conduct certain inquiries in West Germany. I must say I was personally gratified and extremely appreciative that the West German authorities were willing to assist our effort in this way.

During our three-week stay in West Germany, we reviewed the large number of business and export documents seized by the West Germans from Techma GmbH, Elmasch GmbH and other Bruchhausen related entities. We worked closely with a very talented and cooperative West German Customs agent during this period. The documents we reviewed clearly established that Techma and Elmasch were set up solely to receive U.S.-origin goods and to divert to the Soviet Bloc. Of the literally hundreds of shipments we reviewed, only one or two involved non-U.S.-origin goods. After a cursory summation, we estimated that the Soviet Bloc paid more then $12 million for the U. S. high-technology products bought through Maluta over a period from 1977-1980. The apparent domestic value of the goods purchased in the U. S. over the same period was approximately $8 million. As you can see, the scheme, up to the time of its discovery, was extremely lucrative for those who were part of it. At the same time, the system was virtually impossible to detect on its own. This was because

(1) Maluta's cover stories were apparently effective in discouraging manufacturers from questioning his activities; (2) his use of two sets of firms, one to purchase and one to export, made it difficult for the curious to make a face value connection between purchaser and exporter; and (3) the use of in-bond shipments through West Germany and a neutral country, either Switzerland or Austria, precluded undirected discovery of the diversions by foreign governments.

After our visit to West Germany in July and August 1980, I traveled to Switzerland with the Compliance agent to ask the Swiss authorities to help with our investigation. In discussions with Swiss government officials, we were told that American export control enforcement involved political considerations and that the Swiss government could lend no assistance because of that country's political neutrality and because their own business secrecy laws prohibited even the government from making certain business-type inquiries.

In February 1981, based on what we had already learned about Maluta's and Tittel's activities at Continental Technology, I asked the Internal Revenue Service to enter the case. Information and documents reviewed by the Customs and Commerce investigators and myself pointed to the strong likelihood that Maluta and Tittel had not declared significant parts of their gains from the illegal export activities from 1978 and 1979. Within the next five months, IRS special agents and revenue agents amassed enough information to support several felony counts against Maluta and Tittel for tax evasion and subscribing to false income tax returns. This was a considerable achievement on the parts of the IRS investigators, who played no small role in the government's ultimate success in the prosecution of Maluta and Tittel.

The investigation team comprising one Customs special agent and one Compliance special agent and myself again traveled to West Germany in May and June 1981 to interview additional witnesses and to finalize our pre-indictment investigation and prosecution documents. I again met with West German officials and received

their continued, effective cooperation, which was crucial in developing our case against Maluta and his associates. The team returned to the United States after three weeks of investigation, having secured the cooperation of crucial prosecution witnesses.

C. The Indictment

On August 19, 1981, a federal grand jury in Los Angeles returned a sixty-count indictment against Maluta, Bruchhausen, Maluta's secretary, Tittel, and Dietmar Ulrichshofer of Vienna, variously for conspiracy to violate U. S. export laws, making false statements on Shipper's Export Declarations, violations of the Export Administration and Arms Export Control Acts, perjury, and income tax violations.

D. Maluta and Tittel Convicted

On October 26, 1981, Sabina Born Tittel pleaded guilty to six counts of the original indictment, including two false statement counts, two income tax violation counts, and two counts of illegal exports to West Germany.

On October 27, 1981, as a result of a court trial before United States District Judge William Matthew Byrne, Jr., on stipulated facts, Anatoli Tony Maluta was convicted of the fifteen felony counts charged in a Superseding Information, including conspiracy, making false statements on export declarations, illegal exportation of high-technology and Munitions List commodities to the Soviet Bloc, including the Soviet Union, in violation of the Export Administration and Arms Export Control Acts, and of tax evasion and subscribing to a false income tax return. On December 7, 1981, Maluta was sentenced to five years imprisonment and to pay a fine of $60,000. Maluta is currently at liberty on bond pending appeal. Tittel was sentenced to two years imprisonment and to pay a $25,000 fine. Tittel was taken into custody in January 1982 and is currently serving her sentence at the Federal Correctional Institution, Pleasanton, California. On April 2, 1982, Tittel filed a motion for a reduction of her two-year sentence, and the court has taken the motion under submission.

variously for conspiracy to violate U. S. export laws, making false statements on Shipper's Export Declarations, violations of the Export Administration and Arms Export Control Acts, perjury, and income tax violations.

D. Maluta and Tittel Convicted

On October 26, 1981, Sabina Dorn Tittel pleaded guilty to six counts of the original indictment, including two false statement counts, two income tax violation counts, and two counts of illegal exports to West Germany.

On October 27, 1981, as a result of a court trial before United States District Judge William Matthew Byrne, Jr., on stipulated facts, Anatoli Tony Maluta was convicted of the fifteen felony counts charged in a Superseding Information, including conspiracy, making false statements on export declarations, illegal exportation of high-technology and munitions list commodities to the Soviet Bloc, including the Soviet Union, in violation of the Export Administration and Arms Export Control Acts, and of tax evasion and subscribing to a false income tax return. On December 7, 1981, Maluta was sentenced to five years imprisonment and to pay a fine of $60,000. Maluta is currently at liberty on bond pending appeal. Tittel was sentenced to two years imprisonment and to pay a $25,000 fine. Tittel was taken into custody in January 1982 and is currently serving her sentence at the Federal Correctional Institution, Pleasanton, California. On April 2, 1982, Tittel filed a motion for a reduction of her two-year sentence, and the court has taken the motion under submission.

E. The Importance of the Case and the Exported Technology

I am informed by the Justice and Commerce Departments and the Customs Service that the Maluta/Bruchhausen illegal export operation was the most sophisticated and complex, as well as the largest, yet uncovered involving high-technology commodities to Soviet Bloc nations. Not only were the firms involved in the scheme established solely to procure technologically advanced military and "dual-use" commodities for shipment to Communist-controlled nations, the personnel chosen to execute the scheme were carefully selected. More than eight million dollars of some of the most advanced hardware were exported illegally over

a three and one-half year period in the scheme, and most of the equipment was highly prized and dearly paid for by the Soviets and their satellite countries in hard currency. Some of the computers, micro-circuit test systems and manufacturing equipment and peripherals purchased and exported by Maluta, could greatly increase their computer technology and production capability. The controlled commodities also included military microwave surveillance equipment intended for the Soviet Union, and micro-computers and state-of-the art solid state electronic devices for the Soviets and other Bloc users. The equipment illegally exported from the United States in this case represents a vast gain by the Soviet Bloc in advanced technology equipment that would not have been licensed by U. S. authorities for shipment to the Soviet Bloc. Equally important is the fact that our investigation frustrated Maluta and his co-conspirators from obtaining millions of dollars of additional equipment, including a $1.3 million order for semi-conductor test equipment for the USSR, a $700,000 microwave surveillance system which, according to the manufacturer, was capable of missile-tracking applications, and the $300,000 high-pressure furnace systems also for the Soviet Union. These are only some of the items Maluta had on order for export. There were considerable quantities of additional sophisticated equipment that Maluta was in the process of ordering for Bruchhausen's firms when the network was uncovered. The investigation and prosecution closed down a highly successful and established procurement system.

I am convinced that Soviet Bloc efforts to obtain U.S.-origin state-of-the-art technology are relentless and very much alive. This is a critical challenge facing our country and its allies today, and this is a challenge we must meet with resources and resolve.

"CONTROL OF TECHNOLOGY TRANSFERS TO THE SOVIET UNION"

TESTIMONY

OF

THE HONORABLE

JAMES L. BUCKLEY

UNDER SECRETARY FOR SECURITY ASSISTANCE, SCIENCE AND TECHNOLOGY

BEFORE THE

SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATION

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS

MAY 6, 1982

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE,

I AM DELIGHTED AT THIS OPPORTUNITY TO RESPOND TO YOUR INVITATION TO TESTIFY ON THE ROLE OF THE STATE DEPARTMENT IN CONTROLLING OF THE TRANSFER OF MILITARILY CRITICAL TECHNOLOGY TO THE SOVIET UNION AND THE EASTERN BLOC. WHATEVER THE RECORD OF PRIOR ADMINISTRATIONS, REPUBLICAN AS WELL AS DEMOCRATIC, IT IS CLEAR THAT THIS ADMINISTRATION HAS PLACED A VERY HIGH PRIORITY ON IMPROVING THE EFFECTIVENESS OF THE EXECUTIVE BRANCH IN ENFORCING EXPORT CONTROLS. IT HAS LAUNCHED IMPORTANT INITIATIVES WHICH WE BELIEVE WILL GREATLY IMPROVE THEIR OVERALL EFFECTIVENESS WHILE SHARPENING THE FOCUS ON THOSE ELEMENTS OF ADVANCED TECHNOLOGY AND PROCESS KNOW-HOW WHICH ARE OF THE MOST CRITICAL IMPORTANCE TO THE SOVIET BLOC. WE FREELY ACKNOWLEDGE THAT MUCH MORE NEEDS TO BE DONE; AND WE ARE ACTIVELY WORKING WITH OTHER AGENCIES TO IMPROVE COORDINATION OVER A RANGE OF ISSUES. IT WILL TAKE TIME, HOWEVER, FOR ALL THESE EFFORTS TO TAKE HOLD IN PARTICULAR AREAS, ESPECIALLY BECAUSE OF THE LARGE AMOUNT OF NEW DATA THAT HAS HAD TO BE GATHERED BY VARIOUS AGENCIES, AND THE ANALYTICAL WORK THAT HAS TO BE DONE.

IN YOUR LETTER INVITING ME TO TESTIFY, YOU ASKED THE STATE DEPARTMENT TO RESPOND TO SIX SPECIFIC QUESTIONS. I HAVE DONE SO IN THE ATTACHMENT TO MY PREPARED STATEMENT, WHICH I WOULD APPRECIATE YOUR INCLUDING IN THE PROCEEDINGS.

NATIONAL SECURITY EXPORT CONTROLS ARE A BASIC ELEMENT IN OVERALL U.S. POLICY TOWARDS THE WARSAW PACT COUNTRIES. TO PUT IT BLUNTLY, THESE CONTROLS ARE A RECOGNITION OF THE FACT THAT THE GLOBAL OBJECTIVES OF THE SOVIET BLOC ARE INNIMICAL TO OUR OWN, AND THREATEN EVERY VALUE FOR WHICH OUR NATION STANDS. THEREFORE, IT IS SIMPLY HARMFUL FOR US TO PROVIDE THOSE NATIONS WITH WESTERN, MILITARILY USEFUL TECHNOLOGIES, TO BE TURNED AGAINST US.

AS MOST OF THESE SENSITIVE TECHNOLOGIES ARE NOT WITHIN THE SOLE CONTROL OF THE UNITED STATES, IT HAS BEEN ESSENTIAL FROM THE OUTSET TO ACHIEVE AMONG THE MAJOR WESTERN INDUSTRIALIZED POWERS FUNDAMENTAL AGREEMENT AS TO WHAT TECHNOLOGIES ARE MILITARILY CRITICAL AND HOW THEIR TRANSFER TO THE SOVIET BLOC SHOULD BE CONTROLLED.

THE INSTRUMENT THAT HAS BEEN DEVELOPED FOR THIS PURPOSE IS THE COORDINATING COMMITTEE FOR MULTI-

LATERAL EXPORT CONTROLS, OR "COCOM" TO WHICH JAPAN AND ALL NATO COUNTRIES, WITH THE EXCEPTION OF ICELAND, BELONG. COCOM WAS CREATED IN 1949 BY INFORMAL AGREEMENT AMONG ITS MEMBERS, AND HAS THUS BEEN IN EXISTENCE FOR MORE THAN THREE DECADES.

COCOM HAS THREE MAJOR FUNCTIONS:

-- THE FIRST IS THE ESTABLISHMENT AND UPDATING OF LISTS OF EMBARGOED PRODUCTS AND TECHNOLOGIES. ALTHOUGH COCOM LISTS ARE NOT PUBLISHED, THEY BECOME THE BASIS FOR THE NATIONAL CONTROL LISTS ADMINISTERED BY EACH MEMBER GOVERNMENT. THE MEMBER GOVERNMENTS ARE NOW PREPARING FOR A MAJOR REVIEW OF THESE EMBARGO LISTS, WHICH WILL BEGIN IN OCTOBER.

-- SECONDLY, COCOM ACTS AS THE CLEARING HOUSE FOR REQUESTS SUBMITTED BY THE MEMBER GOVERNMENTS TO SHIP SPECIFIC ITEMS TO SPECIFIED END-USERS IN THE PROSCRIBED COUNTRIES. (THE COCOM-PROSCRIBED COUNTRIES ARE THE SOVIET UNION, THE OTHER WARSAW PACT COUNTRIES, CHINA, AND THE OTHER COMMUNIST COUNTRIES IN ASIA).

-- THIRDLY, COCOM SERVES AS A MEANS OF COORDINATING THE ADMINISTRATION AND ENFORCEMENT ACTIVITIES OF THE MEMBER GOVERNMENTS.

THE COCOM LISTS SET UP FAIRLY SPECIFIC LIMITS ON THE TECHNICAL CHARACTERISTICS ABOVE WHICH MEMBER GOVERNMENTS AGREE THAT THEY WILL PROHIBIT EXPORTS TO PROSCRIBED COUNTRIES, UNLESS COCOM ITSELF APPROVES EXCEPTIONS.

IN AGREEING TO A NATIONAL REQUEST TO EXPORT ITEMS ON ONE OF THE CONTROL LISTS, COCOM WORKS ON THE PRINCIPLE OF UNANIMITY. NO APPLICATION, IN SHORT, IS APPROVED IF ANY MEMBER STATE OBJECTS. ONE OF THE EVOLVED STRENGTHS OF COCOM IS THAT IN OVER 30 YEARS OF OPERATION, THERE HAVE BEEN VERY FEW CASES IN WHICH A GOVERNMENT HAS EXERCISED ITS SOVEREIGN RIGHT TO GO AHEAD WITH EXPORTS OVER COCOM OBJECTIONS. THIS IS ALL THE MORE REMARKABLE GIVEN THE ABSENCE OF ANY TREATY OR EXECUTIVE AGREEMENT UNDERGIRDING THE ORGANIZATION.

OVER THOSE DECADES, COCOM HAS GENERALLY BEEN SUCCESSFUL IN INHIBITING THE OVERT FLOW OF STRATEGIC TECHNOLOGY TO OUR ADVERSARIES. DURING THE 1970S, HOWEVER, IN THE HONEYMOON DAYS OF DETENTE, THE U.S. AND THE WEST RELAXED CONTROLS OVER A NUMBER OF EMBARGOED COMMODITIES. IT WAS BELIEVED THAT WIDE-

RANGING TRADE WOULD SOMEHOW ALTER THE INTERNATIONAL BEHAVIOR OF THE SOVIETS AND MODERATE THEIR MILITARY INVESTMENT. DURING THIS PERIOD, THE U.S. WENT FROM BEING THE LEAST, TO THE MOST FREQUENT, SEEKER OF EXCEPTIONS TO MULTILATERAL CONTROLS. COCOM ITSELF CAME TO REFLECT SUCH ATTITUDES, AND EXCEPTIONS TO THE EMBARGO WERE ALLOWED TO THRIVE. WE NOW KNOW THIS WAS A MISTAKE. DURING THE PERIOD OF DETENTE, THE WORLD STOOD WITNESS TO THE GREATEST MILITARY BUILD-UP IN HISTORY, ALONG WITH THE INCREASED SOVIET ADVENTURISM THAT GREW OUT OF AN INCREASED SELF-CONFIDENCE.

THE REAGAN ADMINISTRATION CAME TO POWER FIFTEEN MONTHS AGO DETERMINED TO STEM THE FLOW OF THE TECHNOLOGY THAT THE SOVIET UNION AND ITS WARSAW PACT ALLIES WERE USING TO IMPROVE THEIR ALREADY VAST WAR-MAKING CAPABILITIES. IT WAS CLEAR THAT THE WEST'S CRUCIAL QUALITATIVE EDGE IN MILITARY SYSTEMS WAS BEING UNDERMINED BY THE SOVIETS' INCREASINGLY AGGRESSIVE EFFORTS TO BUY OR STEAL OUR MILITARILY-RELEVANT TECHNOLOGIES AND EQUIPMENT.

MORE PRECISELY, WE SAW THIS WELL-ORCHESTRATED ACQUISITION PROGRAM GIVING THE SOVIETS:

(1) A VERY SIGNIFICANT SAVINGS IN TIME AND MONEY IN THEIR MILITARY RESEARCH AND DEVELOPMENT PROGRAMS,

(2) RAPID MODERNIZATION OF THEIR DEFENSE INDUSTRIAL INFRASTRUCTURE,

(3) THE OPPORTUNITY TO ACCELERATE THE CLOSING OF GAPS BETWEEN OUR WEAPONS SYSTEMS AND THEIRS, AND

(4) THE CHANCE TO DEVELOP, WITH ALARMING SPEED, NEUTRALIZING COUNTER-MEASURES TO OUR OWN TECHNOLOGICAL INNOVATIONS.

AS A CONSEQUENCE, THE ADMINISTRATION HAS INITIATED EFFORTS TO FILL IN GAPS IN THE MULTILATERAL EXPORT CONTROL SYSTEM. AT THE OTTAWA SUMMIT MEETING LAST JULY, PRESIDENT REAGAN RAISED THE PROBLEM OF WESTERN TECHNOLOGY TRANSFER TO THE SOVIET UNION. AN AGREEMENT AT OTTAWA TO CONSULT ON THIS ISSUE CULMINATED IN A HIGH LEVEL MEETING IN PARIS DURING JANUARY, THE FIRST MINISTERIAL LEVEL COCOM MEETING SINCE THE LATE 1950S. THE OTHER COCOM GOVERNMENTS HAVE ASKED THAT THE RESULTS OF THAT MEETING BE KEPT CONFIDENTIAL, AS INDEED ARE ALL COCOM PROCEEDINGS. I CHAIRED THE U.S. DELEGATION TO THAT MEETING, HOWEVER,

95-929 O - 82 - 35

AND I CAN SAY THAT THERE WAS A CONCRETE CONSENSUS THAT THE MEMBER GOVERNMENTS SHOULD RENEW THEIR EFFORT TO IMPROVE COCOM EFFECTIVENESS. WE HAVE BEEN ENCOURAGED BY WHAT APPEARS A NEW, AND MORE CONSTRUCTIVE ATTITUDE OF OTHER COCOM GOVERNMENTS, AND FEEL THAT THIS MEETING FORMS A BASIS FOR A REVITALIZATION OF THE COCOM SYSTEM.

SUCH A REVITALIZATION WILL TAKE MUCH HARD WORK AND IT WILL TAKE TIME, AMONG OTHER REASONS BECAUSE COCOM DEPENDS ON THE NATIONAL ADMINISTRATION OF CONTROLS BY 15 INDIVIDUAL GOVERNMENTS. BUT SOME SPECIFIC STEPS ARE UNDERWAY. EFFECTIVENESS, FOR EXAMPLE, REQUIRES PRECISE DEFINITIONS OF MANY COMPLEX TECHNOLOGIES. WE HAVE MADE PROGRESS TOWARD AGREEMENT ON A NUMBER OF SPECIFIC, TECHNICAL PROPOSALS IN THIS AREA TO TIGHTEN THE EMBARGO.

SECOND, THE U.S. IS NOW WORKING ON PROPOSALS THAT WILL EXPAND COCOM CONTROL LISTS INTO PREVIOUSLY-UNCOVERED PRIORITY INDUSTRIES. THESE INCLUDE GAS TURBINE ENGINES; LARGE FLOATING DRYDOCKS; CERTAIN METALLURGICAL PROCESSES; ELECTRONIC GRADE SILICON; PRINTED CIRCUIT BOARD TECHNOLOGY; SPACE LAUNCH VEHICLES AND SPACECRAFT; ROBOTICS; CERAMIC MATERIALS FOR ENGINES; CERTAIN ADVANCED COMPOSITES; AND COMMUNI-

CATIONS SWITCHING AND COMPUTER HARDWARE AND SOFTWARE TECHNOLOGY AND KNOW-HOW. THIS PROCESS WILL CONTINUE INTO THE TRIENNIAL COCOM LIST REVIEW, WHICH WILL TAKE PLACE THIS OCTOBER, WHEN A GENERAL REAPPRAISAL OF EVERYTHING ON THE CONTROL LISTS WILL TAKE PLACE.

THIRD, WE HAVE DEVELOPED WORKABLE PROPOSALS FOR HARMONIZING THE EXPORT LICENSING PROCEDURES OF THE 15 MEMBER STATES SO AS TO MAKE COCOM DECISION-MAKING MORE EFFICIENT. WHAT WE ARE SEEKING ARE WAYS TO BRING NATIONAL ENFORCEMENT PRACTICES TO A LEVEL OF EQUAL EFFECTIVENESS. THESE TWO QUESTIONS WILL BE ADDRESSED AT A SPECIAL COCOM MEETING WHICH WILL CONVENE IN PARIS LATER THIS SPRING -- AND THE FACT THAT ALL PARTNERS HAVE AGREED TO THAT SPECIAL MEETING IS TESTAMENT TO OUR SHARED GOALS.

FOURTH, ILLEGAL DIVERSION ACTIVITIES ARE A PROBLEM OVERSEAS AS WELL AS AT HOME. WE HAVE BEEN COOPERATING WITH OUR COCOM ALLIES TO IMPROVE ENFORCEMENT AND INVESTIGATIVE CAPABILITIES IN THIS AREA. THE STATE DEPARTMENT, WORKING CLOSELY WITH OUR INTELLIGENCE AND INVESTIGATIVE AGENCIES, HAS BEEN CHANNELING APPROPRIATE INFORMATION TO OTHER GOVERNMENTS TO ALERT THEM TO POTENTIALLY ILLEGAL ACTIVITIES

WITHIN THEIR BORDERS. WE HAVE ALSO ENCOURAGED THEM TO INCREASE THE INVESTIGATIVE RESOURCES AND THE SANCTIONS AVAILABLE FOR EXPORT CONTROL ENFORCEMENT. COMMERCE, AND IN TURN CUSTOMS, HAVE DETAILED OFFICERS TO STATE TO SUPPORT THIS OVERSEAS COMPLIANCE EFFORT.

COCOM HAS THUS, WE BELIEVE, MADE MEASURABLE PROGRESS TOWARDS STRENGTHENING STRATEGIC EXPORT CONTROLS SINCE THIS ADMINISTRATION CAME INTO OFFICE. BUT IT IS ALSO CLEAR THAT THE CONTINUING REVITALIZATION PROCESS WILL BE LONG AND HARD. IN ATTEMPTING TO STRENGTHEN STRATEGIC EXPORT CONTROLS ON EXPORTS TO THE SOVIET UNION AND THE OTHER WARSAW PACT COUNTRIES, WE ARE FACED WITH THE PERENNIAL PROBLEM OF SECURING AGREEMENT WITH ALL THE OTHER COCOM ALLIES ON JUST WHERE TO ESTABLISH THE TECHNICAL CUT-OFFS FOR COMMODITIES AND TECHNOLOGIES UNDER EMBARGO. DETERMINING IN MANY SCORES OF DIFFERENT TECHNICAL AREAS WHAT IS SUFFICIENTLY STRATEGIC TO WARRANT CONTROL IS NOT AN EASY TASK. WE DO NOT ALWAYS AGREE ON WHAT ARE MILITARILY CRITICAL TECHNOLOGIES, YET THE PURPOSE OF THE ORGANIZATION IS LIMITED TO SUCH TECHNOLOGIES. MEMBERS EXERCISE CONSIDERABLE CARE TO AVOID CONTROLS WHOSE PRINCIPAL IMPACT WOULD BE

ECONOMIC RATHER THAN MILITARY, AND EACH HAS ITS OWN VIEWS AND PERSPECTIVE. WESTERN EUROPEAN AND JAPANESE ECONOMIES WOULD, GENERALLY SPEAKING, BE AFFECTED MORE THAN THE U.S. ECONOMY BY SWEEPING CONTROLS ON MANUFACTURED PRODUCTS. BUT SUCH DIFFERENCES BETWEEN OURSELVES AND OUR COCOM ALLIES SHOULD NOT BE OVER-EMPHASIZED. WE SHOULD REMEMBER THAT OUR ALLIES HAVE COOPERATED WITH US FOR OVER THIRTY YEARS TO CONTROL SIGNIFICANT AMOUNTS OF EQUIPMENT, MATERIAL AND TECHNOLOGIES THROUGH COCOM. THAT IS, FIRST AND FOREMOST, BECAUSE WE SHARE A COMMON BELIEF THAT SUCH CONTROLS CONSTITUTE AN IMPORTANT ELEMENT IN OUR MUTUAL DEFENSE.

AS YOU KNOW, THE STATE DEPARTMENT IS ALSO RESPONSIBLE FOR ADMINISTERING MUNITIONS EXPORT CONTROLS WHICH COVER DEFENSE ARTICLES AND SERVICES. MUNITIONS ARE NOT APPROVED FOR EXPORT TO WARSAW PACT COUNTRIES. ACCORDINGLY, THE MAIN ISSUE IN ADMINISTERING THESE CONTROLS RELATES TO SECURITY CONCERNS AND OUR FOREIGN RELATIONS WITH OTHER COUNTRIES.

YOUR LETTER OF INVITATION MENTIONS THAT, IN AN EXECUTIVE BRANCH MORE EFFECTIVELY ORGANIZED TO SHAPE AND ENFORCE EXPORT CONTROL POLICY, YOU ENVISAGE A

PRINCIPAL AND EXPANDED ROLE FOR THE DEPARTMENT OF STATE. WE, TOO, ENVISAGE SUCH A ROLE FOR THE DEPARTMENT.

UPON TAKING OFFICE, THIS ADMINISTRATION UNDERTOOK A FULL REVIEW OF OUR POLICY CONCERNING THE TRANSFER OF STRATEGIC TECHNOLOGY TO THE SOVIET UNION AND THE OTHER WARSAW PACT COUNTRIES. THE STATE DEPARTMENT WAS A MAJOR PARTICIPANT IN THIS REVIEW, WHICH CULMINATED IN THE COCOM HIGH LEVEL MEETING. THE STATE DEPARTMENT LED OUR DELEGATION TO THAT MEETING. SINCE THEN, ON A NUMBER OF OTHER OCCASIONS SENIOR OFFICIALS AT STATE HAVE DISCUSSED WITH OUR ALLIES SECURITY CONCERNS RELATED TO TECHNOLOGY TRANSFERS. WE ARE PERSUADED THAT IMPROVED ALLIED COOPERATION ON SENSITIVE TECHNOLOGY TRANSFER ISSUES IS A REALISTIC OBJECTIVE. THERE WILL, OF COURSE, CONTINUE TO BE SOME DIFFERENCES ON THE DETAILS OF CONTROLS AND THEIR APPLICATION TO INDIVIDUAL CASES. BUT, WITH HARD WORK TO IDENTIFY CLEARLY AND TO JUSTIFY PERSUASIVELY WHAT NEEDS TO BE CONTROLLED AND HOW CONTROLS SHOULD BE ENFORCED AND ADMINISTERED, SUCH DIFFERENCES, WE BELIEVE, WILL BE THE EXCEPTION RATHER THAN THE RULE.

* * * * * * * *

1. Q: We believe there may be a need for legislation to define certain kinds of dual-user technology as being of national security significance. This is a very difficult question. The Department's general response would be valuable.

A: The Department believes that it is not feasible to define in legislation what dual-use technology is of national security significance. To be effective, controls must be technically precise. This not only requires detailed lists, too lengthy for legislation, but also continuing review to take into account new technologies which are emerging more frequently and more rapidly than can feasibly be accomplished by the process of amending legislation. Consultation, in a case like this, can of course meet needs not readily solved by legislation. The Export Administration Act now contains broad authority to control exports for security reasons, and specific guidance on the need to control militarily critical technologies. There may be a few refinements which would improve this legislation. However, we believe that the general approach of the Export Administration Act of 1979 is sound. The review of technologies to determine what is militarily critical is difficult and time-consuming. However, we have benefitted greatly from the work done to date. One important indication of this benefit is that we are much farther advanced in our preparation for the 1982/1983 COCOM List Review than we were at comparable periods in preparing for previous List Reviews.

2. Q: The Department's experience in enforcing the Arms Export Control act is of special interest to the Subcommittee. We would find very useful an assessment from the Department of its working relationship with the U.S. Customs Service, which handles the investigative function for the AECA. We would look forward to the Department's views on the problems caused by the separation of the licensing role from the investigative responsibility.

A: The International Traffic in Arms Regulations (22 CFR) 121-128 and 130) promulgated by the Department under the authority of the Arms Export Control act require the persons intending to export defense articles and defense services from the United States obtain a license from the Department authorizing the exports. When a license has been granted, it must be filed with the U.S. Customs Service prior to the actual export. Additionally, a Shipper's Export Declaration must be filed with, and be authenticated by, the U.S. Customs Service. Customs is therefore in a position to review exports of defense articles or defense services for conformity with the statute and regulations.

The U.S. Customs Service has a longstanding and well-established presence at the ports of the United States. The Service is so organized that the performance of the function fits in with its other responsibilities at the ports. The alternative would appear to be the establishment of a second organization at the ports solely for the purpose of processing the export of defense services. In our judgment, this would be redundant, extravagant and wasteful.

The working relationship between the Department's Office of Munitions Control and the U.S. Customs Service's Office of Investigation is excellent. The Department refers to Customs those cases in which there is reason to believe that a willful violation of the statute and regulations may have occurred. Customs informs the Department of instances that come to its attention. On a continuing basis the offices exchange information relating to investigations. Customs regularly provides to the Department reports of investi-

gations on significant cases. Both offices make a concerted effort to ensure that the special agents assigned to investigate alleged violations are knowledgeable as to the statute and regulations, and are furnished such assistance as may be needed. The exchange of views by personnel of the two offices is informal and candid. Customs is apprised of the foreign policy and security interests that may bear upon an investigation. In turn, Customs alerts the Department to any investigation that may involve such interests, and seeks guidance as to a course of action that might be taken.

With some 600 special agents assigned to fifty-eight U.S. ports, Customs can react quickly to a request for an investigation. The particular expertise of special agents and inspectors, with regard to the movement of goods through ports, results in avenues of inquiry being explored that might not otherwise be looked into. The relationship, through the Customs Cooperation Council, of the U.S. Customs Service with the customs services of eighty-seven other nations enables it to obtain information expeditiously which might otherwise take some time to obtain, or which might not be made available. Because of the close working relationship between the Department and Customs, any problems that arise are settled in an atmosphere of understanding as to each other's concerns.

In a separate but related activity, Customs participates actively in the inter-agency committee advising State on approaches to other governments on dual-use exports and has detailed an officer to work on a full-time basis with the office in State charged with this responsibility.

Finally, our experiences suggest that the advantages of separation of the licensing role, from the investigative responsibility, outweigh problems that may arise in the coordination of the two operations. Customs, not being involved in the licensing process approaches a question of violation from a different

3. Q. The Department's views would be sought on the efficiency of the executive branch in enforcing the Export Administration Act. We would find especially valuable the Department's comments on the possible need to improve coordination and communication between the intelligence community and investigative agencies charged with making inquiry into export control violations regarding dual-use technology.

A. There have been major exports to the USSR and other Warsaw Pact countries of items nominally subject to control by the United States and other COCOM member countries. Therefore, improvement of enforcement is a high priority. Specifically, we recognize the need to improve coordination and communication between the intelligence community and investigative agencies. Substantial progress has already been made. An informal inter-agency group chaired by the Department of Justice has brought the investigative and intelligence communities closer together. The intelligence community, Commerce and the Customs service, have reorganized to give a higher priority to this work. The State-chaired Working Group II of the Economic Defense Advisory Committee, charged with international enforcement activity, has increased its activities markedly and has methodically sorted out vast amounts of intelligence and taken remedial action where the information available to us warranted such action. The Administration has been active in alerting other governments to possible illegal activities within their borders and in establishing cooperation between U.S. intelligence and investigative agencies and counterpart agencies in other countries. Economic Defense officers stationed in our

Embassies overseas provide useful leads and other information on diversion activities and consult with outher governments frequently and in depth. The COCOM Subcommittee on Export Controls has also been active in developing improved means of international coordation of enforcement. We are preparing for a meeting of this Subcommittee later this spring which will consider a number of proposals to improve coopration on export control enforcement and better protect sensitive items in transit.

4. Q: Please provide the Subcommittee with the specific steps the Department is taking to improve the efficiency of the executive branch in defining and then executing export control policy.

A. Our export control policy is reflected by what is actually controlled, how these controls are administered, and what can actually be licensed for shipment. We are taking the following steps to improve the efficiency of the executive branch in these areas:

a) State is working closely with interagency Technical Task Groups which have been established to define specific items of strategic concern. These groups are developing technical proposals and justifications for revising the COCOM lists. They are identifying items which should be considered for addition to the lists and items now on the list which need to be clarified or which may no longer be of strategic concern.

b) State is expediting the U.S. review of COCOM cases and its own agency consideration of domestic export license applications submitted either to Commerce (dual-use items) or to the Office of Munitions Control (munitions items). State's role includes efforts to insure that case decisions are consistent with policy and are equitably applied by researching precedents and other data available from earlier COCOM list reviews, from cases, from industry, and from intelligence agencies.

c) State is leading negotiations with our allies to strengthen the enforcement of multilaterally agreed controls and to harmonize licen ng procedures, including the development of standards for the consideration of license applications in COCOM member countries.

5. Q: Preliminary inquiry has revealed that COCOM nations have not always made export controls a high priority with reference to technology transfers to the Soviet Union and Eastern Bloc. We would want to know the Department's assessment of that preliminary finding. Moreover, we would want to know if the Department believes the goal of achieving full-scale cooperation from COCOM is a realistic objective for this nation's foreign policy.

A: Cooperation from COCOM is a realistic objective, as evidenced by the continuing effectiveness of the organization for more than 30 years. We are doing all we can to further the objective of "full scale" cooperation.

Of course, "full scale" cooperation is unrealistic if, by that expression, is meant Allied acceptance of whatever the U.S. proposes. Indeed the very concept of cooperation involves a willingness to listen to what the other party can constructively contribute to solving the problem. However, there has been a good track record of COCOM acceptance of those U.S. proposals which have been technically precise and well justified in terms of military criticality and Soviet deficiencies, and there are also many useful proposals from other COCOM members to strengthen and/or clarify controls.

Other COCOM members have not devoted as much resources as we believe necessary to the enforcement of controls. We are stressing to them the need to increase their resources as we are doing. As a result, their awareness of the need to improve enforcement has definitely increased.

6. Q: A preliminary finding in the inquiry is that the U.S. Customs Service could be more effective in investigations of export control violations if it had more agents assigned to U.S. missions in certain countries with high technology industries. What is the Department's general response to the preliminary finding?

A: The Department of State agreed that Customs would be more effective in investigations of export control violations if it had more agents assigned to U.S. missions in certain countries with high technology industries. State is now reviewing Customs Service request for such additional overseas slots. The ultimate decision will rest with the Chief of Missions overseas. There is, of course, a continuing need for close coordination of U.S. Government activity overseas, under the leadership of the Ambassador. Moreover, there are frequently extremely sensitive political and legal aspects in the conduct of overseas investigations occasioned by host government insistence on jurisdictional rights which need to be addressed by other elements of our overseas missions. But the degree of Allied consensus on the need to strengthen enforcement of COCOM Controls in combination with the professionalism of the Customs Service leads us to believe that mutually satisfactory arrangements will be possible in the future as they have been in the past.

PREPARED STATEMENT OF MICHAEL LORENZO

STATEMENT ON ROLE AND RESPONSIBILITIES OF DEFENSE RESEARCH AND ENGINEERING IN EXPORT CONTROL

Mr Chairman:

Thank you for the opportunity to testify before the U.S. Senate Permanent Subcommittee on Investigations.

Dr. Frank Kapper, Director of Military Technology Sharing and Dr. Oles Lomacky, Director of the Office of Technology Trade are also here to support this testimony.

This statement deals primarily with the technical policy and assessment aspects of technology transfer functions as they pertain to West-East strategic trade (Dual Use Technology).

This statement on East-West trade is divided into three parts; Defense roles and responsibilities, Defense accomplishments and Defense concerns as related to export control.

Roles and Responsibilities:

In accordance with current Department of Defense Directives, the Under Secretary of Defense for Research and Engineering is the principal advisor to the Secretary of Defense on all technological and scientific matters, including the formation of policy thereto. Within Research and Engineering, International Programs and Technology (IP&T) is charged with a variety of specific technology related duties.

In addition to its international program responsibilities, which in themselves involve a number of technology transfer issues, IP&T is also responsible for development and maintenance of the Militarily Critical Technologies List which is so necessary for the important function of performing technical assessments, reviewing control lists (CoCom, CCL) as well as providing overall technical policy direction for the Department of Defense. One of my first requirements as an incumbent in office since 1 October 1981 was to distinguish between techni- policy and international security policy in order to clearly delineate responsibilities between IP&T and its counterpart in the Office of the Under Secretary for Policy.

Technical policy is that which is pertinent to the operational, technical and acquisitional aspects of technology transfers (T/T), including Foreign Military Sales (FMS), munitions, and dual-use export control cases, critical technologies identification, U.S. and Coordinating Committee (COCOM[1]) embargo list reviews international programs and related activities, Committee on Exchanges (COMEX) activities and NATO technical matters, such as Data Exchange Agreements (DEAs), and Memoranda of Understanding (MOUs). International security policy is the responsibility of the Office of the Under Secretary for Policy. The Policy Office responsibility is pertinent to the broader considerations of international security, political and economic aspects of export control, which tie national policy with military interests with respect to countries and/or regions. In these efforts the Services, other Defense Agencies and the Intelligence community support both the OUSDRE and Policy offices in threir primary roles.

Notwithstanding the delineation of responsibilities, the primary goal of Defense is national security which includes prohibiting the export or acquisition of critical equipment and technology by potential adversaries that could add "significantly" to their military capabilities. This includes all transfer mechanisms both legal and illegal whether the acquisition is from the United States or involves a direct sale or reexport from other countries. In order to achieve this, Defense has established goals with respect to the improvement of source documentation (MCTL[2], data base, etc.), control lists (COCOM, CCL[3], etc.) and case processing (timeliness, consistency, substance, etc.).

---

[1]COCOM (Coordinating Committee) - A voluntary organization consisting of the NATO Countries less Iceland plus Japan that controls dual use export to the East bloc of countries.

[2]MCTL - Military Critical Technology List as required by the Export Administration Act of 1979.

[3]CCL - Commodity Control List under cognizance of the Department of Commerce.

Pursuing these goals has resulted in major workload increases in the last year, particularly with the focus on export controls by this Administration. Both the State and Commerce Departments have increased the level of activity in compliance matters, thereby necessitating more technological inputs and other help from Defense. As an ancillary requirement, it is important for Defense to support Customs' officials to aid in identifying equipment being exported to ascertain whether a validated license is required. According to the Export Administration Annual Report for Fiscal Year 1981, Customs detained 628 questionable shipments of which 160 were attempted illegal exports. By training customs officials and providing some basic guidelines on how to recognize or identify high technology items that are subject to national security controls, Defense hopes to raise the batting average of customs in detaining illegal shipments. It is important to our national security interests that violations of our export controls are quickly identified and properly detained. It is equally important from an economic standpoint that legitimate exports are not unnecessarily detained. In establishing our technology transfer policy, we are mindful of the fact that we work in a free trade system and open society that is a fundamental source of our greatness. It is also recognized that a strong and viable economy is necessary to develop and maintain a strong defense.

Accomplishments

A number of corrective steps have been taken to enhance our performance in these areas. The staff was increased for license application reviews, trained in efficient application of the necessary technical skills to the review process, and management procedures were instituted for orderly and thorough application processing. All agreements with the Department of Commerce have been reviewed, including Delegations of Authority and procedural agreements. An interface has been structured with the Services in seeking their technical and military

expertise, and an excellent relationship exists with the Defense Intelligence and National Security Agencies leading to their active participation in license application review. As a result of these actions, the old backlog of applications awaiting review has been eliminated in recent months completely adhering to the time limits imposed by the Export Administration Act of 1979. We are holding no applications for more than 60 days, and currently are processing only 44 applications for a period of more than 30 days. Coincidentally, industry members are now beginning to appreciate that many of the licensing delays which they have experienced had been unfairly laid at the door of Defense.

The involvement by the Intelligence Community has increased now to processing over 100 cases a month compared with the previous figure of 25 per year and their increased efforts have aided the Defense effort immeasurably.

Defense has achieved consistency and efficiency in processing applications. This was done by pursuing an approach, not only in license processing, but in the many other efforts, which stress the control of technology. This is best exemplified by the work on the Militarily Critical Technologies List (MCTL).

As you know, the MCTL was generated in response to the Export Administration Act of 1979, and the first version was published in October of 1980. We set about refining the list, adding some items and rejecting others. The generation of the list and its refinement represented a large, cooperative undertaking among our technical people, technical specialists from the Services, Services laboratories, other government agencies and industry. The first major opportunity to implement the MCTL was to improve the multilateral controls on export control to the Warsaw Pact in the COCOM List Review preparations that began with the formation of Technical Task Groups (TTG's) last fall. The government is now in the midst of reviewing the COCOM list and finalizing U.S. proposals for negotiations sche-

95-929 O - 82 - 36

duled next October in Paris, the headquarters of COCOM. Defense participation in the List review has concentrated on ensuring that the U.S. government proposals for COCOM consideration include all the Militarily Critical Technologies as well as removing products from control where possible so that we and our Allies will be acting in concert in controlling only what is important. The U.S. is working more closely with the COCOM nations although potential for real problems exist as we move to close the rather wide gaps in coverage of flows of critical technologies and goods to the Warsaw Pact.

The MCTL has provided an important mechanism for cementing our relations with industry and for exposing our concerns and the mechanics of our operations. The results have been most rewarding. An association of industry associations, the Multi-Association Policy Advisory Group (MAPAG), has been working with us on these issues, and approximately 80 companies are currently reviewing the 1981 revision of the MCTL.

Defense continues to examine the Export Administration Regulations to see if there are constructive suggestions we might make to improve their effectiveness. It was determined that Section 379, Technical Data, was indeed the major sieve through which our technology had been leaking. This section was deemed both arcane and ineffective. As a result, we called upon the MCTL once more and extracted from it the lists of "arrays of know-how" developed in the famous Defense Science Board Bucy Report. A proposed revision of Section 379 has been drafted, based on these arrays of know-how and is currently being coordinated throughout the Department of Defense. In due course, it will be submitted to Commerce for their consideration, and to industry for review and comments.

Excellent progress has been made in the development of our data base. Our approach has been to develop a system which, though simple at first, is always useful as it grows since it is formatted to fit the future automated DOD Management Information System known as FORDTIS (Foreign Disclosure and

Technical Information System). It started as a modest system on word processors which provided the data for our monthly reports. It has since been expanded and moved to a greater computer capability. The next step is to integrate our system into FORDTIS which will be the primary DOD management tool to be shared by other agencies for tracking all high technology exports. Into this data base we have entered a large number of cases from 1980 and 1981 as well as the present ones to afford consistent guidelines of a scientific analytic predictive nature. Also included in FORDTIS is the MCTL data base. The MCTL together with a keyword in context index and an index to the Commodity Control List (CCL) are already included. Defense now has an effort underway to revise, update, and reformat the 10,000 pages of supporting documentation for all items on the MCTL so that all of this information may be available to FORDTIS users. The management improvements available from better use of this vast store of concentrated information are expected to be considerable. This data base will greatly support control lists, COMEX and other case reviews as well as policy activities.

As a related activity, significant efforts to collect a volume of information on foreign availability of critical technologies and related keystone equipments are underway. The intelligence community and the industry establishments have been requested to thoroughly assess foreign availability and adversary capabilities on each and every item in the MCTL. Although the Department of Commerce is the focal point for such information per the Export Administration Act, the Department of Defense believes that, by definition, the assessment of foreign availability (in similar quality and quantity) requires primarily technical and intelligence capabilities. We will of course provide such information to the Department of Commerce as the primary repository.

In summary, Defense has made major strides in stressing technology control, such as the MCTL development and application. It also developed a cooperative relationship with industry and brought efficiency and effectiveness to our review of license applications.

Concerns

Currently there is not sufficient specificity with respect to Country/Regional guidelines to enable a case processor to differentiate between various countries and/or regions. This is not too much of a problem from a technological standpoint if one is dealing with the countries of Eastern Europe because technologically all the Bloc countries should be treated essentially the same. The only advantage would occur in handling borderline cases. However, lack of specificity is a major concern in viewing exports to the free world. Defense is working with State and Commerce to improve the situation. Under the Export Administration Act of 1979, Defense has the authority to review and object to proposed sales to free world countries provided the equipment is controlled for national security. For the purposes of clarifying this point, an example is the sale of production equipment and know-how for the manufacture of state-of-the-art integrated circuits, an area in which the United States is a leading supplier in the world today. If sales of this equipment are not carefully controlled and special negotiations completed with the governments of the recipient companies, the thrust of our control efforts within COCOM may be readily undermined by the ensuing foreign availability sources created by such sales. This is a very complex issue which has significant National as well as International overtones. The true scope of this problem is not fully known at this time, but Defense will have to become more directly involved.

Our national security interests are not truly represented when we group all our NATO Allies, Japan, Australia, and New Zealand into the same Country Group for export purposes as Neutrals and Third World Countries. Commerce has proposed a change to this Country Group structure to which Defense has heartily concurred. In the interim, it is incumbent on Defense to establish more specific strategic and technical policy guidelines with respect to the Neutrals and Third World Countries, based on the integration of our political, economic and military interests. Exports to those countries that are not supportive of U.S. policies or to which intelligence advises us to be wary, may appropriately require Defense review.

The Soviet Union has made a concerted effort to exploit scientific exchanges and all technical information available in order to enhance their military posture. The extent of the problem has caused Defense to review its own procedures of controlling unclassified technical data. The Services and other Defense Agencies have established procedures to limit the unstructured release of technical papers from their laboratories and research centers. Other representatives from Defense who are scheduled to testify before this Committee will more appropriately address this subject. In an open society such as ours, the opportunity for a potential enemy to collect meaningful information is extensive. However, the diffusion of technology and information to all sectors of our society, particularly academia and the small R&D firms, is one of the U.S. cornerstones to solve Defense's technological problems and to maintain our technological lead. Different sectors must talk to each other and exchange data to lead to innovation and technological advancement. This is a strength of our society compared to the closed society of the USSR. Defense relates its technology transfer concerns to small industry and academia which generates much of our new technologies. The Soviets know this and will exploit these segments of our technology base if we don't communicate better and more directly with them.

A significant cross-section of highly skilled executives, technicians and scientists from Industry, Academia and Government has been trained in the fundamentals of export control through participation in the development of the MCTL and our COCOM proposals. These personnel constitute a major resource for license application review. It is equally important to keep them current with respect to the status of export control issues. This would have an ancillary benefit by providing an expeditious channel for identifying emerging technologies for consideration of possible control. In order for the Defense facilities to support export control on a continuing basis, it is necessary to identify a centralized program element in the Defense budget for this purpose. The

Services have been requested to do theirs starting in POM-84. These specific actions are necessary management improvements within the context of improving and simplifying our directions to the Services and Defense Agencies to better support us in technology policy development and technology assessments for improved export control for national security purposes. This will help close the loop in the control of technology transfer within Defense.

There are other areas which require Defense's attention. These include more active participation in the various committees chaired by either State or Commerce, such as the Committee on Exchanges (COMEX), Working Group 2 on compliance issues and the Technical Advisory Committees. An increase in permanent staff would obviously overcome this problem.

In closing, I am certain that Administrative policy regarding improved controls on technology transfer to the Warsaw Pact is clear. As a result of our dedicated effort to implement that policy, Defense has achieved significant successes and incurred significant problems. To follow-up and maximize the value of our present successes, we need to improve upon our resources in all technical and intelligence sectors of Defense. There is a need to improve the direction and management control of these resources via new DOD Directives and Program Elements Attempts are being made to communicate more effectively with industry and academia. And, finally, Defense needs to improve multilateral controls in concert with our Allies and other parties having mutual interests. These areas represent major challenges and opportunities for us in the coming months and years. Thank you, Mr, Chairman.

MICHAEL LORENZO

Michael Lorenzo, P.E., was appointed as the Deputy Under Secretary of Defense (International Programs and Technology) in the Office of the Under Secretary of Defense for Research and Engineering (OUSDR&E) on October 1, 1981. He is responsible for technology transfer issues and for all international activities in Defense research, development, and acquisition, serving as the focal point for international cooperative R&D efforts related to defense and for the management of activities involving export control, munitions cases, and equipment transfer to foreign nations.

Prior to this appointment, he served in a variety of application engineering and managerial positions at the Defense and Electronic Systems Center and Civil Systems Division of the Westinghouse Electric Corporation for sixteen years. At Westinghouse, his responsibilities included Manager of Military Planning for Defense, Oceanographic and Space activities; Manager, Air Resources of Westinghouse Management Services, Inc.; Director, Westinghouse Environmental Quality Control and DOD Marketing Specialist. Mr. Lorenzo joined Westinghouse following a distinguished thirteen-year Civil Service career with the USN and USAF where he served in mechanical, aeronautical and aerospace positions including PEM of the USAF Manned Orbiting Laboratory Program during its initiation in 1964. Throughout this period, management and executive functions included work with and for the U.S. intelligence communities with respect to the collection, processing and production of information with additional responsibilities to provide guidance to Westinghouse and Department of Defense organizations while serving on active status as a reserve Rear Admiral. He directed and managed efforts in planning, programming, budgeting, systems analysis, operations research, financial investment and analysis, conceptual engineering, systems development, political assessments and human sensitivity evaluations in the markets of Defense, Intelligence, Environmental Quality and Civil Systems.

Other experiences included three years with the Fischer and Porter Company as a field industrial instrumentation engineer, association with the Stanford Research Institute as a consultant developing models for simulation of OEO programs, and airline pilot with TWA.

In addition to his industrial and governmental experience, Mr. Lorenzo also had a distinguished military career which included over 140 combat sorties flown as a naval aviator in combat zones during WWII and the Korean conflict. During this time, he was the recipient of sixteen military decorations including the Distinguished Service Medal, two Distinguished Flying Crosses, and seven Air Medals, and the Air Force Commendation Medal retiring from the Active Reserves as a Rear Admiral (upper half) in 1973. Admiral Lorenzo started his military career as a member of the Army Corps of Engineers transferring to the Navy as a seaman 2/C immediately after the Pearl Harbor attack. He received the earliest possible accelerated promotions to the maximum attainable ranks permitted by law for reservists.

A Registered Professional Engineer in the District of Columbia and the State of Maryland, Mr. Lorenzo holds three Civil Service engineering ratings and is the author of approximately 70 publications in aerospace and other technological areas including a book and a patent. He is a member of the National Society of Professional Engineers, American Society for Engineering Management, and an Associate Fellow of the American Institute of Aeronautics and Astronautics.

Mr. Lorenzo graduated from Pennsylvania State University in 1947 with a B.S. in Chemistry and Physics. He received his MEA from George Washington University in 1956 and later completed further graduate work toward a Ph.D at GWU and the USDA Graduate School.

Mr. Lorenzo was born in 1920 in Newton, New Jersey. He and his wife, the former Anastasia Hackett, have five children and three grandchildren.

MILITARY TECHNOLOGY TRANSFER

delivered to

American Society for Engineering Management

at

George Washington University

11 March 1982

by

MICHAEL LORENZO, P.E.
Deputy Under Secretary of Defense
Research and Engineering
(International Programs and Technology)

Fellow members of the American Society of Engineering Management, it gives a warm feeling to be invited back to my Alma Mater. This is the institution of higher learning that awarded me an MEA degree in accordance with the academic demands of Dean Mason, Dr. Jack Walters, et al, befitting the style of Kate Turabiam. This degree has been a great management tool for me over the years, particularly in my present assignment--the OUSDR&E International Programs & Technology (IP&T) is responsible for all technology transfer functions among the DoD to all nations and is a truly multi-discipled set of functions.

Technology - The International Language

When the super beings, in my case the good Lord, created the Earth, he endowed all peoples with creative and logical powers in all ethnic groups barring none. At the same time, endowed in everyone on the surface of this earth were the Physical Scientific Laws of Nature.

As different groups evolved, some developed these Laws more than others for the fundamental purposes of enhancing and improving the quality of life, property and welfare. Free societies like ours soon learned that we had to protect these wonderful assets from others with some form of security such as police and armed defense capabilities. While good peoples developed the Laws of Nature for the good of society in general, others used technology to capture or destroy the life, property and welfare of others. Accordingly and unfortunately, some forms of high technologies have to be controlled from the use of potential adversaries. This is a very difficult thing to do and short-lived at best.

For many centuries, engineers and scientists like you and I who have done various forms of scientific research in Universities, Industry and elsewhere were bonded by a Code of Ethics to help our fellow beings by sharing our findings, particularly in the fields of health and comfortable living. This rapport and environment is essential to academia and others to promote a healthy research environment and to promote human understanding. As a result, the Physical Scientific Laws of Nature are in reality an International Language.

In recent months, I have headed U.S. Defense Technological country-to-country cooperation teams in several foreign countries and experienced this phenomenon first hand. As a guest of the Japanese Government and the Kyoto Ceramic Company in the cities of Kyoto and Kagoshima, we became involved with the Japanese researchers concerning their ceramic gun barrel and engine developments among other things. The interpreter was needed for most conversations except during the two-way discussions concerning the ceramic automobile engine, when such subjects as Carnot's Laws of Thermodynamics, dynamometers, torque, stoichiometric temperatures, etc. were discussed. Only scientists and engineers could ever experience such an event and understand each other Internationally! It is indeed too bad that our lawyers, political scientists and politicians cannot ever experience such a dialogue!

Incidentally, the ceramic hot parts, (pistons, piston sleeves, piston head caps, turbo supercharger shaft and turbine assemblies including blades) permit stoichiometric combustion temperatures, hence an approximate 8 to 15 percent increase in fuel efficiency is achievable in a diesel engine requiring no water cooling system! After establishing this International Technology rapport, the chief researcher levied with me saying that they expected such an automobile engine to enter service in approximately 1 to 2 years and attain a 500,000 mile line.

The management of Kyoto Ceramics (KYOCERA) paid a heart-warming compliment to me by connoting that I was now a member of this International Language Team by awarding me a company work uniform jacket with insignia. A recent article describing Kyocera's products, organization and management appeared in the February 18, 1982 issue of the New York Times Business section. The Japanese are using ceramics widely making other products like false teeth, semi-conductors (mostly packaging for sophisticated silicon chips), ceramic cutting tools, pen tips, solar cells, synthetic gem stones, artificial bones and other biological implants.

Here we go again, the U.S. was the original leader of robotics and ceramic engine parts research ten years ago, and now lags behind Japan in its application! Why? There are a lot of reasons, most of which I will leave for the Q's and A's to follow. However, before leaving this subject, one must give Japan credit for their progress principally due to one major reason; namely, they have a great Government-to-Industry relationship, not adversarial like ours which this Administration is changing with time.

The bottom line of technology transfer is, "Yes, you can control some critical technologies, but this is good for the most part only for a few years because when one country has demonstrated something, this generally provides enough motivation for another country to pump in the resources and achieve a like type capability" -- nuclear energy is a classic example. However, we can and must do two things; namely, keep our technological R&D base strong with a healthy lead time and be smarter than any potential adversary.

"DoD Technology Transfer 1981"

During CY 1981, IP&T processed almost 8,000 munitions cases that were referred to us by the Department of State (DOS). Another 23,000 cases were processed by the State Department without referral to DoD. These cases included such things as

exports of 12 gauge shotgun shells and .22 ammunition going to a NATO nation for example. These exports of goods and technologies are covered by a National Security Decision Directive entitled, "Conventional Arms Transfer Policy" signed on July 8, 1981 by the President, and the Arms Export Control Act of 1976 (as amended). Most of these goods and technologies go to our Allies and other friends and are made for the primary purpose of enhancing military capabilities of mutual interest. We find this new Presidential Directive to be an excellent policy, rather straightforward to implement and effective in nature. The number of ITAR (International Traffic in Arms Regulations) cases have been increasing at a rate of 25% per year and are becoming ever more complex in nature. This is a rapidly expanding market. Included in these technology transfer (T/T) functions are Foreign Military Sales, dual-development, co-production, Data Exchange Agreements and selected sections of numerous Memoranda of Understanding.

"T/T Rejection Rates"

That's the good news--growing at a rate of 25% per year. Now for the bad news, the rejection rate was greater than 5% in 1981 compared to less than 2% one year prior. Along with the 1981 rejection rate of 5%, one must add that a lot of cases were approved with exceptions--some people call these constraints, gates or fences. For example, we quite often approve an export license for an advanced turbo jet engine to a foreign country while retaining all of the design, manufacturing and production of the hot sections which have to be purchased from us. Needless to say, an unworthy "friend" could reverse engineer these hot sections but at a tremendous expenditure of resources. The Munitions List contains Military or Single-Use technologies.

Many technologies are primarily developed for civilian use but have military significance. These are called Dual-Use technologies. Industries with these products seek license for export from the Department of Commerce Commodity Control List, which is screened for "significant" enhancement of the military capabilities of a potential "adversary" as outlined in the Export Administration Act of 1979. Of the approximate 86,000 cases received by the DoC in 1981, 3,500 were referred to DoD of which 1,500 were of a COCOM consideration. Here again, many "precedent" cases are delegated to Commerce by DoD once the "performance thresholds" are established and all parties agree to them, which is rather hard to achieve. The acronym COCOM stands for Coordinating Committee which is a voluntary organization established in the 1950's consisting of the NATO nations less Iceland plus Japan. COCOM convenes in Paris for the primary purpose of controlling East-West trade of Dual Use technologies. Computers and associated products are the most prevalent products of the Dual Use technology category that have military implications.

Some people -- consisting of politicians, lawyers and political scientists for the most part -- have created the buzz words "technology hemorrhaging" for the decade of the 1980's. Such a dual use technology transfer case creating this image is Kama River. We must regret the Kama River truck facility. The U.S., France, Italy, UK, West Germany and Austria financed and built the most modern and largest heavy truck facility in the world. The general contractor was Mack Truck Inc. of the U.S. Assurances that these trucks would be for the civilian sector were not kept; many of the heavy vehicles used in the invasion of Afghanistan were manufactured at the Kama River facility. Incidents such as these are not the norm, yet they have happened; and we are insuring that our mistakes are not repeated. The bid has been tightened considerably in this area since, in 1981, we experienced a 15 percent rejection rate compared to less than 2 percent a few years ago. However, the number of Dual Use cases is growing 15-20 percent per year.

In other words, IP&T processes a combination of 1,000 T/T cases per month, plus approximately 3,000 MOU's/DEA international programs per year, which makes it one of the busiest shops in DoD. The International Programs which have a lot of T/T in them are very synergistic with the T/T cases in general. It is interesting to note that over 90 percent of the T/T case processing activity within DoD is technical assessment, the other being Policy and Military considerations.

Sensitive technology is not licensed for sale to potential adversaries. To insure that such technology is not acquired by unfriendly countries, MOU's concerning USG-approved security procedures and re-export assurances are negotiated with all friendly countries and apply to their companies that receive sensitive U.S. technology.

Further assurances that sensitive technology is transferred only to destinations that will not adversely affect U.S. national security are gained through the National Disclosure Policy Committee (NDPC) review process. The NDPC is chaired by DoD and includes representatives from DoS, DoE, CIA, OJCS, and the military departments. The purpose of the NDPC is to establish policy concerning the release of classified/sensitive military information and systems to countries with which the U.S. has trading relations and to consider requests for exceptions to that policy. The NDPC also also participates in the decision making process on export license applications involving the the release of classified information when special concerns arise with respect to foreign government eligibility.

T/T Enforcement

Enforcement responsibility resides with DoC Compliance Division and Bureau of Customs; prosecution is handled through Department of Justice. Currently efforts are underway to improve export control enforcement through the Interagency Working Group on Export Control Enforcement. The departments and agencies participating are Justice, Treasury, Commerce, State, CIA, FBI, Defense and the National Security Council.

Multilateral Export Control enforcement is also being studied through the COCOM High Level Group (HLG) and the NATO Technology Transfer Study Group. The COCOM HLG is evaluating current COCOM controls on the nine defense priority industries in an effort to strengthen those controls. The NATO Technology Transfer Study Group has been established to involve the foreign MOD's in the export control arena and possibly establish an overriding veto for the MOD's in third party transfers. Recent analyses conducted by competent authorities show that less than 25% of the adverse critical technology leaks have gone through legal means which leads us to the conclusion that the current regulations mechanism is more effective than some people think. The efforts underway to improve enforcement are focused on clandestine and illegal acquisitions and should prove quite successful in reducing undesirable T/T.

In closing, DoD will continue to stress as its primary role in technology transfer:

1. Improving and maintaining the U.S. technology base through adequate RD&A resources;

2. Improved armament cooperation with our allies including technology transfer; and

3. Control of transfer of military technologies and dual-use technologies to potential adversaries.

You have been a wonderful audience; the podium will now entertain questions.

Thank you.

STATEMENT OF
CHARLES P. LECHT
FORMER PRESIDENT
ADVANCED COMPUTER TECHNIQUES CORPORATION
NEW YORK, NEW YORK
BEFORE THE
U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
MAY 11, 1982

Mr. Chairman, Senators, my name is Charles Lecht. I am pleased to appear here today to contribute to this Subcommittee's examination of the transfer of American technology to Soviet Bloc nations. During the course of your staff's investigation and these hearings, you have studied that problem, mindful of the views and interests of government, the intelligence and defense communities, law enforcement, and the public itself. Let me now focus your attention on the issue from the viewpoint of that sector which, by all reports, is the target of these Soviet efforts: America's high technology industries.

Until April 26, 1982 I was President and Chairman of the Board of Advanced Computer Techniques Corp. (ACT), a computer software consulting firm which I founded in 1962. Holding a Bachelor of Sciences degree in mathematics from Seattle University and a Masters of Sciences degree in mathematics from Purdue University, I have been actively involved in the computer field since 1951, including the authorship of five books. My company has been in existence now for some twenty years, regularly conducting business with foreign governments, U.S. subsidiaries abroad, multi-national corporations, as well as the United States government. ACT currently employs over 350 persons in both national and international offices, with over fifty per cent of the company's income currently derived from business abroad. We produce computer program software, synthetic languages, and operating systems. On numerous occasions, we have been chosen as subcontractor on U.S. government contracts. As but one example, ACT is responsible for some of the software used in the production of the F-16 airplane.

My years of experience in the field reinforce what this Subcommittee has already heard: the Soviets are engaged in a concentrated effort to seek out and obtain the secrets of America's technology giants. From a personal standpoint, the problem has "hit home" on several occasions during years with ACT.

One of ACT's frequent sources of business and consulting contracts has been the country of Yugoslavia. ACT has become one of the best known American firms operating in that country. Consultant work is prohibited in Yugoslavia except by consent of the government. ACT prospered there, under the auspices of

the necessary government approval. As a systems analyst, we provide advice on what the Yugoslavs should buy and at what prices so that they will not be easily cheated on the American marketplace.

About seven years ago, I had been conducting some ACT business with Honeywell's Yugoslavian sales agents. A Yugoslav Honeywell representative invited me to lecture in Yugoslavia on the current state of computer technology. At first blush, this was not an unusual request -- I had already given numerous speeches in Yugoslavia, as well as in the United States and elsewhere. I understood that the lecture was to be given to Yugoslavs. I did not expect nor was I prepared to address a select corps of the Russian military. Nevertheless, in my discussions with the sales agent just prior to the speech, he told me, somewhat reluctantly, that more than a few representatives of the Soviet military had come "from all over Russia" simply to attend my lecture. I responded by flatly refusing to give the speech. He was visibly upset, but I remained firm in my refusal.

Later that evening, I received a phone call in my Yugoslav hotel room from an individual who identified himself as a general in the Soviet military. He told me that he made the trip to Yugoslavia solely for the purpose of hearing my lecture. He urged me to reconsider my decision. Despite my refusal to do so, the "General" persisted. Finally, he asked me, at the least, to meet him for a drink. I had no desire to speak or drink with the Soviet military and politely declined his invitation.

That incident occurred at least seven years ago. As of last fall, I had not seen nor heard from the sales agent since. Strangely enough, on the very day after this Subcommittee's staff first interviewed me on this subject last October, he phoned me to set up a meeting in my New York office. At that meeting he introduced me to a Yugoslavian businessman who accompanied him. When I reminded him of the aborted lecture incident, he responded with a somewhat nervous laugh and quickly changed the subject.

In another setting, our company has also been confronted with the problem of Soviet approaches to American subsidiaries working abroad. ACT has had a subsidiary located in Milan, Italy. Milan is recognized as an international center for businesses involved in highly advanced technology. In fact, most of America's high technology companies do research and development work in the area.

95-929 O - 82 - 37

As a booming technology center, Milan also accommodates companies from Western European as well as Soviet Bloc nations. In fact, after General Electric began selling computers directly to the Soviets through their Italian subsidiary, they established a GE center in Milan for the express purpose of training Soviet personnel in computers. The Soviet contribution in Milan, however, goes beyond the placement of trainees and legitimate technology companies. It is common knowledge amongst the Milan technology community that Soviet intelligence agencies are more than amply represented in Milan. A restaurant, La Notte, was a favorite hangout.

ACT's business manager in Milan, Jean Patrick Rousseau, was directly approached for information by the Soviets. Identifying himself as an official of the Soviet Chamber of Commerce, the individual asked Rousseau to provide software information and services. The Soviet was specific to Rousseau as to the manner and method to be employed in the proposed deal: he was to pay Rousseau personally with an agreement that there would be no record of the payment or the work performed. When Rousseau related the offer to me, I told him not to deal with that individual or with any other Soviets. Some time after this incident, Rousseau was again approached by another individual from the Soviet Chamber of Commerce with a similar request. As before, Rousseau refused to cooperate.

Clearly, and from all reports, there is a serious and focused attempt by the Soviets to unveil the inner workings of our high technology. Although American initiatives are as yet ill-equipped to deal effectively with the problem, there is, at least, growing recognition that the problem exists. I also see, however, a disturbing development which does not bode well for our future ability to combat technology transfer. The United States, in both government and public circles, has been seriously misled as to the true nature of Soviet efforts to transfer technology. We continue to operate under an absolutely crippling misconception of what the Soviets are stealing and why they are doing so.

It is often said that the Soviets are seeking our technology on a broad scale in order to copy what they are incapable of creating themselves. Mr. Chairman, over twenty years of experience in high technology tells me that their true purposes are much more precise. The Soviets are stealing our technology selectively for military purposes, and military purposes only.

Contrary to popular belief, the Soviets are <u>not</u> significantly behind the United States in the level of technology achieved. In 1980 the Soviets estimated

their yearly production in computer technology at $10-11 billion and growing. Even by American estimates, their yearly production nears $6-7 billion per year. By comparison, American production of new computer technology was $11 billion in 1980.

An analysis of those figures exposes the obvious fallacies in what I will term the "underdeveloped" Soviets theory. Soviet production is by and large new production -- in contrast to the United States, there is, by deliberate choice, no mass production of consumer goods in the Soviet Union. Moreover, theirs is a 75% agrarian economy -- with no banks, no consumer sector, no hotel industry. There is therefore no real need for the white collar computerization which we recognize as a fact of life in the United States. Our industry is 75% of white collar. Thus one wonders what Soviet technology production, currently very near our production, is used for, if not primarily military purposes. To be sure, some is in factory automation, but I am of the opinion that this could not but account for a fraction of the massive production under way.

By contrast, American high technology production is spread over a vast spectrum of industries in both the public and private sectors. Frankly speaking, it is pure "myth" that the Russians are so far behind us technologically. There is more scientific literature printed in the Soviet Union than anywhere else in the world. Intelligence is not, unfortunately, a privileged or solely American commodity.

Years ago, the Soviets were, by comparison, more interested in purchasing American technology for use and for copying. The reason was simple -- they were just starting out in the field and they were broke. If you are surrounded by a sea of countries characterized as technological supermarkets (to the Soviets, a circle of traditionally high technology countries), and have very limited investment capital, you buy what is easily available in order to better focus capital on what you most have but cannot easily buy. To the Soviets this has always meant food and arms.

In the 1980s, the Soviets have far less dependency on surrounding technological "supermarkets". They have acquired some of them (Czechoslovakia, Hungary, Poland, East Germany) as well as the means and the know-how to create and operate their own. The truth is that the Soviets no longer want our technology solely to copy it or because they can't make it. They want it, primarily, because it is the purest reflection of our military capabilities.

That they are stealing computers and microchips from the USA is unquestionable, but it is not because they are inherently incapable of building equivalent technology. The evidence shows that such stealing is primarily devoted to military purposes. In that vein, they are primarily stealing our technology in order to find out, for example, how the F-16 embedded computer systems technology works, how to defend against the power this gives us, and how to incapacitate it in the quickest and most effective way. Their focus on military intelligence and exploitation does not, however, preclude their interest in U. S. technology for their commercial sector in either export operations or internal use.

Unfortunately, current American policy on technology transfer ignores that fact, resting instead on a totally outdated conception of what the Soviets are stealing and what they are stealing it for. With this improper focus, we are not only ineffective in stopping technology transfer, but we are also hurting our own technology in the process. Wholescale, generalized attempts to scuttle all technology transfer on unspecified and unfocused bases do not solve the real problem and are totally unresponsive to the needs of our own technology industry.

One example occurred when the U.S. government prevented a Soviet scientist from delivering a planned speech to a scheduled conference in California in 1979. The speech had been the result of concentrated planning and scheduling efforts by respected members of the American technology community. The Soviet was to deliver a paper on the science of "holography", an area believed to be the key to future military victory and an area in which the Soviets are undisputedly recognized as experts. As a result of unfocused and unrealistic efforts to curb technology transfer, the speech was cancelled. This was done despite protests by IBM as well as other respected members of the American scientific and high technology community. Such actions do not stem the flow of technology to the Soviets. They do seriously halt the flow of expert and needed Soviet technology to American industry.

There are other serious shortcomings in our current policy on technology transfer. The CoCOM control "sieve", once effective, is now begging of revision. Dramatic changes in technology require that we re-evaluate CoCOM's basis. Most of our legal controls on technology transfer center on the export laws and a belief that we can effectively police the transfer of listed materials at our borders. In view of the changes in restricted technologies, just in the last five years that policy is unrealistic and hopelessly outdated. The huge computers of fifteen years

ago are no longer the "jewels" of our technology industry. Today's most powerful computers (and in the foreseeable future) are composed of tiny microprocessor chips, the elements of which vanish into the microscopic world. We should be selling our big computers for as much profit as they will bring, rather than expending resources to restrict their export to the Soviets and elsewhere. Clearly a new computer can be very large in size, so old and new are not equivalent to big and small all the time; just most of the time. But new and big machines are ultimately decomposable into microprocessor chips, bringing me to the point of this part of my testimony.

Even the largest computer systems can be shipped piece by piece and reassembled at their point of destination.

The transfer of microprocessor chips defies detection by currently known means. These are so thin that they can pass through the eye of a needle. Only half a centimeter square, they are essentially undetectable by metal detection devices. No surveillance device is truly effective.

This makes detection at borders virtually impossible. Instituting controls at our borders are therefore impossible. We must institute some policy of controls on technology for previously mentioned reasons. Most impertant, that policy must be effectively communicated to and instituted at the source -- the companies that make these products and deal in them. Unfortunately, to date the government has done little in this respect. Current export control lists are (1) hopelessly outdated and (2) not visibly circulated within the industry sectors. I have seen lists of controlled products which are so outdated that they go back to the days of delivering B-29 parts.

The government should initiate serious efforts to give guidance on foreign involvement and the true strategy of foreign technology transfer to key officers in companies producing the targeted technology. Private briefings of the very top people in these industries by responsible and knowledgeable American officials would be the best beginning to an effective program. Sadly, many USA microprocessor manufacturers have some measure of foreign ownership, including control.

Today the People's Republic of China is currently in the "supermarket" situation which the Soviets were in fifteen years ago. I met with the first purchasing mission from the People's Republic of China in my New York offices. We spent nearly twelve hours together, discussing the scope of their knowledge and

interest in the technology area. All of, certainly most of, the members of the group were university graduates, mostly from schools like Harvard, Princeton, and Yale and well experienced in high technology. They indicated that they, too, had a deep knowledge of microprocessor chips, modern nuclear reactor technology, etc. In passing, I remarked that "you certainly know a lot about modern technology." The Chairman of the Chinese group responded, "We're not stupid. We're just broke."

Like the Chinese, the Soviets are not "stupid". And, unlike fifteen years ago, they are no longer "broke". They do not need to steal all our technology and they know it. By design, they have for the most part chosen to selectively target and secure those areas of American technology which are critical to the secrets of our military defense. They need to know such things as when and where our missiles and planes take off and how to jam the electronics in these. As long as the United States fails to recognize the bases and nature of their strategy and persists in outmoded, ineffective, and unfocused attempts to control the export and transf. of technology, the Soviets will, I am afraid, find their global task that much simpler.

Thank you.

PREPARED STATEMENT OF ADMIRAL BOBBY R. INMAN

Thank you Mr. Chairman for the opportunity to appear before this Committee this morning and to continue dialogue on this most important topic. I believe that we agree that technology transfers to the Soviets and the Eastern Bloc represent a very serious problem.

I would like to take this opportunity to again enter into the public record the kinds of problems we are dealing with, and the importance of the various Soviet Bloc mechanisms for acquiring Western technology.

— First, as we look at the militarily useful, militarily related technology which the Soviets have acquired from the West, about 70 percent of these acquisitions have been accomplished by the Soviet and East European intelligence services, using clandestine, technical, and overt collection operations. They are trying to get technologies of proven Western weapons or component designs that can be applied directly to Soviet weapons R&D and industrial needs.

— The Soviets and their Warsaw Pact allies are concentrating their efforts through purchases openly and legally and, if not successful, then illegally, including espionage. The sources of this technology may be government classified or unclassified reports, private companies "proprietary" reports, open-source technical documents from companies and government organizations. Embargoed equipment falls into this category as well. The Soviets undertake a very thorough vacuum cleaning of anything in the public sector which will let them better target their espionage activities.

-- Of the remaining 20-30 percent of the acquisitions of information of military value to the Soviets, it mainly comes through legal purchases and open-source publications or from other Soviet organizations, such as the Ministry of Trade and related international bodies; only a small percentage comes from the direct technical exchanges conducted by scientists and students.

I would like to enter into the record at this time an unclassified study from the Intelligence Community perspective of our knowledge of Soviet efforts to obtain Western technology and to use it ultimately to improve their own military capabilities.

As we look out into the 1980s, where do we believe the pressure is going to come?

-- Future Soviet and Warsaw pact acquisition efforts--including acquisitions by their intelligence services--are likely to concentrate on the sources of such component and manufacturing technologies, including:

- Defense contractors in the United States, Western Europe, and Japan who are the repositories of military development and manufacturing technologies.

- General producers of military-related auxiliary manufacturing equipment in the United States, Western Europe, and Japan.

- Small and medium-size firms and research centers that develop advanced component technology and designs, including advanced civil technologies with future military applications.

The task is likely to become even more difficult in the future as several trends identified in the 1970s continue into the 1980s:

- First, since the early 1970s, the Soviets and their surrogates among the East Europeans have been increasingly using their national intelligence services to acquire Western civilian technologies--for example, automobile, energy, chemicals, and even consumer electronics.

- Second, since the mid-1970s, Soviet and East European intelligence services have been emphasizing the collection of manufacturing-related technology, in addition to weapons technology.

- Third, since the late 1970s, there has been increased emphasis by these intelligence services on the acquisition of new Western technologies emerging from universities and research centers.

The combined effect of these trends is a heavy focus by Soviet Bloc intelligence on the commercial sectors in the West--sectors that are not normally protected from hostile intelligence services. In addition, the security provided by commercial firms is no match for the human penetration operations of such foreign intelligence services. But the most alarming aspect of this commercial focus by Soviet Bloc intelligence services is that as a result of these operations the Soviets have gained, and continue to gain, access to those advanced technologies that are likely to be used by the West in its own future weapons systems.

I can only conclude that Western security services will be ...rely tested by the Soviet intelligence services and their surrogates among the East European intelligence services during the 1980s. In response, the US and its Western allies will need to organize more effectively than it has in the past to protect its military, industrial, commercial and scientific communities.

I am pleased to say that coordination within the Intelligence Community and intelligence support to the Executive Branch departments and agencies regarding the issue of technology transfer is much better than a year ago when Bill Casey pointed out a number of deficiencies in this area to the Senate Select Committee on Intelligence. For example:

-- The DCI has established a Technology Transfer Intelligence Committee (TTIC) to serve as a focal point within the Intelligence Community on all technology transfer issues. The Committee is able to draw on the highly skilled S&T analysts who are located throughout the military technical intelligence centers and elsewhere in the Intelligence Community to address this complex problem. The Committee also ensures that intelligence information collected on technology transfer is consistent with the DCI's priorities and guidance and meets the needs of Community production organizations. A TTIC Subcommittee on Exchanges advises appropriate US Government departments and agencies of the technology transfer implications and foreign intelligence equities involved in exchange programs and commercial contacts with nationals from designated foreign countries and recommends changes as appropriate. A Subcommittee on Export Control has recently been established to provide foreign intelligence support on export control issues to appropriate US Government agencies.

-- The intelligence agencies are now better organized to support the functions of the export control enforcement agencies. Assistant Attorney General Lowell Jensen is heading an interagency committee at Justice on Export Control Enforcement. This group has the potential to become the most significant forum for coordinating enforcement and investigative efforts dealing with export control matters. As members of this Committee, we will ensure that it draws effectively upon appropriate intelligence data bases and support. The intelligence agencies will also become directly acquainted with the current state of the enforcement effort and the intelligence needs of the enforcement agencies but also will be in a position to acquire first hand and peruse significant information being developed by the enforcement agencies that will add to and enhance the effectiveness of the intelligence effort in the long run. Any intelligence issues that are developed in this forum may be brought back to the TTIC for appropriate consideration in an Intelligence Community setting.

-- The NSC Technology Transfer Coordinating Committee, chaired by Dr. Gus Weiss, serves as a valuable high-level forum for national policy assessment and developments. It is here that the political, foreign policy, intelligence and enforcement elements are woven together and decisions on jurisdictional issues or program choices may be sought. Substantial intelligence support to this group will result in better understanding of the threat, greater support for the efforts of the intelligence and enforcement agencies and result in more considered policy determinations.

-- The intelligence agencies are now in a position to make substantial contributions to Commerce's Advisory Committee on Export Policy, which makes determinations concerning whether particular exports should be licensed and what general policies should be applied by the US.

-- State's Economic Defense Advisory Committee (EDAC) Working Group II structure provides an important opportunity for intelligence, enforcement and foreign policy considerations to be discussed in the context of both general policy concerns and specific cases. Intelligence support here is essential for its value in identifying and assessing international enforcement problems and bridging the gap where there are both domestic and international aspects to a particular case.

PREPARED STATEMENT OF DR. STEPHEN D. BRYEN

I WELCOME THIS OPPORTUNITY TO SPEAK WITH YOU TODAY CONCERNING WHAT WE IN THE DEPARTMENT OF DEFENSE BELIEVE TO BE A MOST SERIOUS NATIONAL PROBLEM - THE CONTROL OF TECHNOLOGY WHICH IS BEING TRANSFERRED TO THE SOVIET UNION AND ITS ALLIES. MY DISCUSSION WILL FOCUS ON WHAT WE HAVE ACHIEVED SO FAR, WHAT IS IN THE WORKS, AND WHAT WE HAVE YET TO DO. IN THIS CONNECTION YOU SHOULD KNOW THAT ONE YEAR AGO WHEN I UNDERTOOK THIS MISSION, I HAD ONLY FOUR STAFF MEMBERS, A FULL PLATE OF RESPONSIBILITIES, NO PREVIOUS RECORDS OR ASSESSMENT, AND NO ORDERLY SYSTEM FOR DISCHARGING MY RESPONSIBILITIES. I CAN SAY NOW, WITH SOME PRIDE, THAT WE HAVE MADE CONSIDERABLE PROGRESS IN SOLVING SOME OF THE PROBLEMS; OTHERS REMAIN ON THE AGENDA.

PREVIOUS TESTIMONY HAS GONE TO CONSIDERABLE LENGTH TO ILLUSTRATE THE SCOPE OF OUR PROBLEM. IT WOULD BE VERY DIFFICULT TO ESTIMATE THE REAL DAMAGE DONE TO U.S. NATIONAL SECURITY BY THE BELL CASE, WHICH HAS BEEN BRIEFED TO YOU. THAT LOSS CONSISTS OF BOTH MILITARY DAMAGE IN MAKING THOSE WEAPON SYSTEMS VULNERABLE TO COUNTER-MEASURES AND IN COST TO THE TAXPAYER TO OVERCOME THE VULNERABILITIES THAT THOSE COMPROMISES ENTAIL. THESE ARE COMMON ASPECTS OF SUCH CASES AND CAN BE READILY UNDERSTOOD WHEN BLATANT ESPIONAGE IS INVOLVED AND U.S. MILITARY WEAPON SYSTEMS HAVE BEEN DIRECTLY COMPROMISED BY SOVIET EFFORTS. THE SAME KIND OF DAMAGE, HOWEVER, IS DONE IN MORE SUBTLE WAYS BY A VARIETY OF MECHANISMS THAT ARE CENTRALLY DIRECTED BY THE SOVIET UNION TO THE DETRIMENT OF THE UNITED STATES.

** A SO CALLED "GRADUATE STUDENT" STUDIES FUEL AIR EXPLOSIVES IN AN AMERICAN UNIVERSITY, RETURNS TO MOSCOW AND EMPLOYS THAT KNOWLEDGE IN THE DEVELOPMENT OF THOSE KINDS OF WEAPONS FOR THE SOVIET UNION.

** A TOUR OF A U.S. MANUFACTURING FACILITY ENGAGED IN BUILDING WIDE BODY AIRCRAFT IS COMPRISED OF VISITING SOVIET OFFICIALS WITH GUMMY SOLED SHOES WHO CAN BE PRESUMED TO HAVE ACQUIRED SUFFICIENT METALLURGICAL KNOWLEDGE THROUGH THE SOLES OF THEIR FEET TO ADVANCE THE STATE-OF-THE-ART OF SOVIET METALLURGY APPLICABLE TO THE SAME KIND OF AIRCRAFT FOR SOVIET MILITARY PURPOSES.

** IN A PERIOD OF DETENTE AND BRIDGE BUILDING WE LICENSE THE SALE OF PRECISION BALL BEARING GRINDERS WHICH PERMIT THE SOVIETS TO INCREASE THE ACCURACY OF THEIR STRATEGIC MISSILES. THE U.S. TAXPAYER ASSUMES THE COST OF UPGRADING U.S. ICBMS TO REDUCE OUR VULNERABILITY.

** OVER A PERIOD OF 3 OR 4 YEARS THE SOVIETS ACQUIRE THE BITS AND PIECES REQUIRED TO CONSTRUCT A COMPLETE MANUFACTURING FACILITY FOR INTEGRATED CIRCUITRY, THUS IMPROVING THE RELIABILITY, THE WEIGHT AND PERFORMANCE CHARACTERISTICS OF SOVIET MILITARY SYSTEMS FOR A WIDE VARIETY OF APPLICATIONS.

** FOR A FEW THOUSAND DOLLARS THE SOVIETS ACQUIRE VIRTUALLY ALL UNCLASSIFIED U.S. MILITARY STANDARDS APPLICABLE TO THE PRODUCTION OF U.S. MILITARY MATERIEL.

** THE LIBRARY OF CONGRESS SENDS THE OPERATING AND MAINTENANCE MANUALS FOR THE EMPLOYMENT OF U.S. FIELD ARTILLERY AND MISSILES TO THE SOVIET UNION IN HONORING A 19TH CENTURY TREATY FOR THE EXCHANGE OF GOVERNMENT PRODUCED PUBLICATIONS.

UNDOUBTEDLY YOU HAVE HEARD, OR WILL HEAR IN THE FUTURE, FROM THOSE WHO SAY THAT ONLY BY CONSTANT INVESTMENT IN THE TECHNOLOGY BASE UPON WHICH OUR DEFENSE IS FOUNDED, CAN THE U.S. HOPE TO REMAIN AHEAD OF ITS STATEGIC ADVERSARY. LIKEWISE YOU WILL HEAR THAT IT IS IMPOSSIBLE TO CONSTRAIN KNOWLEDGE AND TO DO SO IS, IN FACT, COUNTER TO THE EFFORT TO ADVANCE THE ONWARD PROGRESS OF TECHNOLOGY. UNDOUBTEDLY WE MUST PURSUE THE ADVANCEMENT OF OUR OWN TECHNOLOGY BASE. LIKEWISE, WE DO NOT SEEK TO CONSTRAIN THE FREE FLOW OF IDEAS. HOWEVER, WE BELIEVE THAT IT WOULD BE IMPRUDENT IN THE EXTREME TO SHRINK FROM THE DIFFICULT TASK OF DEVISING AND ENFORCING REASONABLE CONTROLS TO PRECLUDE THE USE BY THE SOVIETS OF THE FRUITS OF OUR TECHNOLOGICAL GENIUS TO DESTROY THE VERY SYSTEM BY WHICH IT IS NOURISHED. IT IS OUR ATTEMPT TO STRUCTURE, WITHIN THE DEPARTMENT OF DEFENSE, REASONABLE CONTROLS OVER TECHNOLOGY; CONTROLS WHICH WILL EFFECTIVELY INHIBIT THE FLOW OF TECHNOLOGY CONTRIBUTING TO THE GROWTH IN SOVIET MILITARY CAPABILITY.

IT IS A TRUISM THAT THERE IS NO SUBSTITUTE FOR CASE-BY-CASE REVIEW OF PROPOSED EXPORTS. ONLY BY CAREFUL AND OBJECTIVE ANALYSIS OF THE FACTS OF EACH CASE CAN THE OPERATIONAL, TECHNICAL AND PRECEDENTIAL IMPACT OF AN EXPORT BE PROPERLY ASSESSED. WE HAVE NO INTENTION WHATEVER OF ELIMINATING THIS VITAL ELEMENT OF DOD'S CONTRIBUTION TO THE GOVERNMENT'S EXPORT CONTROL EFFORT. HOWEVER, THE CASE-BY-CASE APPROACH FUNCTIONS BEST WITHIN A FRAMEWORK OF GUIDELINES AND CRITERIA; PROVEN STANDARDS BY WHICH INDIVIDUAL JUDGEMENTS CAN BE MADE. IN THE PAST, OUR INDIVIDUAL JUDGEMENTS WERE MADE IN SO FLEXIBLE A FASHION THAT WE WERE OVERLY SUBJECT TO THE VAGARIES OF THE MOMENT. INDEED, A SMALL INDUSTRY HAS ARISEN IN WASHINGTON COMPOSED OF INDIVIDUALS WHO KNOW HOW TO "PLAY THE SYSTEM" WITHIN THE EXPORT CONTROL COMMUNITY. THESE PEOPLE, THOUGH OFTEN WELL INTENTIONED, RECOGNIZE THAT TIMING AND APPROACH CAN MAKE THE DIFFERENCE BETWEEN APPROVAL AND DENIAL OF AN INDIVIDUAL CASE, PARTICULARLY THOSE CASES WHICH ARE RECOGNIZED AS BEING ON THE MARGINS OF ACCEPTABILITY. THE EFFECT HAS BEEN GENERALLY TO ADVANCE THE MARGINS OF ACCEPTABILITY OF EXPORTS THROUGH THE GRADUAL ACCRETION OF PRECEDENTIAL APPROVALS WITHOUT PARTICULAR REGARD FOR THE BASIC STANDARDS BY WHICH EXPORTS SHOULD BE JUDGED - - THE NATION'S SECURITY. ACCORDINGLY, WE ARE ENGAGED IN A MAJOR EFFORT TO DEVELOP, IN A COGENT AND COHERENT FASHION, A FRAMEWORK OF POLICY WITHIN WHICH THE DEPARTMENT OF DEFENSE CAN PROVIDE ITS ADVICE AND COUNSEL TO THE ULTIMATE LICENSING AUTHORITIES. SOME OF THIS EFFORT IS BEING UNDERTAKEN IN THE CRUCIBLE OF SPECIFIC, CURRENT CASE REVIEWS. OTHER EFFORTS ARE BASED UPON QUIET ANALYSIS OF THE LESSONS OF PAST EXPORT ACTIVITY. THE OBJECTIVE IS THE SAME IN BOTH ACTIVITIES; TO IMPLEMENT THIS ADMINISTRATION'S VIEW THAT OUR EXPORTS SHOULD NOT UNDERMINE OUR EFFORTS TO REPAIR THE EFFECTS OF A PERIOD OF NEGLECT FOR OUR NATIONAL DEFENSE WHICH HAS PLACED OUR ADVANTAGE OVER THE SOVIET UNION IN QUESTION.

STARTING WITH FOUR PEOPLE, WE IN THE OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR POLICY, HAVE EXPANDED OUR STAFF TO TWELVE AND HAVE INTENSIFIED OUR ROLE IN THE EXPORT REVIEW PROCESS WHILE UNDERTAKING THIS MAJOR EFFORT IN OBJECTIVE POLICY FORMULATION. I WOULD LIKE TO SHARE WITH YOU SOME OF THE THINGS WE HAVE DONE TO DATE, AND SOLICIT YOUR SUGGESTIONS FOR OUR FUTURE EFFORTS.

FIRST, AN AUGMENTATION TEAM COMPOSED OF REPRESENTATIVES OF THE SERVICES HAS BEEN ASSIGNED TO MY OFFICE AND IS PREPARING FOR THE SECRETARY OF DEFENSE'S SIGNATURE A POLICY STATEMENT ON CONTROL OF TECHNOLOGY TRANSFER. THIS WILL REPLACE A 1977 INTERIM POLICY SIGNED BY SECRETARY BROWN, DESIGNED TO SUPPORT U.S. EFFORTS TO CONTROL EXPORTS OF MILITARY CRITICAL TECHNOLOGY AND RELATED PRODUCTS. WHEREAS THE INTERIM POLICY FOCUSED ALMOST EXCLUSIVELY ON THE KNOW-HOW OF TECHNOLOGY, THE THRUST OF OUR NEW POLICY WILL REFLECT A BALANCED BUT FORCEFUL EMPHASIS ON TECHNOLOGICAL KNOW-HOW, KEYSTONE EQUIPMENT, AND END PRODUCTS. THE POLICY WILL REFLECT SEVERAL CHANGES THAT HAVE OCCURRED SINCE 1977. THE EXPORT ADMINISTRATION ACT OF 1979 IS IMPORTANT IN THIS RESPECT AS IS THE INCREASED AWARENESS AND CONCERN OF MANY AMERICANS TOWARD THE VAST AMOUNTS OF U.S. TECHNOLOGY REACHING OUR POTENTIAL ADVERSARIES.

THIS TEAM IS ALSO PROVIDING MANAGEMENT ASSISTANCE TO MY OFFICE IN THREE FORMS. THE FIRST OF THESE IS TECHNICAL ASSISTANCE TO AUTOMATE SOME OF THE ROUTINE ADMINISTRATIVE TASKS INVOLVED IN DETERMINING POLICY AND PROCESSING CASES. THE SECOND IS TO ASSIST THE INTEGRATION OF EXISTING DATA BASES USED IN ROUTINE CASE PROCESSING. THE THIRD IS THE CREATION OF A CENTRAL LIBRARY TO PROVIDE THE BASIC DOCUMENTS REQUIRED FOR DEVELOPING POLICY. EXISTING AUTOMATION SYSTEMS THROUGHOUT DOD, INCLUDING THOSE IN MY OFFICE, IN OUSDRE, AND THE NAVAL RESEARCH LABORATORY AS WELL AS THE NEWLY EMERGING FORDTIS SYSTEM, ARE BEING REVIEWED WITH THE END OBJECTIVE OF CREATING A COMPREHENSIVE, EFFECTIVE SYSTEM FOR USE BY THE DEFENSE POLICY MAKERS.

IN THE SAME VEIN, WE HOPE TO IMPROVE THE PROCESSING OF PROPOSED TRANSFER CASES BY RECOMMENDING IMPLEMENTATION POLICY AND PROCEDURES WHICH WILL MAKE OPTIMUM BENEFIT OF AVAILABLE (AND RECOMMENDED) MANPOWER AND AUTOMATION CAPABILITIES. THE POLICY INVENTORY LIBRARY WILL BE A REPOSITORY OF EXISTING AND PROPOSED LEGISLATION, DIRECTIVES AND REGULATIONS OF GOVERNMENTAL DEPARTMENTS AND AGENCIES INVOLVED IN MAKING AND IMPLEMENTING TRADE AND EXPORT CONTROL POLICY.

THIS COMMITTEE SHOULD KNOW, THAT ON TAKING OFFICE THERE WERE NO COHERENT RECORDS AVAILABLE ON PAST DOD DETERMINATIONS; NOR WAS THERE ANY SINGLE SOUURCE TO APPRAISE THE RESULTS OF PAST ACTIVITY.

THIS DEFICIENCY IS SLOWLY BEING CORRECTED, AND MY STAFF IS BEING TRAINED TO APPLY MORE RIGOROUS STANDARDS AND FOLLOW MORE DISCIPLINED PROCEDURES. IN THE LONG RUN, THESE EFFORTS WILL GO A LONG WAY IN ASSURING AN INSTITUTIONALIZED LEARNING CURVE IN HARMONY WITH OUR SECURITY INTERESTS.

IN ORDER TO FURTHER EDUCATE U.S. CITIZENS AT HOME AND FRIENDS ABROAD ABOUT THE RISKS TO THEIR SECURITY POSED BY INDISCRIMINATE TRANSFER OF TECHNOLOGY AND ABOUT THE MEANS OF TRANSFER, THE AUGMENTATION TEAM IS, UNDER MY DIRECTION, PREPARING A WHITE PAPER ON THE SUBJECT. THE GOALS OF THE PAPER ARE TO DEMONSTRATE THE IMPORTANCE OF DUAL-USE TECHNOLOGIES TO THE DEFENSE SUPPORT INDUSTRIES IN THE SOVIET UNION; TO PROMOTE MORE VOLUNTARY COMPLIANCE WITH EXISTING EXPORT PROCESSES; AND SECURE SUPPORT FOR AND ASSISTANCE IN DEVELOPING METHODS WHICH MORE CLOSELY REVIEW DEFENSE RELATED TECHNOLOGIES PROPOSED FOR EXPORT. THE PAPER WILL ALSO ATTEMPT TO PRESENT THE ROLES AND CONTRIBUTIONS OF THE DEPARTMENTS OF STATE, COMMERCE, TREASURY, JUSTICE AND THE BUREAU OF CUSTOMS. WE ANTICIPATE THAT OUR WHITE PAPER WILL BE AN IMPORTANT EDUCATIONAL TOOL AND REFERENCE SOURCE. WE HOPE, AS WELL, THAT IT WILL STIMULATE OUR ALLIES AND FRIENDS TO WORK WITH US IN THIS EFFORT. ACCORDINGLY, WE PLAN TO DISTRIBUTE THIS PAPER WIDELY AND HOPE IT WILL FORM PART OF THE DIALOGUE AND DEBATE ON TECHNOLOGY TRANSFER IN THE MONTHS AND YEARS AHEAD.

ANOTHER MAJOR EFFORT IS OUR ATTEMPT TO WORK CLOSELY WITH THE DEPARTMENTS OF STATE AND COMMERCE IN SEEKING TO STRENGTHEN STRATEGIC TRADE CONTROLS IN COCOM AND, THUS, TO STEM THE FLOW OF WESTERN TECHNOLOGY TO THE SOVIET UNION AND ITS ALLIES. AS YOU KNOW, COCOM IS AN INFORMAL NON-TREATY ORGANIZATION ESTABLISHED IN THE EARLY 1950'S COMPRISED OF THE NATO COUNTRIES LESS ICELAND PLUS JAPAN. IT HAS NO FORMAL LINK TO NATO, HOWEVER. THE COCOM SYSTEM WORKS ON THE BASIS OF CONSENSUS. THIS IS BOTH ITS STRENGTH AND ITS WEAKNESS. BECAUSE IT IS A VOLUNTARY ORGANIZATION AND REQUIRES UNANIMITY TO ACT, IT CAN CONTINUE TO OPERATE WITH REASONABLE EFFECTIVENESS ONLY THROUGH A SYSTEM OF COMPROMISE, EXCEPTIONS AND PRECEDENT. THE MEMBERS SEEK TO BALANCE THE STRATEGIC CONCERNS OVER COCOM RESTRICTED TECHNOLOGY TRANSFERS AGAINST THEIR COMMERCIAL AND POLITICAL INTERESTS.

95-929 O - 82 - 38

UNFORTUNATELY, THE NEED TO SEEK COMPROMISE HAS ALLOWED CONTROLS TO BE ERODED, ESPECIALLY IN RECENT YEARS. THIS EROSION TAKES THE FORM OF NUMEROUS EXCEPTIONS REQUESTS WHICH HAVE THE EFFECT OF VIRTUALLY ALLOWING THE EXPORT OF ALL BUT THE MOST ADVANCED TECHNOLOGIES. AS INDICATED, THE SOVIET UNION HAS SOUGHT TO ACQUIRE THESE THROUGH ILLEGAL CHANNELS WITH CONSIDERABLE SUCCESS.

FROM THE OUTSET, THIS ADMINISTRATION HAS SOUGHT TO STRENGTHEN THE STRATEGIC PURPOSE AND WILL OF COCOM. KEY TO THIS EFFORT HAS BEEN THE COCOM HIGH LEVEL MEETING CONVENED LAST JANUARY IN PARIS. THE PURPOSE OF THIS POLITICAL MEETING WAS THREEFOLD: TO REAFFIRM THE STRATEGIC PURPOSE OF THE COCOM EMBARGO; TO GAIN AGREEMENT TO STRENGTHEN CONTROLS OVER CERTAIN KEY MILITARY-RELATED TECHNOLOGIES SUCH AS ROBOTICS, COMPUTERIZED MESSAGE SWITCHING, METALLURGY AND MICROELECTRONICS; AND TO HARMONIZE COCOM PROCEDURES AND INCREASE COOPERATION AMONG MEMBERS IN ENFORCING CONTROLS. WE ALSO SOUGHT TO ESTABLISH A COMMITTEE OF MILITARY TECHNOLOGY EXPERTS TO ADVISE COCOM. EXCEPT FOR THE U.S. AND ONE OR TWO OTHER COUNTRIES, DEFENSE MINISTRIES ABROAD PLAY LITTLE OR NO ROLE IN THE REVIEW OF STRATEGIC TRADE EXPORTS.

IT WAS OUR RESPONSIBILITY TO PREPARE FOR COCOM AN ELABORATE BRIEFING, POINTING OUT THE GAPS AND LOOPHOLES IN THE PRESENT SYSTEM AND THE HARM THIS WAS BRINGING TO THE INDIVIDUAL AND COLLECTIVE DEFENSE EFFORTS OF THE COCOM MWMBERS. COUPLED WITH A GRAPHIC AND EFFECTIVE OVERVIEW OF SOVIET TECHNOLOGY ACQUSITION SUCCESSES, U.S. PROPOSALS PRESENTED AT COCOM BY UNDER SECRETARY OF STATE BUCKLEY, UNDER SECRETARY OF COMMERCE OLMER, AND UNDER SECRETARY OF DEFENSE IKLE. FOR THE RECORD, YOU SHOULD KNOW THAT THESE BRIEFINGS REQUIRED CONSIDERABLE EFFORT, AS WE HAD TO CONDUCT THE INVESTIGATIVE WORK AS WELL AS PREPARE THE ACTUAL PRESENTATIONS. THE LACK OF A CENTRAL DATA BASE AND HISTORICAL DOCUMENTATION (AS WELL AS EVALUATION) REQUIRED A FAR MORE EXTENSIVE UNDERTAKING ON OUR PART THAN OTHERWISE MIGHT HAVE BEEN NECESSARY.

I AM PLEASED TO REPORT THAT THE GENERAL STRENGTHENING PROGRAM SOUGHT BY THE U.S. WAS WELL RECEIVED BY OUR ALLIES AND WE ARE WORKING TOGETHER TO ESTABLISH A SOLID FRAMEWORK TO REVITALIZE COCOM AS AN EFFECTIVE MEDIUM FOR THE CONTROL AND ENFORCEMENT OF THE STRATEGIC TRADE EMBARGO.

SEPARATELY, MY OFFICE HAS SUPPORTED A MAJOR NEW NATO STUDY ON THE SECURITY IMPLICATIONS FOR THE ALLIANCE OF THE TRANSFER OF MILITARILY RELEVANT TECHNOLOGY TO THE WARSAW PACT COUNTRIES. THIS UNDERTAKING WAS THE RESULT OF SECRETARY OF DEFENSE WEINBERGER'S INITIATIVE AND IS THE FIRST NATO REVIEW OF THE TECHNOLOGY TRANSFER ISSUE. THE STUDY GROUP ASSESSED THE SOVIET ORGANIZATION AND MECHANISMS FOR ACQUIRING TECHNOLOGY, AND IDENTIFIED A REPRESENTATIVE LISTING OF TECHNOLOGIES THAT ARE ESSENTIAL TO NATO MILITARY MISSIONS. ALTHOUGH THE FINDINGS OF THIS SEVEN MONTH EFFORT WILL NOT BE APPROVED UNTIL LATER THIS MONTH, SOME OF THE BENEFITS WHICH HAVE EMERGED FROM THE EFFORT INCLUDE A BETTER UNDERSTANDING OF THE MAGNITUDE OF THE SOVIET EFFORT TO ACQUIRE WESTERN TECHNOLOGY, THE APLICABILITY OF "CIVILIAN" TECHNOLOGIES TO MILITARY WEAPONS, AND A GREATER APPRECIATION OF THE RISK TO NATO RESULTING FROM TECHNOLOGY TRANSFER TO THE SOVIETS. WE ARE ENCOURAGING NATO TO CONTINUE THE DIALOGUE BEGUN BY THIS INITIATIVE THROUGH ESTABLISHING AN OFFICE AT NATO HEADQUARTERS TO ALERT THE ALLIANCE TO SOVIET EFFORTS TO ACQUIRE ADVANCED TECHNOLOGY. I WANT TO EMPHASIZE OUR BELIEF THAT THE TRANSFER OF TECHNOLOGY IS FAR MORE THAN A PAROCHIAL U.S. CONCERN. IT IS A POTENT ALLIANCE ISSUE WITH WIDE RANGING IMPLICATIONS.

THE INCREASING IMPORTANCE OF ADVANCED DUAL-USE TECHNOLOGIES TO MILITARY APPLICATIONS HAS RAISED DEFENSE DEPARTMENT CONCERNS ABOUT THE LOSS OF TECHNOLOGY THROUGH ACADEMIC ACTIVITIES TRADITIONALLY CONSIDERED OUTSIDE THE AREA OF GOVERNMENT CONCERN. THIS NEW CONSCIOUSNESS OF THE MILITARY IMPORTANCE OF DUAL-USE TECHNOLOGY HAS RAISED SUSPICIONS IN THE ACADEMIC COMMUNITY ABOUT THE INTENTIONS AND MOTIVES OF THE GOVERNMENT, WHILE THE GOVERNMENT HAS BEEN DISMAYED BY THE LACK OF COOPERATION OR SYMPATHY FROM THE COLLEGES AND UNIVERSITIES OVER THE PROBLEMS OF TECHNOLOGY TRANSFER.

WE ARE CONCERNED WITH ESTABLISHING A DIALOGUE BETWEEN THE GOVERNMENT AND THE UNIVERSITIES, AS WELL AS PRIVATE RESEARCH LABS. WE HAVE TAKEN STEPS TO INCREASE COMMUNICATION WITH UNIVERSITIES, TO PRESENT OUR POINT OF VIEW, AND TO LISTEN TO THEIR RESERVATIONS AND FEARS. THE NATIONAL ACADEMY OF SCIENCES HAS FORMED A PANEL

ON SCIENTIFIC COMMUNICATION AND NATIONAL SECURITY TO STUDY THE PROBLEM OF TECHNOLOGY TRANSFER IN UNIVERSITY-RELATED AREAS AND TO ASSESS WHAT CAN OR SHOULD BE DONE ABOUT IT. WE HAVE COOPERATED WITH THIS GROUP IN PRESENTING OUR VIEWS FOR CONSIDERATION IN THEIR DELIBERATIONS.

THERE IS ALSO A UNIVERSITY FORUM ON EXPORT CONTROL IN WHICH DEFENSE DEPARTMENT PERSONNEL PARTICIPATE IN DISCUSSION OF THESE ISSUES. OUR OFFICE IS INTIMATELY INVOLVED IN A WORKING GROUP OF THIS FORUM, AND WE ARE ATTEMPTING TO PROVIDE THE INFORMATION AND ORIENTATION THAT IS NECESSARY FOR THE MEMBERS TO UNDERSTAND THE DEFENSE PERSPECTIVE AND BE ABLE TO ASSESS THE PROBLEM OF TECHNOLOGY TRANSFER TO THE SOVIETS.

IT IS ESSENTIAL THAT THIS KIND OF COMMUNICATION BE FOSTERED TO KEEP LINES OPEN BETWEEN THE DEFENSE DEPARTMENT AND THE UNIVERSITIES. WE CANNOT DO OUR JOB WITHOUT UNIVERSITY COOPERATION IN R&D, AND WE NEED THEIR SUPPORT FOR OUR EFFORTS TO IMPROVE OUR DEFENSE READINESS. WE BELIEVE IMPROVED COMMUNICAT AND UNDERSTANDING IS CRUCIAL. WE HOPE WE WILL AGREE ON VIABLE WAYS TO DECREASE SOVIET ACCESS TO OUR TECHNOLOGY WITHOUT INHIBITING SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENT.

MY OFFICE HAS ALSO BEEN WORKING CLOSELY WITH ENFORCEMENT AGENCIES TO PREVENT ILLEGAL DIVERSIONS OF SOPHISTICATED TECHNOLOGIES TO THE SOVIETS. AS A RESULT OF THE JANUARY HIGH LEVEL MEETING, SPECIFIC MEASURES DESIGNED TO CLAMP DOWN ON ILLEGAL EXPORTING AND DIVERSIONS WILL BE NEGOTIATED AND DEVELOPED SHORTLY IN COCOM. FOR ITS PART, THE DEPARTMENT OF DEFENSE IS IN THE PROCESS OF DRAWING UP A "MUSHROOM BOOK" - A DESCRIPTIVE LIST DESIGNED TO AID CUSTOMS OFFICIALS IN IDENTIFYING THE MOST CRITICAL TYPES OF SOPHISTICATED, TECHNOLOGICAL EQUIPMENT. USING THIS BOOK AS A TOOL, U.S. CUSTOMS AGENTS WILL BE ABLE TO CONCENTRATE ON IDENTIFYING WHETHER SOPHISTICATED EQUIPMENT IS BEING EXPORTED LEGALLY OR NOT. WE HOPE TO GET OTHER COCOM MEMBERS TO USE THIS BOOK ALSO.

THE DEPARTMENT OF DEFENSE HAS BEEN SERIOUSLY CONCERNED ABOUT THE IMPLEMENTATION OF U.S. DISTRIBUTION LICENSES. DISTRIBUTION LICENSES ALLOW THE BULK SHIPMENT OF ITEMS INCLUDING COMPUTERS, TO

A HOST OF COUNTRIES OUTSIDE THE SOVIET BLOC. HOWEVER, A NUMBER OF THESE COUNTRIES ARE WILLING TO ALLOW, IF NOT COOPERATE WITH, SOVIET ACQUISITION OF COCOM EMBARGOED EQUIPMENTS. THE CURRENT SYSTEM LEAVES A LARGE LOOPHOLE OPEN FOR DIVERSIONS TO THE USSR OF SOPHISTICATED EQUIPMENT. WE ARE URGING THAT THIS LOOPHOLE IN THE SYSTEM BE CLOSED AS COMPLETELY AS POSSIBLE. THERE ARE SOME WHO QUESTION WHETHER THE EXPORT ADMINISTRATION ACT IS SUFFICIANTLY CLEAR TO CARRY THIS OUT. IF IT PROVES INADEQUATE, WE WILL ASK THAT THE STATUTE BE AMENDED TO ENABLE US TO CLOSE DOWN THIS GAP IN OUR COVERAGE.

WE HAVE BEEN CLOSELY INVOLVED IN THE ADMINISTRATION'S REVIEW OF THE DRAFT LAW OF THE SEA CONVENTION. OUR FOCUS IS ON ITS POTENTIAL IMPACT ON THE TRANSFER OF TECHNOLOGY TO THE SOVIET UNION AND ITS CLIENT STATES. IN THAT CONTEXT, A CRITICAL EXAMINATION OF THE DRAFT TREATY TEXT WAS UNDERTAKEN TO REASSESS THE POTENTIAL FOR THE TRANSFER OF MILITARILY SENSITIVE TECHNOLOGY. A MAJOR OBJECTIVE IS TO ASSURE THAT THE CONVENTION WILL NOT FORM THE BASIS FOR ANY WEAKENING OR UNDERMINING OF OUR DRIVE TO STRENGTHEN THE COCOM SYSTEM. I WOULD LIKE TO EMPHASIZE THAT, IN ITS PRESENT FORM, THE CONVENTION CONTINUES TO HAVE SERIOUS IMPLICATIONS FOR THE TRANSFER OF U.S. TECHNOLOGY. FOR THAT REASON, IT MUST BE CAREFULLY WEIGHED AGAINST OTHER NATIONAL SECURITY CONSIDERATIONS.

ONE CURRENT EFFORT OF PARTICULAR INTEREST TYPIFIES BOTH THE PROBLEMS OF DEVELOPING ADEQUATE CONTROLS AND THE RISKS OF NOT DOING SO. THAT EFFORT CONCERNS THE VHSIC PROGRAM. VHSIC, WHICH STANDS FOR VERY HIGH SPEED INTEGRATED CIRCUITS IS DESIGNED TO FILL THE GAP BETWEEN OUR HIGH PERFORMANCE MILITARY NEEDS AND CURRENT TECHNOLOGY IN MICROPROCESSORS. THE RESULTING PRODUCT WILL PERFORM ADVANCED SIGNAL PROCESSING FUNCTIONS FOR WEAPONS SYSTEMS INCLUDING ELECTRONIC WAREFARE, COMMUNICATION, RADAR, AND PRECISION GUIDED MUNITIONS AND DO SO WITH LESS COST, VOLUME, POWER, AND WEIGHT THAN CURRENT DIGITAL TECHNOLOGY. THE PROTECTION OF THIS TECHNOLOGY, SO IMPORTANT FOR OUR FUTURE DEFENSE NEEDS AND WEAPONS SYSTEMS, IS OF THE HIGHEST PRIORITY. CONGRESS SPECIFICALLY MANDATED THE CONTROL OF THIS TECHNOLOGY WHEN IT FUNDED THE VHSIC PROGRAM. TO DATE, THE WHOLE SYSTEM OF INTENDED CONTROLS HAS NOT BEEN IMPLEMENTED. WE ARE NOW DOING OUR BEST TO REMEDY THIS SITUATION AND TO PROTECT THIS TECHNOLOGY FROM OUR ADVERSARIES AND THUS PRESERVE OUR QUALITATIVE LEAD IN CRITICAL DIGITAL TECHNOLOGIES.

A MOST PRESSING TASK AT THIS JUNCTURE IS TO PUT THE VHSIC PROGRAM UNDER THE PROTECTION OF THE INTERNATIONAL TRAFFICE IN ARMS REGULATIONS (ITAR), AS THE CONGRESS INTENDED. WE ARE WORKING WITH THE STATE DEPARTMENT TO ACCOMPLISH THIS. OUR IMMEDIATE TASK IS TO PROTECT THE TECHNICAL DATA AND MILITARY HARDWARE THAT IS NOW BEING DEVELOPED BEFORE IT IS TOO LATE TO PREVENT THE DISSEMINATION OF THESE TECHNOLOGIES TO OUR ADVERSARIES. TO DO THIS, WE MUST PUT THE VHSIC DEVICES THAT HAVE ALREADY BEEN DESIGNED AND THE SUPPORTING TECHNICAL DATA ON THE MUNITIONS LIST, TO ENSURE PROTECTION UNDER THE ITAR. SOME LEGAL PROBLEMS ARE INVOLVED IN DEFINING JUST WHAT CAN BE COVERED UNDER THE ITAR, BUT WE ARE CONFIDENT THAT THESE CAN BE SOLVED.

IN THE INTERIM, WE ARE TAKING STEPS TO SAFEGUARD THIS TECHNOLOGY THROUGH THE USE OF THE EXPORT ADMINISTRATION REGULATIONS (EAR). THIS WILL REQUIRE UNDERTAKING SOME IMPORTANT REVISIONS OF THE EAR TECHNICAL DATA CONTROLS AND COMMODITY CONTROL LIST.

FOR SOME ELEMENTS OF THIS PROGRAM, WE BELIEVE THERE IS NO EFFECTIVE CONTROL SHORT OF CLASSIFICATION. WE HAVE FOUND THAT, UNDER EXISTING CONTROLS, MUCH OF THE LITERATURE, SOFTWARE, AND HARDWARE CANNOT OTHERWISE BE FULLY PROTECTED. NEITHER THE ITAR NOR THE EAR ARE EXEMPT FROM ACCESS TO THIS SENSITIVE TECHNICAL DATA THROUGH THE FREEDOM OF INFORMATION ACT. MEMBERS OF THE PUBLIC CAN EASILY OBTAIN INFORMATION BY MERELY INVESTING A 20 CENT STAMP AND THE TIME NECESSARY TO WRITE A SHORT LETTER. ONCE THIS INFORMATION IS OBTAINED, IT CAN EASILY BE PASSED TO THE SOVIETS, OR PUT IN THE PUBLIC DOMAIN WHERE IT CANNOT BE PROTECTED. IT IS PARTICULARLY IMPORTANT THAT WE PROTECT THOSE INDICES AND LISTS WHICH GIVE AN OVERVIEW OF THE PROGRAM, AND ALLOW OUR ADVERSARIES TO PINPOINT THOSE PARTS OF THE PROGRAM THAT ARE PARTICULARLY USEFUL TO THEM. IF OUR ADVERSARIES OBTAIN ANY OF THIS ADVANCED TECHNOLOGY, WE WANT TO MAKE SURE THEY DO SO ONLY AFTER EXERTING THE MAXIMUM OF TIME AND EFFORT. WE ARE SENSITIVE TO THE NEED FOR CONTRACTORS AND OTHERS WORKING ON THE PROGRAM TO HAVE ACCESS TO THE DATA AND INFORMATION THAT THEY NEED, BUT WE BELIEVE THAT THROUGH SELECTIVE CLASSIFICATION WE CAN CONTROL ELEMENTS OF THE PROGRAM DIRECTLY ASSOCIATED WITH OUR FUTURE MILITARY SYSTEMS.

TO PROTECT AND MONITOR THE VHSIC PROGRAM, WE HAVE FORMED A VHSIC WORKING GROUP ON EXPORT CONTROL WHICH I CHAIR. THE WORKING GROUP IS NOW WORKING TO SELECTIVELY APPLY THE NEEDED CONTROLS. WE INTEND TO USE THE MINIMUM CONTROLS COMPATIBLE WITH PROTECTION OF THIS TECHNOLOGY. THE GROUP HAS ALREADY PROPOSED CLASSIFICATION OF ELEMENTS OF THE VHSIC PROGRAM AND HAS DEVELOPED DOCUMENTATION ALLOWING PORTIONS OF THE VHSIC PROGRAM TO BE CONTROLLED UNDER THE ITAR. WE STILL HAVE A GREAT DEAL TO DO BEFORE WE ARE SATISFIED THE PROGRAM IS APPROPRIATELY COVERED. BUT, WE BELIEVE, THE EXPERIENCE OF THE WORKING GROUP, AND THE TECHNIQUES BEING USED, WILL BE OF IMPORTANCE WELL BEYOND THE VHSIC PROGRAM. WE INTEND FULLY TO USE THE SAME MODEL TO PROTECT OTHER EMERGING TECHNOLOGIES SUPPORTED BY THE DEPARTMENT OF DEFENSE.

I WOULD LIKE TO TURN NOW TO AN IMPORTANT SOURCE OF THE SOVIETS' ABILITY TO ACQUIRE SOPHISTICATED WESTERN TECHNOLOGY. ENERGY EXPORTS TO THE WEST, PRIMARILY NATO EUROPE, CURRENTLY PROVIDE ABOUT HALF THE HARD CURRENCY EARNINGS FOR THE SOVIET UNION. WHILE MOST SECTORS OF THE SOVIET ECONOMY ARE STAGNANT, ENERGY REMAINS A BRIGHT SPOT. ONE PARTICULARLY PROMISING AREA IS NATURAL GAS AND THE SOVIETS ARE PLANNING TO DOUBLE THEIR SALES TO WESTERN EUROPE BY BUILDING A MASSIVE PIPELINE FROM WEST SIBERIA TO WESTERN EUROPE. WHEN THIS PROJECT IS COMPLETED IT WILL GENERATE SOME $8 BILLION PER YEAR IN NEW REVENUES. ABOUT 25 PER CENT OF WESTERN EUROPE'S IMPORTED GAS WILL THEN COME FROM THE USSR AND IN THE CASE OF SOME COUNTRIES, SUCH AS WEST GERMANY, THE FIGURE WILL BE EVEN HIGHER.

WE ARE NATURALLY CONCERNED ABOUT THE POTENTIAL FOR POLITICAL, ECONOMIC, AND EVEN MILITARY MANIPULATION WHICH SUCH LEVELS OF ENERGY DEPENDENCE IMPLY. WE ARE ALSO PERPLEXED AS TO WHY SO MANY OF OUR NATO ALLIES ARE EAGER TO TIE THEMSELVES TO A HIGH PRESSURE 56-INCH UMBILICAL CORD TO THE SOVIET UNION WHEN ADEQUATE, ECONOMIC, AND RELIABLE ALTERNATIVES EXIST IN THE WEST. THE NORTH SEA ALONE, FOR EXAMPLE, COULD SUBSTITUTE FOR MOST OF THE ENERGY FROM THE WEST SIBERIAN PROJECT AND AT THE SAME TIME PROVIDE JOBS AND ECONOMIC STIMULUS TO THE WEST. FURTHERMORE, ALL THE HARD CURRENCY GENERATED BY GAS SALES WOULD REMAIN IN THE INDUSTRIALIZED DEMOCRACIES AND NOT FLOW TO THE EAST. OTHER WESTERN OPTIONS, ARCTIC GAS, AMERICAN COAL, AND GAS AND OIL FROM LATIN AMERICA, AFRICA AND ELSEWHERE, ALSO EXIST.

THE SIGNIFICANCE OF THE WEST SIBERIAN PROJECT FOR TECHNOLOGICAL ACQUISITION FROM THE WEST IS ENORMOUS. WITHOUT THE REVENUES FROM THE NEW GAS SALES THE SOVIETS' FINANCIAL SITUATION WOULD DETERIORATE GREATLY. AT A TIME WHEN ENERGY PRICES ARE DEPRESSED AND RAW MATERIAL EXPORT EARNINGS ARE DOWN, WHEN SOVIET CROPS ARE FAILING AND WHEN EASTERN EUROPE IS ON THE VERGE OF BANKRUPTCY, NEW GAS SALE EARNINGS ARE CRITICAL TO THE SOVIET HARD CURRENCY POSITION. REVENUES FROM THE WEST SIBERIAN PROJECT ALONE, FOR EXAMPLE, WILL FINANCE MORE THAN ALL THE MACHINERY AND EQUIPMENT IMPORTS THE USSR PURCHASES FROM THE WEST EACH YEAR. WHILE WE WOULD EXPECT THE SOVIETS TO DEFER SOME OTHER PURCHASES IF THEY DID NOT HAVE THESE PIPELINE REVENUES, IT IS CLEAR THAT DEFENSE-RELEVANT IMPORTS, PARTICULARLY ITEMS OF SOPHISTICATED TECHNOLOGY AVAILABLE ONLY FOR HARD CURRENCY, WOULD BE ADVERSELY AFFECTED BY THE LOSS OF NEW NATURAL GAS SALES TO WESTERN EUROPE.

ANOTHER MAJOR PROBLEM WITH THE PIPELINE IS THE LEVERAGE THAT PARTICIPATION IN THE PROJECT GIVES TO THE SOVIETS IN TECHNOLOGY ACQUISITION. WITH A $10-15 BILLION INVESTMENT IN THE PROJECT, IT WILL BE HARDER FOR THE WESTERN EUROPEANS TO REFUSE SOVIET REQUESTS FOR TECHNOLOGY, WHERE THE DOLLAR AMOUNTS ARE SMALL BY COMPARISON. IT IS DIFFICULT TO REFUSE A REQUEST FOR A $1 MILLION COMPUTER WHEN YOUR CLIENT HAS JUST PLACED AN ORDER FOR $1 BILLION IN PIPE! FURTHER DOWN THE ROAD, WHEN BILLIONS OF DOLLARS IN NATURAL GAS ARE WARMING WEST EUROPEAN HOMES, GENERATING ELECTRICITY, AND RUNNING FACTORIES, IT WILL ALSO BE DIFFICULT TO TURN DOWN REQUESTS FOR SENSITIVE TECHNOLOGIES AND EQUIPMENT. SINCE THIS PROJECT IS SLATED TO LAST TWENTY YEARS OR MORE, WE SEE IT HAVING AN IMPACT ON FUTURE PROPOSALS TO TIGHTEN TECHNOLOGY CONTROLS OR EVEN MAINTAIN THEM FAR INTO THE FUTURE.

I HAVE COVERED QUITE A VARIETY OF OUR EFFORTS TO DATE. CLEARLY, WE DO NOT HAVE ALL THE ANSWERS. WE NEED ASSISTANCE FROM THE CONGRESS IN TERMS OF RESOURCES ADEQUATE TO THE TASK AND THE LEGISLATIVE BASIS FOR OUR EFFORTS. AS YOU WEIGH OUR REQUESTS FOR SUCH ASSISTANCE, YOU MAY WISH TO CONSIDER THE IMPLICATIONS OF THESE EFFORTS FOR U.S. NATIONAL STRATEGY. ONE APPROACH MAY BE TO ASK WHAT THE

ALTERNATIVES MIGHT BE. IF WE ARE FACED WITH A SITUATION IN WHICH THE SOVIETS ACHIEVE QUALITATIVE PARITY WITH US IN TERMS OF THE CAPABILITIES OF OUR WEAPONS SYSTEMS, THEN WHAT NATIONAL STRATEGY OPTIONS REMAIN TO US? WHAT STRATEGY COULD WE SUSTAIN? WOULD WE BE FACED WITH A CHOICE BETWEEN MATCHING THE SOVIETS MAN FOR MAN AND TANK FOR TANK, OR ABANDONING OUR ALLIES AND DEFENDING AMERICA AT THE EASTERN SHORE? WE BELIEVE THAT MAJOR IMPROVEMENTS IN TECHNOLOGY TRANSFER CONTROLS WOULD BE FAR MORE ECONOMICALLY EFFECTIVE AND POLITICALLY ACCEPTABLE THAN THE ALTERNATIVE MILITARY SOLUTIONS.

STATEMENT OF LAWRENCE J. BRADY
ASSISTANT SECRETARY OF COMMERCE
FOR TRADE ADMINISTRATION
BEFORE THE SENATE
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
May 12, 1982

I am very pleased to have the opportunity to testify before this subcommittee on an issue which is of vital concern to the Reagan Administration: technology transfer from the West to the Soviet Union. Only now, as a nation, are we beginning to understand the extent of these technology transfers during the past decade, and the contributions such transfers have made to strengthening the Soviet military-industrial base.

Stopping the extensive acquisition by the Soviets of sensitive, dual-use Western technology in ways that are both effective and appropriate in our open society is one of the most complex and urgent issues facing America and the rest of the Free World today. Moreover, only now are we beginning to recognize that the technology transfer issue is much more than just an enforcement problem.

Apart from strengthening enforcement, in order to deal successfully with the increasing Soviet effort to acquire advanced Western technology, we need to:

- Understand what technology the Soviets need, how such acquisition has helped the Soviet Union achieve its goal of military superiority, and what methods the USSR is using to obtain it;
- On a multilateral basis, marshall the support and commitment of our allies to prevent further technology leakage to the Soviet Union by Western industrial concerns and by U.S. subsidiaries and licensees operating abroad;

- Build up our counterintelligence efforts to counteract the Soviet intelligence organization;

- Work closely with industry segments involved in the development production of high technology to assess ways of retarding the growing industrial security problem; and

- Examine all possible avenues for identifying and protecting defense sensitive technologies, including technical documents, which are not now subject to our classification system.

Mr. Chairman, we are now approaching the problem on all these and other fronts. I want to emphasize that today we are in a far different strategic, political, and technological environment than the one that shaped our export control system 30 years ago.

Strategically, we need to recognize that the USSR is far more powerful militarily than the nation we faced at the end of World War II, and is far more capable of procuring and applying our latest technological advances. We could not, however, take adequate protective action until we had accurately assessed the nature of that threat. Therefore, one of the first actions taken by the Administration was to request the intelligence agencies to prepare a comprehensive analysis of Soviet technology acquisition methods.

Not until the Fall of 1981, when we started to receive these analyses, did we begin to appreciate the magnitude of Soviet activities against the West. In April of this year, the C.I.A. released the unclassified version of its report, "Soviet Acquisition of Western Technology," which verified the fact that the USSR's efforts were massive and planned at the highest levels of government, KGB and the military.

It now appears that the USSR is placing greater emphasis on the procurement of production equipment technology, as opposed to actual weapons designs in some cases. The commercial sector, which generally is not adequately protected against penetration by hostile intelligence services, is being targeted.

Industrial espionage has become one of the most productive areas for Soviet and East European intelligence services. We anticipate greatly enhanced activity in automobile technology, energy, chemicals, consumer electronics, and computers.

Politically, we face a much more formidable task in working with our allies to stem the flow of security sensitive technology to the USSR. For them, trade in high technology products means relief from the growing pressures of high unemployment. The past ten years of Detente and expanded trade with the USSR has also created interdependence and vulnerabilities in the West to subtle and not-so-subtle Soviet blandishments to ignore national security in favor of commercial considerations. Also, the pressure to export and to retain access to the Soviet market is, for certain industries within these countries, enormous.

Revolutionary advances in technology and in the structure of business enterprises have also created enormous new obstacles for our efforts to regulate strategic trade with the Warsaw Pact. The rate at which new technologies are conceived and applied to industrial process continues to accelerate. We are in the midst of perhaps the most rapid period of technological advance in human history.

The private sector has now risen to prominence in technology leadership, with the governments following behind. Leading-edge technology -- once primarily generated by the military -- is now frequently developed first in the civilian

sector. It has thus become more difficult for national governments to control the dissemination of technology to foreign recipients. Identification and protection of new and emerging technology remains one of our toughest challenges.

At the same time, the rise of multinational corporations, combined with the speed of modern communications and transportation, has intensified the proliferation of advanced technology. Overseas corporate acquisitions, joint ventures, manufacturing associations, cross licensing, multinational data communications transfers all make the task of national enforcment more difficult.

We also discovered that Third country diversions constitute the largest source of illegal transfers to controlled destinations, far exceeding the number of illegal shipments from the United States. It therefore became obvious that the magnitude and international scope of technology leakage far exceeds our previous assessments.

Mr. Chairman, this Administration, even prior to taking office, was acutely aware of the technology transfer problem. In the months since assuming office, we have moved systematically to ascertain the threat posed by this leakage, to ascertain how the Soviets and East Europeans are working to acquire Western technology, and finally taken remedial actions to deal with this matter. Since the major bulk of the technology transfer problem is international, we addressed that aspect first.

At the Ottawa Summit in July 1981, President Reagan made a personal appeal to the leaders of Europe, Canada, and Japan to join with us in this endeavor. As a result, agreement was reached to hold a high level meeting of the Coordinating Committee (COCOM) -- the first in twenty-five years -- to discuss the U.S. proposals.

This meeting, in which Commerce played a key role, took place in January of this year. Important progress was achieved. There is now a political commitment from our COCOM partners which will serve as the foundation for refocusing and strengthening international control efforts toward critical technologies and equipment.

Such a commitment is vital to the mutual security of the West. COCOM controls have played a major role in stemming the tide of technology transfer to the East, and have proved most successful in the computer area. As a consequence of these controls, the Soviets lack the most advanced Western computers, even though such computers have been commercially available in the West for more than a decade.

Since the high level meeting we have devoted many months to striving for tighter controls on legal sales and increased enforcement efforts within COCOM member countries. We have stressed, and our fellow COCOM members agree, that without immediate remedial action, the growing leakage of technology from the West to the USSR would reach proportions too great to rectify.

This Administration has repeatedly pointed out that our short-sighted export licensing policies during the detente of the late sixties and early seventies has encouraged the most extensive raid on Western technology by the Soviet Bloc since World War II. In the process, they have gained expertise in electronics, computer sciences, manufacturing techniques, aviation, and a host of other disciplines that has been of incalculable value to their military establishment and, thus, of immeasurable harm to our own interests on this planet.

There is no conceivable way in which our short-term financial gains could ever balance the damage done to our national security as a result of past export control policies.

Thus, Mr. Chairman, these hearings come at a propitious time. The security of the Free World demands responsible, united action by Free World governments to deprive our adversaries of those industrial and technical tools they covet. It is in this spirit that I welcome the hearings and the review conducted by your staff of Commerce's compliance organization.

I have reviewed the Minority Staff report. Based on both my experience as Assistant Secretary and my earlier tenure as Acting Director of the Office of Export Administration, I agree that the report has identified some of the fundamental problems in the Commerce enforcement mechanism. The Staff Report is a useful historical document in that respect. Unfortunately, it only addresses a small part of the technology transfer problem. Moreover, it does not recognize that the policies of this Administration represent a sharp change from the practices of the past; that we view the pressing need for more effective control as a top priority.

The report also does not address the organizational realignment and enhancement of the Compliance Division we now have underway

I must also disagree with the report's assertion that Commerce has trade promotion as its major objective to the detriment of enforcing the Export Administration Act. From the President on down, the clear policy is that trade must be carefully weighed against national security considerations. I would not object if you said past administrations emphasized trade promotion over all other concerns. I, too, was a severe critic of such past practices. But we are in the present; circumstances have changed.

Within the organization that I oversee, Trade Administration, our management focus has been on effective and efficient execution of our regulatory mission.

On the Import Administration side, we are charged with enforcement of the laws governing unfair trade practices. Our mission was spelled out unambiguously by the Congress in its deliberations leading to passage of the 1979 Trade Agreements Act. In transferring this function to the Department of Commerce from Customs, Congress instructed us to protect American industry from injurious and unfair foreign trade practices by administering the countervailing duty and antidumping laws of the Unites States; and, before its suspension the provisions of the Steel Trigger Price Mechanism. This we are doing.

The challenges were similarly pressing in Export Administration. Various factors had combined over the past several years to cause unacceptable delays in the processing of export license applications. These factors ranged from a lack of clear policy guidance to a simple manpower shortage. However, Congress and the private sector had become increasingly critical with respect to the delays and bottlenecks encountered in the licensing process.

In the early days of this Administration, both Secretary Baldrige and Under Secretary Olmer told me to solve the serious backlog problem we had inherited so that, by the end of fiscal year 1981, the number of application not processed within the statutory deadlines would be reduced to as near zero as possible.

To this end we dedicated ourselves, mustering the necessary resources, enlisting the temporary aid of the Department of Defense's export licensing analysts, and streamlining the

administrative inhibitions to getting the job done. The result by last October was elimination of the backlog of over 2,000 cases and maintenance in the six months since then of only a modest number of extraordinary cases in process beyond the statutory timetables.

Our thesis was, and remains, that export controls can be both effective and efficient; export controls should reflect clear Administration policies and be applied with reasoned judgment by technically qualified people using that policy guidance. These are instances of the Reagan Administration's proven ability to reverse some serious regulatory obstacles of the past and to make the export control system function in the manner originally intended by Congress.

We also took steps to evaluate the enforcement function of the Office of Export Administration in order to improve its performance. Approximately one year ago, Under Secretary Olmer asked the Inspector General of the Commerce Department to undertake an independent review of the programs, functions, and activities of the Compliance Division. As Inspector General Funk has explained to your staff, other priorities precluded such a survey at the time. Last month, however, Mr. Funk directed his staff to conduct the inspection. We expect to receive the Inspector General's findings and recommendations before the month is out.

Customs has upgraded the inspection effort, and I am pleased to announce today the organizational realignment and enhancement of the Compliance Division. The Division is itself being elevated to Office status and, together with the Office of Antiboycott Compliance, will comprise a new export enforcement organization to he headed by a Deputy Assistant Secretary reporting directly to me. The candidate we have selected for that post is currently an Assistant U.S. Attorney for the Central District of California. Theodore W. Wu is a celebrated expert in the law enforcement community whose successful

prosecutions of two of this country's most notorious export diversion cases render him highly qualified for this considerable undertaking.

In addition, with recent Congressional approval in February of our proposed reprogramming, the resources of the Compliance Division have been increased by about 40% and new field offices are being established in San Francisco and Los Angeles to supplement our Washington Headquarters and New York Field Office.

In summation, Mr. Chairman, it is our belief that the Administration, in office now for little more than 14 months, has a deliberate and sensible, yet ambitious, program to upgrade and revitalize the nation's export control enforcement efforts. Our emphasis will be leanness and efficiency; we don't envision it ever becoming a major law enforcement bureaucracy housing competing missions. Rather, ours will be an office well coordinated with the intelligence community and other enforcement agencies reflecting the comprehensive thrust of Soviet acquisition methods. Yet it will exist in an environment that is highly integrated with the other components of the government's international trade promotion and regulation sectors.

The value of Commerce's close relationship with the private sector should not be understated. As any witness from the enforcement community will verify, the information provided by the business sector is an essential element of an effective enforcement effort. This partnership exists in no other agency. The historical ties between the Department of Commerce and U.S. business, along with the new steps I have outlined regarding the strengthening of our enforcement office, make it not only the ideal, but the only logical agency to carry on the primary enforcement function mandated by the Export Administration Act.

Mr. Chairman, I want to commend you for your interest in this vital area, and I encourage you and others in Congress to join with us in this Administration's effort to improve our export control system. If you do, our partnership will go far in enhancing the security of our nation and the Free World.

REPORT OF INSPECTION

COMPLIANCE DIVISION
OFFICE OF EXPORT ADMINISTRATION
INTERNATIONAL TRADE ADMINISTRATION

Prepared by
Office of Inspector General
U.S. Department of Commerce
June 11, 1982

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Office of Investigations

I. REPORT OF INSPECTION

A. BASIS FOR THE INSPECTION

On April 13, 1982, the Inspector General directed that an inspection be made of the Office of Export Administration's Compliance Division, which oversees the enforcement of export controls for the U.S. Government. The inspection was a direct result of continuing concern of Under Secretary for International Trade Lionel H. Olmer and Inspector General Sherman M. Funk regarding the Department of Commerce's enforcement of the Export Administration Act of 1979. The inspection was conducted during the period April 19 through 30, 1982.

B. INSPECTION TEAM

The inspection was conducted under the supervision of Michael M. Ryman, Assistant Inspector General for Investigations. The inspection team included two criminal investigators, two auditors, and a management analyst from the Office of Inspector General. Personnel for this inspection team were selected to provide a wide range of both technical expertise and professional judgment.

C. SCOPE OF THE INSPECTION

The focus of the inspection was on present operations, resources and management of the Office of Export Administration's Compliance Division (OEA/CD). Assessment of the overall effectiveness of OEA/CD and the Department's responsibility to enforce the Export Administration Act was limited by the two-week length of the inspection, the immediacy of the Division's current problems, and the Department's plans to reorganize and strengthen the compliance effort in the next few months. The Office of Inspector General intends to follow up this inspection with a more detailed management audit of OEA and OEA/CD operations after the reorganization has been implemented, to ascertain the latter's impact on the effectiveness of the Compliance function.

Our inspection of OEA/CD included a review of the following:

- Goals and objectives of the compliance program, and the criteria used by management to determine their achievement;

- Procedures for identifying, initiating, and conducting compliance inspections and investigations, and the use made of the results;

- Pertinent laws and directives, budgets and financial reports;

- Conditions existing within the Compliance operation which might be hindering the Division's ability to carry out its mission.

The inspection team conducted its evaluation through interviews in Washington, D.C. with key management, supervisory and OEA operational staff (e.g., investigators, inspectors, intelligence workers, and support personnel), representatives of the U.S. Customs Service, and intelligence community liaison personnel. The team reviewed operational records, management information reports, procedural and policy guidelines, and other pertinent documents. Past evaluations of the OEA/CD -- prepared by the Department of Commerce, General Accounting Office, and others -- were also reviewed.

Classified information was reviewed during the course of the inspection, but this report contains no classified information.

D. BACKGROUND ON THE COMPLIANCE DIVISION

The Office of Export Administration's Compliance Division (OEA/CD) is responsible for enforcing the provisions of the Export Administration Act of 1979 (50 U.S.C. 2401, et seq.), except for those provisions relating to foreign boycotts which are enforced by the Office of Antiboycott Compliance. Both offices are part of the Department's International Trade Administration.

The OEA/CD is responsible for the prevention of unauthorized exports from the United States. This includes leadership of a multiagency enforcement effort; the development of information regarding possible export control violations; the investigation of suspected violations; preparation of violation cases for Department of Commerce administrative proceedings before the Hearing Commissioner; and the referral of cases to the Justice Department for criminal prosecution. The Compliance Division is also responsible for preventive enforcement activities and an ongoing program to educate exporters on export control regulations.

The OEA Compliance Division presently has three branches.* The primary functions of each are outlined below:

* The International Trade Administration has announced its intention to reorganize the Compliance Division and to raise the function to a higher level under a new Deputy Assistant Secretary for Export Enforcement. The exact realignment plan and schedule are not yet available.

1. Intelligence Branch -- develops intelligence information regarding areas of possible export administration violations; collects intelligence data on overseas firms and individuals in order to identify and evaluate their suitability and reliability as recipients of U.S. exports;

2. Investigations Branch -- investigates suspected export administration violations; in consultation with the Department's Office of General Counsel, prepares cases on violations for referral to the Hearing Commissioner or for other legal action;

3. Facilitation Branch -- conducts on-site physical inspections of cargo for evidence of export control violations; promotes compliance with export clearance regulations; maintains liaison with the U.S. Customs Service, Census Bureau and Postal authorities.

Until recently, the U.S. Customs Service provided limited investigative and inspection support on a reimbursable basis to OEA/CD. The U.S. Customs Service, with its initiation of Project EXODUS, has greatly expanded its own role in export compliance enforcement over the past 18 months.

II. SUMMARY OF FINDINGS

The inspection team found the Office of Export Administration's Compliance Division (OEA/CD) impaired by numerous internal and external problems which severely hamper its ability to enforce controls on U.S. exports. These problems include:

- -- No comprehensive appraisal of or effective overall strategy to address the Nation's technology leakage problem;
- -- Insufficient trained personnel;
- -- Inadequate management direction and oversight;
- -- Failure to use modern, state-of-the-art intelligence, investigative and enforcement techniques and systems;
- -- Lack of strong leadership and clear lines of organizational responsibility within OEA/CD;
- -- Unwarranted interference in the detailed conduct of OEA/CD investigative operations by the Deputy Assistant Secretary for Trade Administration;
- -- Inadequate cooperation and coordination with the U.S. Customs Service and vital information sources in the U.S. intelligence community;
- -- Inadequate travel funds, law enforcement equipment and other support resources; and
- -- Use of antiquated or inefficient internal administrative and management systems and procedures.

Many of the problems highlighted in this report have been identified in earlier reviews provided to ITA management. The Department of Commerce has failed to correct these problems despite strong public statements by the present and past Administrations in support of tight controls over the export of high and dual-use technologies. This failure raises serious questions about the Department's commitment to, and ability to enforce, the Export Administration Act of 1979.

The inspection team repeatedly was advised that the problems it noted reflect the Department's dual and possibly conflicting missions of trade promotion and export control. The team was not able to reach this conclusion unequivocally. It is clear, however, that the Department's failure to provide adequate

resources, policy guidance and management direction has impeded the compliance effort and produced at very least the perception of a de facto supremacy of the trade promotion mission over the Department's export control function.

What is also clear, from the findings in this report, is that the Department of Commerce has not taken a bold lead in forging an aggressive multi-agency effort to halt the illicit export of controlled products.

ITA Response

The International Trade Administration has reviewed the draft inspection report and concurs with most of the findings and recommendations. ITA's comments, which are provided in their entirety as an addendum to this report, emphasize that corrective action has already been initiated to address many of the problems cited in this inspection report. Other improvements are planned for the near future.

The Inspector General has asked the Under Secretary for International Trade to submit, within 60 days, a detailed implementation plan for each of the inspection report recommendations. The Office of Inspector General will followup on ITA's planned corrective action and will, within the coming year, conduct a review to assess the Department's progress in improving enforcement of export controls.

III. DETAILED FINDINGS

A. DUAL MISSIONS: TRADE PROMOTION AND EXPORT CONTROL

Finding # 1

There is a widespread perception that a basic conflict exists between the trade promotion goals of ITA (on the export development side) and the agency's trade restraint goals (on the export administration side). This conflict is interpreted by many observers as a major reason for inadequate commitment of Commerce resources to the enforcement function in OEA/CD.

Discussion

Virtually without exception, each of the staff interviewed in OEA, OEA/CD, the Office of General Counsel and the U.S. Customs Service referred to this conflict and acknowledged its impact -- real or perceived.

The primary mission of ITA is to foster exports, as part of the Department's overall goal to promote U.S. domestic and international business. There appears to be an inherent internal conflict when the same agency harbors within its structure organizations charged with pushing export trade and other organizations charged with restraining it, through a regulatory licensing function and the interdiction of illicit exports. Some critics have accused the Department of consciously maintaining a weak enforcement effort, of being less than enthusiastic in blocking the sale and export of controlled products, even those in the high-tech area.

The Assistant Secretary for Trade Administration recently testified that such criticism was wholly unwarranted. He emphasized that the Department's trade policy must be delicately balanced against national security considerations. We found no evidence of any ITA policy pointed toward weakening export controls in favor of export promotion. On the other hand, we found no evidence that the "delicate balance" referred to, or the Department's dual commitment to trade promotion and export control, have yet been translated into adequate staffing resources and management priorities for enforcement of the Export Administration Act. We did find ample evidence that those involved in implementing the Act, both inside and outside the Commerce Department, perceive the long history of inadequate enforcement as a manifestation of a lower priority vis-a-vis export promotion.

Recommendation

A stronger policy commitment, backed up by significantly increased manpower resources and more aggressive management, should be assigned to the control of illicit exports. The projected realignment of the compliance function in ITA must include enhanced organizational stature as well as sharply increased resource commitments. The problems arising from past inadequacies cannot be corrected by rhetoric; only effective enforcement of the Export Administration Act can erase the conflict -- real or perceived -- between the Department's trade promotion and enforcement missions.

B. INADEQUATE RESOURCES AND OPERATIONS

Finding #2

The lack of operational travel adversely affects the quality and scope of criminal investigations conducted by the Compliance Division, compounding the problems created by a shortage of staff resources.

Discussion

The Investigations Branch has less than 12 special agents to cover the entire United States. Most of OEA/CD's investigations are conducted by telephone and correspondence, handled out of the Washington, D.C. Headquarters office. A restrictive travel practice has developed in OEA/CD through the years and is a serious impediment to an effective investigative program. Investigators have been limited in their travel and must wait for inspectors from the Facilitation Branch to travel to an area to work investigative cases as a side-track from their normal inspection duties.

Operational travel is essential to an adequate pursuit of investigative leads. This requirement for travel is universally recognized by law enforcement agencies. In most OEA/CD cases examined by the inspection team, investigator travel was necessary. In many instances, however, the OEA/CD travel requests were not approved. This has resulted in delays or termination of investigations, and has allowed continued criminal activity and nonenforcement of the export laws.

Examples of lost opportunities for enforcement and prosecution of export control violations are not diffiicult to find. One recent denial of an OEA/CD agent's travel request has permitted a consortium of companies to continue their illegal export of high technology products to the U.S.S.R. and Communist Block countries via several European intermediaries; the Assistant U.S. Attorney willing to prosecute this case remains without the necessary investigator to work his case. Another agent's request for travel to the West Coast was denied despite substantial evidence of unlicensed shipment of micro chips and other restricted items. This travel denial was made by OEA/CD management with the suggestion that the case be followed through the mail.

Recommendation

More agents are needed to investigate export violation cases. The Assistant Secretary for Trade Administration should conduct a review to determine an adequate level of staff for this function, as well as other functions of the Compliance Division. Such adequate staffing should be provided as soon as possible, if necessary by shifting other ITA resources, obtaining personnel detailed from other agencies, and/or requesting an emergency budget supplement.

OEA/CD operational travel should be approved and taken as necessary in pursuit of criminal cases. Adequate management systems and controls should be established to insure that domestic travel can be taken in a timely manner. International travel should be similarly approved where justified, particularly when U.S. Customs Service or other appropriate U.S. overseas investigative personnel are not available.

Finding # 3

The Assistant Secretary for Trade Administration has been unreasonably slow in establishing Export Compliance Field Offices on the West Coast.

Discussion

Approximately 86 percent of the total value of U.S. controlled exports leave from West Coast ports and airports. Despite the bulk of these known export violations and the concentration of high technology manufacturers in the "Silicon Valley" and other West Coast areas, OEA/CD investigations and inspec performed there only a few weeks a year.

About one year ago, the Assistant Secretary for Trade Administration announced plans to establish OEA/CD field offices in Los Angeles and San Francisco, each staffed with a trained team of compliance investigators and inspectors. ITA records of July 1981 show that the Under Secretary for International Trade had discussed this plan with the Secretary who gave full support for the idea and stressed the need to accelerate the proposed operation.

On August 3, 1981, a Newsweek article mentioned the establishment of West Coast field offices by Commerce as a means to help combat high-technology smugglers. ITA records show that the Assistant Secretary for Trade Administration advised the Secretary two days later that the San Francisco and Los Angeles field offices were scheduled to open October 1, 1981, and both offices would be fully operational within three to six months. However, these field offices had not been opened and staffed as of April 30, 1982.

The Assistant Secretary for Trade Administration cites internal OEA/CD management problems as the reason he did not push ahead with the West Coast offices last fall. He did not wish to put new staff and resources out in the field, when OEA/CD was already engulfed in severe management problems which made it difficult to manage its existing structure and resources. Within the last month, the Assistant Secretary has announced a plan to reorganize the Compliance Division, raise it to office status headed by a new Deputy Assistant Secretary with a strong law enforcement background. Plans to open the West Coast offices apparently are now back on track.

Despite the above explanation for the delays in opening the West Coast offices, there is no doubt that the Compliance Division's enforcement of the export law suffered because of the repeated delays. We believe that the mere presence of additional OEA/CD manpower on the West Coast during the past year would have provided worthwhile deterrence and detection coverage.

Recommendation

ITA management should expedite the establishment and staffing of Export Compliance Field Offices on the West Coast. These offices should be staffed with adequate numbers of trained and experienced investigators and inspectors.

Finding #4

The Compliance Division frequently hires inexperienced investigators and provides no training for its investigative staff.

Discussion

The Compliance Division has hired entry-level investigators with no experience or specialized training, instead of badly needed journeymen. In one case, an untrained and inexperienced new hire was allowed to investigate for six months without investigator's credentials.

Compounding the problems created by inexperienced manpower, OEA/CD requires or offers no investigative, intelligence or enforcement training to its investigative staff. There is no program or materials to provide training to new hires or journeyman investigators. On-the-job training is also very limited and only available from individual OEA/CD investigators who were trained by other agencies before coming to the Compliance Division. Some of the investigators had no investigative training or experience at all when they assumed their OEA/CD duties; this is a violation of OPM standard X-118. Investigators have requested formal training, but it has been refused because they could not be spared from their normal duties.

The training program in effect in FY 1980 appears to have been limited to a report writing course for all special agents, a short version of a white collar crime course, and a case management course for the supervisor of the Investigations Branch. Such training, inadequate then, has been further reduced: financial records show a total expenditure of $24.98 for training of Compliance Division personnel in FY 1981, and no expenditure at all thus far in FY 1982.

Recommendation

The Compliance Division should develop and implement a formal training program for all newly hired and present undertrained personnel. This should include utilization of the Federal Law Enforcement Training Center and other established law enforcement training facilities, as well as structured on-the-job training. A training profile should be developed for each OEA/CD investigator to determine his individual training needs. OEA/CD personnel should be adequately trained in all aspects of law enforcement, including intelligence, surveillance, investigations and inspections, judicial proceedings and case handling. The Department should provide adequate funding for OEA/CD's training needs.

Finding #5

The Compliance Division lacks virtually any law enforcement technical equipment, although such equipment is needed to conduct investigations effectively.

Discussion

The Compliance Division does not have technical equipment for the collection of criminal evidence, such as cameras, surveillance team communications equipment, consensual monitoring and other law enforcement devices. In the past, when investigative technical aids were needed, they were either borrowed from other agencies or were personal equipment loaned by individual investigators. Past efforts to procure these essential items have been unsuccessful.

OEA/CD's failure to obtain required investigative equipment is particularly difficult to understand inasmuch as OEA/CD funds for this purpose have been used to purchase equipment for other OEA offices and to furnish OEA/CD's unoccupied new field office in Los Angeles. Examination of ITA accounting records maintained by the Office of Financial Operations, Office of the Secretary, revealed that $37,445 of approximately $52,000 in office furniture and equipment charged to the Compliance Division for the period October 1980 to March 1982 was used for a record processor microcopier system installed and used in the Operations Division's licensing activity. Also, office furniture valued at approximately $1,800 was delivered to the Los Angeles Export Compliance Field Office, although this office is still neither open nor staffed.

Recommendation

The Department should purchase the essential investigative equipment required by the Compliance Division.

Finding #6

The Compliance Division's current intelligence operations are almost exclusively reactive rather than proactive in nature. An efficient and effective intelligence operation cannot be conducted in such a manner.

Discussion

Due to manpower shortages and/or policy and management direction, OEA/CD has never aggressively developed its own intelligence leads on potential export violators, or actively solicited such leads from the intelligence community. The Department should be directing and/or soliciting a steady flow of information and close working cooperation between the Department and the U.S. intelligence community and COCOM intelligence agencies to identify targets, patterns and sources of controlled technology leakage.

In actuality, however, OEA/CD's Intelligence Branch even fails to regularly use the information currently available through OEA's License Accounting Retrievel System (LARS). The Compliance Division has taken little or no initiative to work with OEA to expand and improve its ability to develop "intelligence" information through the export licensing and other review processes. The LARS data base could provide a valuable source of intelligence information. The data base information is particularly useful for trend and cross-pattern analyses in detecting illegal transshipments and diversions of goods through other countries. In some cases, the OEA Operations Division used LARS data to strengthen ongoing investigative cases. However, to date LARS or other intelligence data is not systematically being used by OEA/CD personnel in a similar manner. One major reason for this is that the Intelligence Branch currently lacks sufficient staffing and expertise, including computer specialists, to undertake this type of intelligence operation.

Recommendation

The Commerce Department and its Compliance Division must increase its cooperation with and the flow of relevant information from the U.S. and COCOM intelligence communities, including specific information on the Soviet Bloc's Western technology import strategy and targets, exporters of controlled technologies, their diversionary routes and schemes, and third country participants in such schemes.

The Intelligence Branch should be given sufficient computer specialist and analytical staff, and full access to LARS, to enhance their in-house intelligence operations. The LARS data base should be expanded to include distribution license information and other available data which may be useful to the intelligence operation.

Finding #7

OEA/CO intelligence operations are severely hampered by

- o Inadequate and delayed intelligence analyses of information or leads on possible export violations.
- o A failure to adequately control, protect and centrally maintain source documentation establishing possible investigative leads.

Discussion

The Intelligence Branch is responsible for processing, analyzing, and augmenting information on potential violations of export laws and regulations for possible referral for investigative action. Sources of information include Application Screen leads referred from OEA's Operations Division, voluntary and informant disclosures, referrals from other agencies, violations discovered by the Facilitation Branch, information from the intelligence community and others.

For the period October 1, 1981 to April 21, 1982, the Intelligence Branch logged in 598 cases or referrals of potential violations; only 74 cases were reviewed during that period. In addition, there are several hundred backlogged cases from prior years; the Intelligence Branch is currently able to do no more than store these cases. While the inspection team was unable to assess the quality of the intelligence reviews conducted on the 74 cases processed, it is not unreasonable to conclude that the Intelligence Branch is ineffective in providing timely and accurate assessments of suspected violations. Less than 15 percent of the leads received by the Intelligence Branch were processed during this one six-month period, and hundreds of leads from prior years have gone untouched.

The effectiveness of an intelligence arm of a law enforcement agency is only as good as its ability to respond in a timely manner with a careful and informed analysis of the intelligence information. Failure to do so only thwarts the necessary followup investigation, possible prevention of the actual export violation and successful criminal prosecution of or administrative action against violators. A large backlog in the Intelligence Branch slows the investigative process since most investigations are not started without the intelligence referral. Furthermore, the backlog puts undue pressure on the small staff in the Intelligence Branch to cut short their intelligence analyses, close cases prematurely, or forego further information gathering from the intelligence community or other sources. A staff of five persons is totally inadequate to provide necessary intelligence data and analyses on suspected export violations.

The Intelligence Branch's manpower problems are further compounded by the absence of any systematic review of incoming cases or information leaks and an internal filing and accounting system to keep track of the Branch's backlog to ensure that the cases are handled in order of priority and are not lost or misplaced. The current system places almost total reliance upon the memory and judgment of the Chief of the Intelligence Branch to determine the significance and disposition of the backlog of potential violations. Little or no effort is made within the Intelligence Branch to process or prioritize the received intelligence. It functions as little more than a depository and ineffective conduit to the investigative section.

Recommendation

Additional manpower should be assigned to the intelligence function, whether it remains as presently structured or is relocated to another unit in OEA, combined with OEA/CD investigations or given greater resource assistance from other intelligence agencies. A review should be made of the entire OEA intelligence processes to determine whether intelligence information is adequate and effectively collected, whether maximum and timely cooperation is available from all appropriate segments of the intelligence community, and how the analysis of intelligence information and leads could be better handled and expedited to prevent, or at least detect and detain, illegal export shipments.

Automation of the intelligence gathering and internal filing and control systems is needed, but more drastic improvements also must be made to increase the effectiveness and efficiency of the intelligence operation.

Finally, a special effort must be made to eliminate the current backlog of Intelligence Branch cases. A special team of intelligence and investigative agents, perhaps including details from other agencies, should be assigned this task with clear, written instructions on how to review these cases and recommend appropriate action. We suspect that most of these leads are lost opportunities, but they contain crucial information on possible violators, illegal export items, importers and foreign government or company practices, which should be fed into the current intelligence data base.

Finding #8

OEA's license application screening, which is vital to the compliance function, is an antiquated manual process which, in practice, does little to help detect violations of export laws and regulations.

Discussion

One of the principal sources of leads for OEA/CO investigative followup is the Application Screen. The Application Screen is a file containing an alphabetical listing of the names of persons and/or firms (exporters, consignees, distributors, etc.) which were previously denied export privileges or are suspected of illegal exporting activities. Those of national security concern are also on the list. Additions and deletions of names from the screen are made by the Operations Division at the direction of the Compliance Division.

The Application Screen process involves four full-time processing clerks (three GS-5's and one GS-6) who manually check all the information on the face of a license application against the large rotary card screen file. If any of the individual or business names on the license application match those in the screen file, the application is referred to OEA/CO's Intelligence Branch.

There are several shortcomings in this vital screening process:

1. Manual operation of the review process provides too many opportunities for human oversight or error. Names can be overlooked, or not recognized because of misspelling or purposeful omission by the applicant without detection by OEA clerks. Given the volume of applications and the screen file listings, it is not surprising that human oversights have resulted in suspect licenses going through the screen undetected.

2. The present screen name listings are, in large part, historical. They represent companies or persons involved in past export violations or suspect cases. A manual system is not updated with the speed necessary to provide vital, current intelligence data and information on today's violators. The current process also does not screen out the repeat violators who change the name of their company, use a new intermediary company, change their own names, or recruit new "principals" for their illegal export operations.

Recommendation

We understand that OEA is now planning an overall review of computer applications for various OEA functions. Priority should be given to automation of the screen process and the Compliance Division's intelligence gathering and internal control needs. Such automated systems, which can be accessed by all appropriate agencies, are needed for immediate entry of data on all current investigations, new violations, and new suspects from the intelligence community and other sources. The new automated screen process should also be able to go far beyond a simple match of names; it should help detect deceptive submissions, omissions or substitutions by applicants, or at least flag the more obvious ones for further review.

C. COOPERATION WITH THE U.S. CUSTOMS SERVICE

Finding # 9

Cooperation and coordination between the Compliance Division and the U.S. Customs Service are inadequate and adversely affect enforcement of export laws.

Discussion

Strong cooperation between OEA/CD and the U.S. Customs Service is essential to effective enforcement of export controls and to supplement the Compliance Division's insufficient investigative and inspection manpower in the U.S. and overseas. The OEA/CD inspectors must use Customs officials for search and seizure of suspected cargo, since OEA/CD inspectors do not have such authority. Despite the obvious need for cooperation between the two agencies, the Compliance Division does not maintain effective liaison with the U.S. Customs Service. There have even been efforts by some Compliance Division personnel to avoid coordination with Customs. There have also been incidents of interagency hostility and investigative case interference by both the Compliance Division and Customs.

One major source of the hostility has been Commerce's narrow interpretation of Paragraph 12(c) of the Export Administration Act and OEA's unwillingness to disclose confidential licensing information to Customs and other law enforcement agencies. (See Finding #11.) Customs-Compliance Division competition and turf battles have intensified during recent months with Congressional hearings focused on the enforcement of export laws and interagency rivalry. The absence of a signed ITA-Customs interagency agreement for FY 1982 has further hampered their cooperation. (See Finding # 10.)

Current OEA liaison with U.S. Customs Service on Project EXODUS is being handled chiefly by an individual-- an expert/consultant-- whose efforts are divorced from the operations of the Compliance Division. Even though the liaison effort is assisted by the presence of U.S. Customs Service agents assigned to OEA, this arrangement is inadequate. (See Finding #13).

Recommendation

The Assistant Secretary for Trade Administration should make a

policy commitment to and negotiate strong Customs-OEA/CD cooperation. This commitment must be communicated down through the ranks of both agencies as operating policy. Written guidelines and procedures should be developed to support improved cooperation; they should clearly spell out the jurisdiction of each agency, how and what constitutes liaison, what arrangements and resources exist for domestic and overseas support, and what are the responsibilities and obligations of each agency to a unified export enforcement effort. (Also see Finding #10.)

Finding #10

OEA and Compliance Division officials are not aware of the actual level of support furnished by the U.S. Customs Service for ITA's export control compliance matters. The transfer of appropriated funds from the Compliance Division accounts could be excessive.

Discussion

Until January of this year, the U.S. Customs Service provided investigative, inspection, and administrative support to OEA under a cost reimbursable interagency agreement with ITA. For FY 1981, at a total cost of $200,000, the U.S. Customs Service agreed to provide:

- 2 manyears of at-large investigative support
- 2 inspector positions at J.F.K. International Airport in New York
- 3 manyears of at-large inspector services at various posts throughout the U.S.

There is no record of the actual support provided by the U.S. Customs Service under this interagency agreement. Lacking this record, ITA cannot certify that payment to the U.S. Customs Service is correct and proper, as stated on the Voucher and Schedules of Withdrawals and Credits (SF 1081). A 1980 management study, conducted by the Deputy Assistant Secretary for Export Administration, concluded that the U.S. Customs Service was paid for services it did not provide.

There is no written agreement for U.S. Customs Services to provide export control compliance support in FY 1982. OEA cancelled Customs' services effective January 15, 1982, and requested information on the actual services rendered during the fiscal year to that date. No response had been received from Customs as of April 30, 1982.

Recommendation

A follow-up request should be sent to the U.S. Customs Service by the Assistant Secretary for Trade Administration to obtain a record of actual services rendered by Customs in FY 1982 and under the FY 1981 interagency agreement. Such documentation is necessary to support ITA certification that the SF 1081s are correct and proper for payment.

For all future cost reimbursable interagency agreements with Customs, or any other agency, OEA and the Compliance Division should clearly specify in the agreement what services or products are to be provided at what cost. In addition, OEA or the Compliance Division should maintain its own cost accounting records and require monthly charge reports from the provider agency.

95-929 O - 82 - 41

Finding #11

A strict construction or a narrow interpretation of Paragraph 12(c) of the Export Administration Act of 1979, by the Office of Export Administration and the General Counsel's Office, has impeded the progress of criminal investigations and prosecutions.

Discussion

Commerce interprets Paragraph 12(c) of the Act to require that written permission of the Secretary of Commerce must be obtained in each incident where ITA licensing information is released for disclosure during a criminal procedure. This policy includes disclosures to grand juries and U.S. magistrates. It also includes information placed in statements made in requesting legal powers; e.g., search warrants. This requirement has delayed OEA/CD's release of vital investigative case information and has been used to justify minimal or delayed cooperation with the U.S. Customs Service when it requests information in connection with criminal investigations.

Numerous questions have been raised about the wisdom and legality of Commerce's interpretation of Paragraph 12(c). We note that the same restriction applies as well to disclosures of information regarding munitions and weapons exports under the control of the State Department. However, the State Department has issued blanket authority to allow such disclosures in law enforcement efforts involving its export cases. No such authority has been issued by Commerce.

Recommendation

The Secretary of Commerce should issue blanket authority for release of Paragraph 12(c) type information in law enforcement efforts.

D. MANAGEMENT DIRECTION AND OVERSIGHT BY ITA

Finding #12

The Deputy Assistant Secretary for Export Administration and the Director of OEA have circumvented OEA/CD management and become personally and directly involved in the conduct and disposition of investigations. This has tended to:

- denigrate the established chain of command and management;
- create multiple sources of concurrent supervisory instruction to the operating staff; and
- detract from the efficient and effective operation of the Compliance Division.

Discussion

The DAS and Director of OEA justify their direct personal involvement in individual investigations on the basis of their perception that the Compliance Division's investigators and managers are largely unqualified, and are naive regarding the political ramifications of their actions. While there may be some validity to these charges, there is an alternative and more effective approach which should have been taken by the DAS to handle the situation. The DAS could have worked to improve the qualifications, resources and effectiveness of the Compliance Division, rather than circumventing OEA/CD and pursuing investigations without the direct involvement of Compliance Division managers. The DAS apparently prefers to use "favorite son" investigators and a paid consultant to manage and conduct important investigations.

In addition to using investigative teams outside of the formal OEA/CD structure, the DAS personally intervenes and conducts crucial aspects of sensitive investigations. For example, he personally intervened in the Piher/Suin investigation (Case No. 81-359) by traveling in lieu of an experienced investigator, as was requested by the Foreign Commercial Service, and failed to file a written report of his activities, as requested by the Director of the Compliance Division. The DAS subsequently directed that this case be reassigned from the original case agent to an agent of his choosing. Similar actions were detected in inspection team's review of Case Nos. 82-76, 82-68, 81-271, 82-55, 81-377, and 80-12.

It is obviously both the perogative and responsibility of the DAS to set overall policy for and oversee OEA operations, including

those of the Compliance Division. In special cases, this may even warrant some degree of personal DAS involvement in case investigations. However, it is counter-productive for the DAS to conduct day-to-day operations or call the shots routinely in an investigative case. it is a waste of available trained investigators and can have a devastating impact on the morale of the Compliance Division employees, particularly inasmuch as the DAS himself is neither a trained investigator nor has any background in criminal investigation.

Recommendation

Investigations of potentially criminal violations and national security matters should be conducted by trained OEA/CD investigators, without interference in their day-to-day fact-finding operations.

The Department should obtain qualified individuals to manage the OEA/CD, if they are not now available. This would include the pending employment of Theodore Wu as a new DAS for Export Enforcement to oversee intelligence and enforcement operations. However, it should also extend down to the management of all OEA/CD operating units. Efforts should be made to upgrade the quality of the existing staff and resources. These efforts should include the development and implementation of a training program, inasmuch as newly hired personnel learn on the job from investigators whose own qualifications are limited. (See Finding #4).

Finding #13

The Deputy Assistant Secretary for Export Administration has weakened the Compliance Division by shifting part of its functions and responsibilities to a consultant and task force which operate outside of the Division. The DAS has misused this expert/consultant whom he hired ostensibly to evaluate and upgrade the compliance function. Personnel regulations have been violated, as well as sound management practices, by interjecting this consultant in an operating role for which he has little expertise.

Discussion

The DAS originally authorized the hiring of the expert/consultant for a 30-day term and has since extended his appointment five times. According to his position description, the consultant is to enhance the efficiency and effectiveness of the Compliance Division. Specifically, he is to

- Make recommendations to improve intelligence capabilities and operations;
- Evaluate the need, if any, for additional law enforcement powers;
- Design and establish programs in support of future and ongoing investigations;
- Perform other special projects as agreed upon between him and the Director of the Compliance Division.

In fact, however, the consultant has not improved the operations of the Compliance Division, nor has he worked with the management or staff of that Division. The consultant's activities bear little, if any, resemblance to his position description. Rather, there is considerable evidence that the consultant and DAS have further reduced the effectiveness of OEA/CD by stripping it of many of its assigned functions and resources. The inspection team found numerous problems and inconsistencies between planned (as outlined in his position description) and actual activities of the consultant which have disrupted or weakened OEA/CD operations. These include:

- A task force has been assembled to work with the consultant. It includes two U.S. Customs agents and OEA's principal computer expert, but does not include anyone from the Compliance Division. This group independently carries out many of the investigative and interagency liaison and intelligence coordination functions assigned to the Compliance Division.

- The consultant's task force operates without any specified scope of work, time frame, or performance and reporting requirements.

- The consultant's task force, rather than the Compliance Division, acts as the central liaison between the Department of Commerce and the U.S. Customs Service on Project EXODUS.

- The consultant works closely with OEA's computer and licensing people to develop new and improved intelligence information. However, this again is done without consultation or cooperation with OEA/CD.

- The consultant has had very little interaction with the Director and employees of the Compliance Division. He reports directly to the DAS and not to the Director of the Compliance Division, as stated in his position description.

- The consultant's position designation as critical nonsensitive is in conflict with the direct investigative duties he has performed and the provisions of DAO 207-4. The DAS has turned over several classified investigative cases, initiated by the Compliance Division, to the consultant.

- The consultant has performed no significant analysis or evaluation of the operations of the Compliance Division as is stated in his position description. No identifiable product was located.

Although there are some benefits to be derived from the consultant's efforts his independent operation further fragments Commerce's already limited effort to enforce export controls and provide strong, unified leadership to an interagency program to prevent or detect illegal export of controlled technologies.

The inspection team also questions the legality and propriety of the hiring of this consultant. Instructions covering the employment of experts and consultants are contained in Chapter 304 of the Federal Personnel Manual. Manual subchapters 1-3 state that improper employment of experts and consultants is not only illegal, but also wasteful and destroys the morale of career specialists. One of the manual examples of improper employment of an expert is assignment to a noncritical, nonsensitive position which could be handled as well by a regular Federal employee. Such a violation seems to have been made in this case. Financial compensation ($93 per day) for this full-time position may also have been made to avoid competitive employment procedures and General Schedule pay limits.

Recommendation

The consultant's task force should be disbanded; the work initiated by the task force should be continued by the Compliance Division as follows:

- The liaison function with the U.S. Customs Service should be continued and enhanced by the Intelligence Branch;

- The expanded use of the LARS data base for intelligence gathering operations should continue to be pursued by the Intelligence Branch with OEA's computer experts.

To the extent that the Compliance Division and the DAS believe that there is a need to continue the services of this or another expert/consultant, the latter should report to the Director of the Compliance Division. Certain aspects of the consultant's efforts have significant merit, but appear far outside the scope of his position description as currently written. A written agreement should be prepared to specify his mission and work products.

Both the DAS and OEA/CD should adhere to all appropriate personnel regulations concerning the hiring and use of experts/consultants. Special care must be taken to avoid assigning consultants to operational duties which would normally be handled by civil servants. Rules regarding extension of term appointments and financial compensation should be followed.

E. INTERNAL ADMINISTRATION AND MANAGEMENT SYSTEMS

Finding #14

The Compliance Division does not have an effective management information system or automated administrative processes, including case control and time reporting systems and information storage. The current manual processes waste staff time, lend themselves to human errors, and do not provide management with sufficient information to effectively and efficiently carry out the compliance function.

Discussion

The Chief of the Intelligence Branch has the primary responsibility for compiling and maintaining statistics for the Compliance Division. Branch Chiefs and staff members of the Compliance Division also devote a substantial portion of their time generating statistical and administrative reports for various sources in OEA, ITA, and the Congress. This information is usually necessary for management's use, but could be more quickly and efficiently produced if the manual information storage and retrieval systems now in existence were automated. The current systems place excessive reliance on the memories of individual managers and agents as to the significance and status of hundreds of investigative cases and leads. Furthermore, the time devoted to compiling and reporting this information detracts from the time devoted to intelligence, inspections, and investigative operations. Given limited staff resources, the need to automate is that much more urgent.

Recommendation

An analysis of computer applications within the Compliance Division should be performed. This can be done in conjunction with the requirements analysis being arranged by the OEA Operations Division. Wherever the benefits outweigh the costs, management information and administrative processes should be automated. Strong consideration should also be given to the creation of a dedicated, secured system for the licensing and compliance operations, due to the national security issues involved and the use of sensitive and classified information.

Finding #15

Operational policies and procedures of the Compliance Division were found to be nonexistent or outdated and not widely disseminated to staff members.

Discussion

The inspection team found few operational policies and procedures for the Compliance Division. The most significant procedural guidelines applicable to the operations of the Compliance Division are the OEA manual and the agent's manual. The Compliance Division did not have a copy of the OEA manual and some employees did not even know of it's existence. The team reviewed a copy of the OEA manual maintained by the Operations Division; it is fairly comprehensive and informative on the interaction and relationship between the licensing and compliance functions. However, the OEA manual's section on "Intelligence Information, Investigation, and Enforcement" was last updated in 1973, with many sections written as early as 1956.

The agent's manual was similarly outdated. Most of the investigators do not have a copy of that manual; there are few copies available. Furthermore, the manual is classified at a level above that of most OEA/CD agents. Such classification seemed unwarranted.

Recommendation

OEA/CD operating procedures and manuals should be updated and readily available to staff. If classified information must be included in the agent's manual, it should be restricted to a separate appendix to permit free and ready access by agents to the manual's basic operating procedures and information. Considering the present lack of training provided new investigators, an agent's manual is an absolute necessity.

Finding #16

The Compliance Division has maintained inaccurate accounting records of its travel costs. Its reports to the Office of Export Administration in Fiscal Year 1982 significantly understated actual monthly travel costs.

Discussion

Since November 1981, units of the Office of Export Administration have been directed to provide monthly cost data on certain categories of expenses for internal management purposes. One of these cost categories is for travel.

Comparison between travel costs reported by the Compliance Division ($13,032) and actual costs shown in Commerce accounting records ($26,778) show a difference of more than 100 percent as of February 1982. The inspection team found no evidence that this discrepancy was due to diversion of OEA/CD travel funds to non-OEA/CD uses. Rather, the team attributed the difference, at least in part, to a failure to include all OEA/CD travel claims for each month in the reports prepared for the Director of the Compliance Division.

Recommendation

The Compliance Division should reconstruct its travel costs for FY 1982 and provide the Office of Export Administration with corrected financial reports. An accurate internal financial accounting system should be established and maintained by OEA/CD to ensure proper and effective use of all available OEA/CD funds.

Finding #17

The assigned working space of the Compliance Division is inadequate and has an adverse effect on the ability of the Division to perform its mission.

Discussion

The Compliance Division's working space is crowded, poorly equipped, ill-maintained, and noisy. This contributes to low staff morale and impedes investigative effectiveness. While this condition, of itself, would not usually disrupt normal activity, its impact is grossly magnified by the myriad of other problems and shortages facing OEA/CD.

The currently assigned space provides no opportunity for staff to conduct private meetings with sources of information, other enforcement agency personnel, co-workers or other persons wishing to discuss confidential matters or cases. Furthermore, it is not good security practice to hold staff discussions of sensitive and, on occasion, classified information in the current open work areas.

Recommendation

The Department should provide adequate and secure working and file space for the Compliance Division.

ADDENDUM

UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for International Trade
Washington, D.C. 20230

July 2, 1982

MEMORANDUM FOR SHERMAN FUNK

FROM: Lionel H. Olmer

SUBJECT: Comments on Draft Report on Export Enforcement

I have reviewed your draft Report and its findings and recommendations concerning operations of the export enforcement group in Trade Administration. ITA's comments are attached.

I hope that you recognize that many of the problems your investigators reported upon are soon to be things of the past or already are. ITA has agreed to report back to the Senate Permanent Investigations Subcommittee later this year on the progress we have made in addressing these problems; we will have a very positive story to tell on that occasion.

I hope you will incorporate as much as possible of our response into your final Report. I would especially urge you to ensure that your final Report takes notice of several important ITA initiatives taken well before the date of the draft Report to correct the situation. These include, for example, the planning and implementation of a major reorganization designed to improve export enforcement, including the appointment of a new Deputy Assistant Secretary for Export Enforcement.

By failing to make adequate mention of this key reorganization, as well as other ITA initiatives on enforcement, the draft Report gives the incorrect impression that ITA has taken no effective remedial action whatsoever during the past year.

In any event, please include our entire response as an addendum to your Report.

Attachment

SUMMARY OF FINDINGS
(Report page 4)

FINDING: No comprehensive appraisal of or effective overall strategy to address the Nation's technology leakage problems

RESPONSE: The Department has undertaken several initiatives to rectify this problem. As explained by Assistant Secretary Brady in his May 12, 1982 testimony before the U.S. Senate Permanent Subcommittee on Investigations, the Administration directed the intelligence agencies to prepare a comprehensive appraisal of Soviet technology acquisition efforts. On the basis of the initial results of that appraisal the Department has taken the following steps:

(1) Creation of a Foreign Technical Assessment Center within the Office of Export Administration, tasked with maintaining a data base enabling the Department to assess foreign availability of technology.

(2) Pursuit of stronger ties with the intelligence community and other enforcement agencies, both with respect to intelligence collection and intelligence utilization.

(3) Elevation to office status of the Compliance Division, to be headed by a new Deputy Assistant Secretary for Export Enforcement (DAS/EE). The Office of Export Enforcement (OEE) will be an aggressive enforcement organization, with field offices in Los Angeles, San Francisco and New York. The establishment of additional field offices will be considered as needs arise.

(4) Tasking of the DAS/EE with the responsibility for developing strategy for addressing the Nation's illegal technology transfer problems. Such a strategy is now in the formulation stage.

FINDING: Insufficent trained personnel

RESPONSE: We concur in this finding. However, it should be recognized that the Department has already taken important steps to correct the situation, including initiation of a vigorous program to recruit professional law enforcement personnel with extensive criminal investigation experience. In this connection, the Department is in the process of eliminating current obstacles to

the recruiting of experienced law enforcement personnel, such as the unavailability of premium pay for administratively uncontrollable work by export enforcement special agents. We are also actively pursuing the matter of obtaining firearms, and search, seizure and arrest powers for our export enforcement special agents. Finally, we plan to deliver an effective, professional training program which will include instruction not only in conventional law enforcement, such as surveillance and search and seizure techniques as well as Federal criminal procedures, but also will include training in problems unique to export enforcement. The in-house portion of the training program will concentrate on specialized export control enforcement techniques, trade intelligence and technology acquisition trend analysis.

FINDINGS: (a) Inadequate management direction and oversight

(b) Lack of strong leadership and clear lines of organizational responsibility within OEA/CD

RESPONSE: Recognizing that the management structure inherited from the prior Administration was inadequate to the task of stemming an accelerating tide of illegal technology transfer, we have taken steps to rationalize that structure. As a result, the Department has established the post of Deputy Assistant Secretary for Export Enforcement, whose only responsibility will be directing the Department's export control enforcement and antiboycott compliance efforts. The new DAS/EE brings solid law enforcement management skills to his position. One of his highest priorities is to establish management objectives and milestones in order to concentrate resources and talents on the timely fulfillment of the Department's export enforcement mission.

FINDING: Failure to use modern state-of-the-art intelligence, investigative techniques and systems

RESPONSE: We agree that much remains to be done in the area of developing a sophisticated, comprehensive response to illegal technology transfer. However, the Department has made a good start in recent months toward attaining this objective. For example, we have created a specialized analytical unit which correlates licensing and other intelligence data in order to identify

possible diversions and diversion routes. This unit will soon be fully integrated with the Department's operational export licensing and enforcement arms. Further, the Office of Export Administration (OEA) has established a technology transfer unit which is tasked with providing data to the Office of Export Enforcement. Moreover, the Office of Export Enforcement's own intelligence unit will be staffed by personnel having both intelligence and criminal investigation expertise.

FINDING: Unwarranted interference in the detailed conduct of OEA/CD investigative operations by the Deputy Assistant Secretary for Trade (sic) Administration

RESPONSE: (See our response to Finding #12 below.)

FINDING: Inadequate cooperation and coordination with the U.S. Customs Service and vital information sources in the U.S. intelligence community

RESPONSE: Concurrent with the restructuring and enhancement of our export enforcement effort, the Department is continuing to move vigorously to improve cooperation and coordination with the intelligence agencies. For example, the Department is sharing and will continue to share with the intelligence agencies certain threat appraisal and technology transfer intelligence collection and analysis responsibilities. In addition, the Department's licensing and export control arms will make every effort to improve the frequency and effectiveness of their liaison with the intelligence agencies.

The Department has increasingly sought to improve cooperation with the Customs Service at all levels. For example, the Department made a special effort in recent months to share licensing and intelligence data with Customs personnel in order to facilitate the development of profiles for use in "Operation Exodus." In addition, the Department is presently exploring with Customs ways of more efficiently allocating the export control responsibilities of the two agencies, such as assigning primary responsibility for inspections at points of exit to Customs.

We fully expect these efforts at improved cooperation to be successful and to result in a more effective united front against the illegal technology transfer threat.

FINDING: Inadequate travel funds, law enforcement equipment and other support resources

RESPONSE: We agree with this finding to the extent that it reflects the priorities accorded in past years to the budget and manpower needs of export control enforcement. The Department is now fully committed to funding the travel, logistical, space and equipment needs which are associated with the development of an investigative force which will be greatly improved both in terms of quality and quantity.

FINDING: Use of antiquated or inefficient internal administrative and management systems and procedures

RESPONSE: We agree with this finding of the Report. The need for application of advanced data processing techniques to the licensing and intelligence analysis functions, as well as to the enforcement mission, is critical. To achieve this goal, there must be both complete commitment and a vigorous follow-through on the part of all management levels of the Department.

DETAILED FINDINGS
(Report pages 6-32)

FINDING #1: There is a widespread perception that a basic conflict exists between the trade promotion goals of ITA (on the export development side) and the agency's trade restraint goals (on the export administration side). This conflict is interpreted by many observers as a major reason for inadequate commitment of Commerce resources to the enforcement function in OEA/CD.

RECOMMENDATION: A stronger policy commitment, backed up by significantly increased manpower resources and more aggressive management, should be assigned to the control of illicit exports. The projected realignment of the compliance function in ITA must include enhanced organizational stature as well as sharply increased resource commitments. The problems arising from past inadequacies cannot be corrected by rhetoric; only effective enforcement of the Export Administration Act can erase the conflict — real or perceived — between the Department's trade promotion and enforcement missions.

RESPONSE: The language employed in the report implies a conscious effort by past and present ITA management not to increase resources for enforcement of the Export Administration Act. Since FY 1973, the number of positions and level of resources devoted to export enforcement increased from 29 positions and $1.5 million to 54 positions and $2.3 million in FY 1983. This increase is primarily composed of an FY 1978 Supplemental that increased compliance by 2 positions and a reprogramming of 15 positions to export enforcement at the expense of other ITA programs. ITA management is actively considering requests for other resource increases.

Nevertheless, we recognize that this perception has existed to some extent in the past, even though the Department's interest in export promotion is obviously limited to the promotion of lawful exports. However, we believe that this perception is in the process of changing from one of inadequate commitment to export enforcement to one of complete commitment.

We agree with the recommendation and have taken the steps outlined in our reply to the first Summary Finding.

95-929 O - 82 - 40

FINDING #2: The lack of operational travel adversely affects the quality and scope of criminal investigations conducted by the Compliance Division, compounding the problems created by a shortage of staff resources.

RECOMMENDATION: More agents are needed to investigate export violation cases. The Assistant Secretary for Trade Administration should conduct a review to determine an adequate level of staff for this function, as well as other functions of the Compliance Division. Such adequate staffing should be provided as soon as possible, if necessary by shifting other ITA resources, obtaining personnel detailed from other agencies, and/or requesting an emergency budget supplement.

OEA/CD operational travel should be approved and taken as necessary in pursuit of criminal cases. Adequate management systems and controls should be established to insure that domestic travel can be taken in a timely manner. International travel should be similarly approved where justified, particularly when U.S. Customs Service or other appropriate U.S. overseas investigative personnel are not available.

RESPONSE: We concur in this finding. An effective law enforcement operation tasked with stemming illegal exports necessarily involves extensive mobility and must therefore be predicated upon an adequate travel budget, as well as the appropriate delegation to line managers of the authority to approve operationally critical travel requests.

The lack of investigative travel is not attributable solely to resources as the following data show:

	Travel Expenses ($000)	
	Export Enforcement	Other OEA
FY 1980	46	52
FY 1981	43	44
FY 1982 (est.)	60	60

ITA program managers are allocated resources for official travel based both on past experience and on the presentation of evidence of future expansion. Until the arrival of the new DAS/EE, however, compliance management had not voiced to senior ITA management any need for additional travel resources.

Also, we found in an April 1980 study that most of the former Compliance Divisions investigators were reluctant to travel, principally for personal reasons. In expectation of a vigorous pursuit of his duties by the new DAS/EE, ITA senior management is planning to increase the level of travel resources available to export enforcement.

We are also working to determine the appropriate level and sources for additional staffing of the export enforcement effort.

FINDING #3: The Assistant Secretary for Trade Administration has been unreasonably slow in establishing Export Compliance Field Offices on the West Coast.

RECOMMENDATION: ITA management should expedite the establishment and staffing of Export Compliance Field Offices on the West Coast. These offices should be staffed with adequate numbers of trained and experienced investigators and inspectors.

RESPONSE: A notification of proposed reprogramming was sent on May 28, 1981 to Senate Appropriations Committee Chairman Hatfield and to House Appropriations Subcommittee Chairman Smith. The request included shifting 15 positions from other program areas of ITA for the export compliance function.

Establishing offices on the West Coast was not explicitly mentioned in that reprogramming notification. The special reprogramming notification to create field offices was held up pending departmental resolution with OMB of ITA's FY 83 budget request—agreed to in December, 1981. Promptly upon Congress' return, the Department sent a second reprogramming notification requesting specific approval for the establishment of export enforcement offices in San Francisco and Los Angeles. Approval of this request by Congress came on February 23, 1982. In view of the imminent reorganization of ITA's export enforcement organization, implementation of the staffing of the West Coast offices was deferred to give the new DAS/EE the opportunity to direct that staffing.

As the Report's discussion of this finding recognizes, plans to open the West Coast field offices are now back on track. The Department is now pressing GSA to provide appropriate quarters as soon as possible to handle the enhanced staffing for these offices.

FINDING #4: The Compliance Division frequently hires inexperienced investigators and provides no training for its investigative staff.

RECOMMENDATION: The Compliance Division should develop and implement a formal training program for all newly hired and present undertrained personnel. This should include utilization of the Federal Law Enforcement Training Center and other established law enforcement training facilities, as well as structured on-the-job training. A training profile should be developed for each OEA/CD investigator to determine his individual training needs. OEA/CD personnel should be adequately trained in all aspects of law enforcement, including intelligence, surveillance, investigations and inspections, judicial proceedings and case handling. The Department should provide adequate funding for OEA/CD's training needs.

RESPONSE: This problem is now being dealt with on two levels. First, we are now recruiting only experienced investigative and intelligence personnel of the highest professional quality. In order to ensure that this is done, all selections for these positions must be approved by the new DAS/EE, who has in-depth experience in the investigation and prosecution of technology transfer crimes. Second, we are providing a systematic and continuing training program for all ITA special agents, covering not only conventional law enforcement skills but also the specialized investigative and intelligence skills which are vital to development of technology transfer cases. Further, recognizing that voluntary compliance and cooperation by the private sector remains the first line of defense against the loss of critical technology, Commerce special agents will be trained to work with the business community.

The question of basic (X-118) qualifications held by two specific employees in OEA was discussed between a representative of the IG's office and ITA's Office of personnel. The backgrounds of the two employees were reviewed and it was agreed that both were qualified for the grades at which they were hired.

FINDING #5: The Compliance Division lacks virtually any law enforcement equipment, although such equipment is needed to conduct investigations effectively.

RECOMMENDATION: The Department should purchase the essential investigative equipment required by the Compliance Division.

RESPONSE: The Office of Export Administration had $30,000 in its FY 1981 and 1982 budget allocations for the purchase of equipment and has spent only $10,000 through April 30, 1982. Thus, it is not clear that this is a resource problem, so much as Export Administration's lack of positive action to secure needed equipment.

Nevertheless, we agree with the conclusion that the export enforcement investigative staff is inadequately equipped. It is essential that this situation be remedied without delay.

Accordingly, the procurement of such equipment will be given increased priority, both in terms of funding and acquisition.

FINDING #6: The Compliance Division's current intelligence operations are almost exclusively reactive rather than proactive in nature. An efficient and effective intelligence operation cannot be conducted in such a manner.

RECOMMENDATION: The Commerce Department and its Compliance Division must increase its cooperation with and the flow of relevant information from the U.S. and COCOM intelligence communities, including specific information on the Soviet Bloc's Western technology import strategy and targets, exporters of controlled technologies, their diversionary routes and schemes, and third country participants in such schemes.

The Intelligence Branch should be given sufficient computer specialist and analytical staff, and full access to LARS, to enhance their in-house intelligence operations. The LARS data base should be expanded to include distribution license information and other available data which may be useful to the intelligence operation.

RESPONSE: The new Office of Export Enforcement will move aggressively to develop intelligence leads on two fronts. First, through improved staffing and training of its intelligence division, it will develop the capacity to generate intelligence information on its own initiative, as well as to use intelligence information received from other sources. Second, it will encourage its intelligence and investigative personnel to work more closely with other intelligence and law enforcement

agencies in order to promote effective intelligence lead development and utilization. OEE will continue to utilize OEA licensing officers' technical expertise in generating technical data and will work closely with OEA's pre licensing analysts. In addition, OEE and OEA will continue their efforts to make the License Accounting Retrieval System (LARS) more productive in generating intelligence data.

FINDING #7: OEA/CD intelligence operations are severely hampered by:

- o Inadequate and delayed intelligence analysis of information or leads on possible export violations.
- o A failure to adequately control, protect and centrally maintain source documentation establishing possible investigative leads.

RECOMMENDATION: Additional manpower should be assigned to the intelligence function, whether it remains as presently structured or is relocated to another unit in OEA, combined with OEA/CD investigations or given greater resource assistance from other intelligence agencies. A review should be made of the entire OEA intelligence processes to determine whether intelligence information is adequate and effectively collected, whether maximum and timely cooperation is available from all appropriate sgements of the intelligence community, and how the analysis of intelligence information and leads could be better handled and expedited to prevent, or at least detect and detain, illegal export shipments.

Automation of the intelligence gathering and internal filing and control systems is needed, but more drastic improvements also must be made to increase the effectiveness and efficiency of the intelligence operation.

Finally, a special effort must be made to eliminate the current backlog of Intelligence Branch cases. A special team of intelligence and investigative agents, perhaps including details from other agencies, should be assigned this task with clear, written instructions on how to review these cases and recommend appropriate action. We suspect that most of these leads are lost opportunities, but they contain crucial information on possible violators, illegal export items, importers and foreign government or company practices, which should be fed into the current intelligence data base.

RESPONSE: We agree with the conclusions of the Report concerning the case backlog. The DAS/EE has directed that the backlog be inventoried, analyzed and assigned priorities without delay, and this is being done. Once this phase is completed, he will decide what further resources must be applied to disposition of the backlog, and what case processing priorities must be followed.

Finally, we are committed to the complete and deliberate review of the entire intelligence collection, analysis and distribution process relating to export enforcement. Moreover, we intend to draw upon appropriate resources in the intelligence community to assist us in this endeavor. In the short time he has held his new post, the DAS/EE has already begun to establish smooth working relations with representatives of the intelligence community.

FINDING #8: OEA's license application screening, which is vital to the compliance function, is an antiquated manual process which, in practice, does little to help detect violations of export laws and regulations.

RECOMMENDATION: We understand that OEA is now planning an overall review of computer applications for various OEA functions. Priority should be given to automation of the screen process and the Compliance Division's intelligence gathering and internal control needs. Such automated systems, which can be accessed by all appropriate agencies, are needed for immediate entry of data on all current investigations, new violations, and new suspects from the intelligence community and other sources. The new automated screen process should also be able to go far beyond a simple match of names; it should help detect deceptive submissions, omissions or substitutions by applicants, or at least flag the more obvious ones for further review.

RESPONSE: We agree that the current manual screening process leaves much to be desired. OEA is now planning an overall review of computer applications for various OEA functions. Priority will be given to automation of the "screen" process, intelligence gathering, and internal control needs. Such automated systems, which can be accessed by all appropriate agencies, are needed for immediate entry of data on all current investigations, new violations, and new suspects from the intelligence community and other sources. The new automated screen process should also be able to go far beyond a simple match of names; it should help detect deceptive submissions, omissions or substitutions by applicants, or at least flag the more obvious ones for further review.

FINDING #9: Cooperation and coordination between the Compliance Division and the U.S. Customs Service are inadequate and adversely affect enforcement of export laws.

RECOMMENDATION: The Assistant Secretary for Trade Administration should make a policy commitment to and negotiate strong Customs-OEA/CD cooperation. This commitment must be communicated down through the ranks of both agencies as operating policy. Written guidelines and procedures should be developed to support improved cooperation; they should clearly spell out the jurisdiction of each agency, how and what constitutes liaison, what arrangements and resources exist for domestic and overseas support, and what are the responsibilities and obligations of each agency to a unified export enforcement effort. (Also see Finding #10.)

RESPONSE: Progress in dealing with perceived difficulties involving Section 12(c) of the Export Administration Act of 1979 has been made by the signing on June 18, 1982 by Secretary Baldrige of a blanket determination under that section permitting the Department of Justice to use certain protected information in connection with prosecution of export control violation arising from "Operation Exodus".

Both Assistant Secretary Brady and Deputy Assistant Secretary Wu are totally supportive of improved cooperation and coordination between the Office of Export Enforcement and the Customs Service. They have each met with their counterparts at Treasury as a first step in producing a comprehensive written understanding allocating responsibilities between the two agencies. We believe that this will result in a more efficient utilization of existing resources, such as the assignment of primary

responsibility for inspections at points of exit to Customs, which is already staffed, equipped and trained to take the lead in performing this function. Moreover, we anticipate these discussions will help to eliminate jurisdictional overlaps and conflicts between the two agencies and to foster a spirit of reciprocal cooperation. We expect that Customs and Commerce will, through better communication and teamwork, present a united front in this Nation's fight against illegal diversion of technology.

We concur in the conclusion of the Report that the liaison function between OEA and Customs, now performed by an outside consultant, should be fully integrated into the Office of Export Enforcement organization. It will be.

FINDING #10: OEA and Compliance Division officials are not aware of the actual level of support furnished by the U.S. Customs Service for ITA's export control compliance matters. The transfer of appropriated funds from the Compliance Division accounts could be excessive.

RECOMMENDATION: A follow-up request should be sent to the U.S. Customs Service by the Assistant Secretary for Trade Administration to obtain a record of actual services rendered by Customs in FY 1982 and under the FY 1981 interagency agreement. Such documentation is necessary to support ITA certification that the SF 1081s are correct and proper for payment.

RESPONSE: The U.S. Customs Service indicated in an April 30, 1981 letter that to track actual costs incurred against an agreement would require additional staff-hours which Customs did not have. They maintained that the reimbursable agreement was insufficient to cover the additional expense which would be incurred by Customs. However, pursuant to the recommendation of the Report, a follow-up request will be sent by ITA to Customs in order to obtain a record of actual services rendered by Customs in FY 82 and under the FY 81 interagency agreement.

The Report also recommends that the Office of Export Enforcement maintain its own cost accounting records. We do not agree. This would unnecessarily duplicate the accounting support provided ITA by the Office of the Secretary.

FINDING #11: A strict construction on a narrow interpretation of paragraph 12(c) of the Export Administration Act of 1979, by the Office of Export Administration and the General Counsel's Office has impeded the progress of criminal investigations and prosecutions.

RECOMMENDATION: The Secretary of Commerce should issue blanket authority for release of Paragraph 12(c) type information in law enforcement efforts.

RESPONSE: This finding reveals a serious misunderstanding regarding the Department's position with respect to Section 12(c) of the Export Administration Act. The Department has always shared information subject to Section 12(c) with other agencies for their use in assisting the Department in administering and enforcing the Act. However, these agencies, and the Department, are precluded from making the information public unless the Secretary of Commerce determines that the withholding of the information is contrary to the national interest. Contrary to the statement made in the Report, Section 12(c) has never delayed any criminal enforcement proceeding. Indeed, the Department is unaware of any instance in which intelligence or

law enforcement agency access to information needed for a criminal investigation and subject to Section 12(c) has been blocked by denial of such a determination Although Commerce has historically dealt with such requests on a case by case basis, Secretary Baldrige recently issued a "blanket" national interest determination authorizing the use by the Justice Department of Section 12(c) information (as well as Shipper's Export Declarations which are subject to the confidentiality provisions of the Census Act), for the purpose of criminal prosecution of Export Administration Act violations discovered through "Operation Exodus", subject to certain conditions.

It is important to note that the information subject to Section 12(c)'s confidentiality provisions includes confidential business information which is submitted to the United States Government only in order to receive an export license. Accordingly, great care must be taken by the Department to ensure that the confidentiality of such information not be compromised.

FINDING #12: The Deputy Assistant Secretary for Export Administration and the Director of OEA have circumvented OEA/CD management and become personally and directly involved in the conduct and disposition of investigations. This has tended to:

- denigrate the established chain of command and management;
- create multiple sources of concurrent supervisory instruction to the operating staff; and
- detract from the efficent and effective operation of the Compliance Division.

RECOMMENDATION: Investigations of potentially criminal violations and national security matters should be conducted by trained OEA/CD investigators, without interference in their day-to-day fact-finding operations.

The Department should obtain qualified individuals to manage the OEA/CD, if they are not now available. This would include the employment of Theodore Wu as a new DAS for Export Enforcement to oversee intelligence and enforcement operations. However, it should also extend down to the management of all OEA/CD operating units. Efforts should be made to upgrade the quality of the existing staff and resources. These efforts should include the development and implementation of a training program, inasmuch as newly hired personnel learn on the job from investigators whose own qualifications are limited. (See Finding #4).

RESPONSE: We concur in the recommendation, but the record should show that the DAS for Export Administration and the Acting Director of OEA state they never got personally involved in the day-to-day fact finding process of the Compliance Division or in the details of investigations. As a prerogative of management, however, they did inquire as to what Compliance Division personnel were doing with their time, to get an idea of the Division's effectiveness. It should be noted that in those cases in which they were involved, the Deputy Assistant Secretary for Export Administration and Acting Director of OEA (who was involved in only one case) did so solely for the purpose of enlisting the cooperation of concerned foreign governments in paving the way for Compliance Division and investigators. Their respective conduct in these cases was entirely proper and consistent with the practice of other law enforcement agencies, whose senior officials often take initiatives to enlist the cooperation of their senior foreign government counterparts in paving the way for U.S. agency investigators.

FINDING #13: The Deputy Assistant Secretary for Export Administration has weakened the Compliance Division by shifting part of its functions and responsibilities to a consultant and task force which operate outside of the Division. The DAS has misused this expert consultant whom he hired ostensibly to evaluate and upgrade the compliance function. Personnel regulations have been violated, as well as sound management practices, by interjecting this consultant in an operative role for which he has little expertise.

RECOMMENDATION: The consultant's task force should be disbanded; the work initiated by the task force should be continued by the Compliance Division as follows:

— The liaison function with the U.S. Customs Service should be continued and enhanced by the Intelligence Branch;

— The expanded use of the LARS data base for intelligence gathering operations sould continue to be pursued by the Intelligence Branch with OEA's computer experts.

To the extent that the Compliance Division and the DAS believe that there is a need to continue the services of this or another expert/consultant, the latter should report to the Director of the Compliance Division. Certain aspects of the consultant's efforts have significant merit, but appear far outside the scope of his position description as currently written. A written agreement should be prepared to specify his mission and work products.

Both the DAS and OEA/CD should adhere to all appropriate personnel regulations concerning the hiring and use of experts/consultants. Special care must be taken to avoid assigning consultants to operational duties which would normally be handled by civil servants. Rules regarding extension of term appointments and financial compensation should be followed.

RESPONSE: The comments regarding the consultant doing work not comprehended in his position description are correct. His position was accurately designated as non-critical sensitive. Although he later requested a Top Secret and Special Access clearance, it has not been granted. Accordingly, as the Report says, he should not have access to such information. ITA has taken steps to have the consultant conform to the terms of his employment and appropriate security regulations.

FINDING #14: The Compliance Division does not have an effective management information system or automated administrative process, including case control and time reporting systems and information storage. The current manual processes waste staff time, lend themselves to human errors, and do not provide management with sufficient information to effectively and efficiently carry out the compliance function.

RECOMMENDATION: An analysis of computer applications within the Compliance Division should be performed. This can be done in conjunction with the requirements analysis being arranged by the OEA Operations Division. Wherever the benefits outweigh the costs, management information and administrative processes should be automated. Strong consideration should also be given to the creation of a dedicated, secured system for the licensing and compliance operations, due to the national security issues involved and the use of sensitive and classified information.

RESPONSE: The Report accurately describes the need for improved management information systems and automated administrative processes. (See response to Finding #8.)

FINDING #15: Operational policies and procedures of the Compliance Division were found to be nonexistent or outdated and not widely disseminated to staff members.

RECOMMENDATION: OEA/CD operating procedures and manuals hould be updated and readily available to staff. If classified information must be included in the agent's manual, it should be restricted to a separate appendix to permit free and ready

access by agents to the manual's basic operating procedures and information. Considering the present lack of training provided new investigators, an agent's manual is an absolute necessity.

RESPONSE: One of the highest priorities of the new DAS/EE will be the development of standardized and rationalized operating procedures. These will be incorporated by the staff of the DAS/EE into a new OEE manual, as well as into a comprehensive, up-to-date manual for special agents.

FINDING #16: The Compliance Division has maintained inaccurate accounting records of its travel costs. Its reports to the Office of Export Administration in Fiscal Year 1982 significantly understated actual monthly travel costs.

RECOMMENDATION: The Compliance Division should reconstruct its travel costs for FY 1982 and provide the Office of Export Administration with corrected financial reports. An accurate internal financial accounting system should be established and maintained by OEA/CD to ensure proper and effective use of all available OEA/CD funds.

RESPONSE: While it is not clear in this finding exactly what categories of travel the Compliance Division was asked to report on, the problem could have been one of interpretation, timing, or part of the overall problem ITA is having in obtaining accurate accounting data from the Department's accounting system. It is not the Department's, policy to have the program units keep their own accounting systems.

FINDING #17: The assigned working space of the Compliance Division is inadequate and has an adverse effect on the ability of the Division to perform its mission.

RECOMMENDATION: The Department should provide adequate and secure working and file space for the Compliance Division.

RESPONSE: We concur in this finding and expect that the Department will move expeditiously to adopt the recommendations of the Report on this matter.