DEPARTMENT OF DEFENSE

DTIC FILE COPY

THE TECHNOLOGY SECURITY PROGRAM

AD-A194 106

CASPAR W. WEINBERGER
SECRETARY OF DEFENSE

A REPORT TO THE 99TH CONGRESS

SECOND SESSION

DTIC
ELECTE
APR 27 1988
S D
E

1986

This document has been approved for public release and sale; its distribution is unlimited.

88 4 26 083

THE SECRETARY OF DEFENSE

WASHINGTON, THE DISTRICT OF COLUMBIA

PREFACE

We have set our course on technology security and, after five years, we have enough experience to know that it is the right course. If we continue the effort our nation will be measurably stronger and safer.

Technology security unites Republicans and Democrats, Congress and the Administration. In the Export Administration Act (EAA) of 1979 and the EAA Amendments of 1985, Congress has recognized that technology security is an essential part of national security. Congress has directed the Executive Branch to take all necessary steps to ensure that security while encouraging legitimate exports.

(Coordinating Committee on Export Controls)

The report that follows shows that the Reagan Administration is fulfilling your mandate with vigor and tenacity. Within the Department of Defense, the military services are working with the Defense Technology Security Administration and other offices to develop and implement effective and practical controls on advanced technologies. DoD has proposed and has collaborated with the Department of Commerce to establish a certified end-users system for granting export licenses that will ease greatly the burden of exporting to reliable foreign firms. DoD has made technology security a central element in agreements with our allies on the President's Strategic Defense Initiative and on other cooperative programs in military technology. The United States, the other NATO nations and Japan continue to revise the COCOM control list and to negotiate with non-COCOM countries for the protection of Western technology. One measure of our success is that COCOM has not licensed a single new turnkey factory for the production of sensitive goods to the Soviet Union in the past five years.

In the next five years, our efforts in technology security will be primarily consolidation and further institutional development. In the coming half decade we must reinforce a proven program, making it even more effective and efficient.

Here at home we must complete the automation of the export control system. DoD has used automation to reduce greatly the time for reviewing applications for export licenses. I believe that our system can be a model for other departments. As the government reduces the time to process export cases, it reduces costs to U.S. exporters and increases their chance to compete successfully with foreign firms, whose governments often issue licenses very rapidly. It is no surprise that many COCOM countries and friendly governments protecting their own technology have been interested in the automation advances we have made.

This document has been approved for public release and sale; its distribution is unlimited.

A

We must continue to encourage our allies and friends to strengthen their programs of technology security. Many of them must give greater political importance to export controls, set tougher penalties for violators, and tighten export enforcement procedures. The United States must work with COCOM and with other governments to gain information on how the Soviets are trying to acquire our technology and to plan joint strategies to stop them.

We also must refuse to compromise our technology security for ephemeral and illusory political gains. To do so would be to repeat the mistakes of the 1970s, when the United States unwittingly sacrificed true security to the hope for security.

Holding firm to our present course will make us a more secure nation in the 1990s. America's natural advantage over the Soviet Union is our dynamic technology. If we can keep our lead in technologies with military applications, we can disrupt the Soviet drive for military superiority. This will force the USSR to adopt a more restrained and responsible role in world affairs. Sustaining a maturing and effective technology security program can help bring about this result.

Our Report outlines in depth the DoD Technology Security Program headed by the Defense Technology Security Administration.

Accession For
NTIS GRA&I ☒
DTIC TAB ☐
Unannounced ☐
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1

QUALITY INSPECTED 4

FOREWORD

The Gramm-Rudman-Hollings legislation showed that the Ninety-ninth Congress supports the Reagan administration's view that government must make tough, cost-conscious decisions before it spends the taxpaper's money.

I am confident that the Defense Technology Security Program remains one of the most cost-effective programs in government.

I use the term "cost-effective" in two ways. I am convinced that this program saves money for the taxpayer because it lowers the level of future defense budgets. It also saves money for American exporters because it increases their chance to compete successfully in the world marketplace.

Over the past year the Department of Defense has taken major steps to increase the efficiency and effectiveness of the technology security program. The new Defense Technology Security Administration has eliminated previous redundancies, improved day-to-day coordination, and ensured that both technical and policy considerations are introduced into export control cases at the outset. The DTSA has undertaken an ambitious program of automation that is speeding up the completion of routine administrative tasks and opening new possibilities for government-wide cooperation. Throughout, we are sharpening our focus on protecting those technologies which give our country the greatest advantages over its adversaries and our citizens the greatest return on their defense dollar.

These savings for the taxpaper help make possible savings by the exporter. American firms know that they can compete successfully with foreign firms if the rules are the same for both. That is why the Reagan administration is campaigning aggressively to reduce trade barriers abroad and to obtain closer cooperation on export controls matters among the COCOM nations. In the United States, the Department of Defense has reduced substantially the time it takes to review export license cases. The average time has now been cut to about 15 days for both dual-use (CCL) and munitions cases. That will cut administrative costs for U.S. firms. It also will greatly increase their chance to outsell firms from foreign countries, where export licenses often are granted very quickly.

I urge you to read this report carefully and to propose improvements to me or to Deputy Under Secretary Steve Bryen. Working together, Congress and the Executive Branch can further develop a model public program that contributes to national security, American economic competitiveness and efficient government.

Fred C. Ikle

Fred C. Ikle

EXECUTIVE SUMMARY

Now that the Department of Defense has established the Defense Technology Security Administration as its focal point for technology security efforts, we are able to move into a new management phase, concentrating on our objectives of efficiency, predictability, and transparency. These objectives are aimed at one overall goal: protection of our national security by limiting Soviet acquisition of militarily significant technology.

DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," institutionalized, for the first time, technology security responsibilities within DoD. The Directive establishes working relationships among the Offices of the Under Secretary for Policy, the Under Secretary for Research and Engineering, the Organization of the Joint Chiefs of Staff, the Military Services, and the Defense agencies. DoD Directive 5105.51 further refined this process by establishing the Defense Technology Security Administration (DTSA). The unification of the Office of the Secretary of Defense's export control effort under DTSA has enabled DoD to develop a more coherent technology security program based on national security considerations and more efficient, predictable, and transparent procedures for reviewing export licenses.

Evidence of the need for a strong well-implemented technology security program is clear from reading the 1985 report, "Soviet Acquisition of Militarily Significant Western Technology - An Update." According to the Soviets' own assessment, contained in that report, over 5000 of their military research projects benefit each year from technical documents and hardware obtained from the West. Their goals are to raise the technical level of their military systems and supporting manufacturing processes, and to acquire dual-use manufacturing and test equipment for direct use in their production lines.

There are significant cost savings to the taxpayer associated with the DoD Technology Security Program. Had our controls been less effective in the last few years and a number of significant technologies been acquired by the Soviets, U.S. and Allied defense expenditures would have had to have been increased by $5 billion to $13.2 billion. In addition, we would have suffered a considerable degredation in the NATO/Warsaw Pact military balance.

Soviet Bloc countries have stepped up illegal attempts to divert strategic commodities denied them through the licensing process. Such attempts leave little doubt as to what the Soviet Bloc is targeting for military use. To obtain these commodities, they have established an elaborate array of front companies, principally in COCOM countries, with routings through transit zones of neutral nations. We are taking steps, with the enforcement agencies, to spot these diversion attemps and stop them. In addition, specially

trained Navy and Air Force reserve units are working in DTSA to help spot potential diversion attempts through intelligence analysis.

The Soviet Union and its allies are engaged also in a sophisticated disinformation campaign designed to influence governments that are strengthening existing, or building new, technology security programs.

Various innovative programs are underway in the U.S. Government to protect sensitive technologies. For example, DoD has successfully integrated technology security with technology cooperation objectives at the outset of a major program--the Allied Strategic Defense Initiative (SDI). U.S. negotiators have succeeded in not only furthering Allied participation in SDI research, but also in ensuring that the critical technologies being researched can be protected from Soviet acquisition efforts.

The export licensing process at DoD continues to be guided by the desire to reduce the potential for competitive disadvantage to US industry while safeguarding national security under existing regulations. Through automation and streamlining of procedures, we have consistently reduced the length of time it takes to process an export license to an average of 20 days for all munitions and for West-to-East dual-use applications. West-to-West dual-use application reviews are completed in a matter of days. DoD is a pioneer in extensive use of automation in export licensing and has plans underway to make even better use of this valuable tool.

For example, to further assist export license review officials, DoD is developing an export case precedent decision-aid system based on an export case history/policy database. The database will contain policy guidance enabling identification of key current export control policy considerations relevant to applications in process. New rules can be integrated into the system, new policy direction can be quickly disseminated to system users, policy guidance and licensing criteria can be kept current, and the historical licensing information in the database will ensure consistent treatment of like exports to the same destination.

Another means of increasing the predictability of export licensing is the SOCRATES foreign availability assessment system currently under development. The system is designed to track the technological capability of all technologically significant countries in terms of years-ahead or years-behind the U.S.

Of immediate benefit to exporters is the remote electronic bulletin board known as ELISA (Export License Status Advisor). ELISA allows exporters to check on the status of their applications on a 24-hour basis. ELISA is updated automatically each day and

can be accessed from anywhere in the world by any other computer and a modem. ELISA is also used to transmit a variety of both general export control information to all users and messages accessible only to specific users.

As a part of DoD's goal of complete transparency in export control operations, DTSA and its operations are open to the exporting community and other interested parties.

DTSA recognized early on that one of the most important steps in slowing the Western technological subsidy of the Soviet military is to increase both government and private sector awareness of the problem. Many briefings have been presented to industry, government officials (U.S. and foreign), and the general public, covering the following: national security importance of the West's technological lead; Soviet threat to the Western technological lead; U.S. Government program to counter the threat; and the need for industrial/public commitment to a technology security effort.

There are a number of major goals that are being pursued in the COCOM list review. Efforts are under way to maintain the vigor of the process by means of technically sound and thorough evaluation of other members' proposals. Where they have merit, and where changes can be made in controls that accommodate other members' concerns at no loss to our national security, the U.S. has tended to accept them or modify them enough to be accepted. Efforts are also underway to strengthen the existing controls on items such as superconducting materials and metals, computer software, super-precision measuring equipment, photosensitive devices, acoustic wave devices, electronic materials, lasers, recording equipment, power sources and microwave components. We have an additional goal of securing control of other sensitive technology, such as coating processes, substrates and coating materials of a strategic nature by introducing new list items.

Efforts to modernize COCOM operations have resulted in an enhanced and formally organized Secretariat staff including newly authorized positions for database management, translation and security. DoD has provided funds for COCOM to purchase a special computer room, a new computer system with terminals, two large memory storage disk drives, and customized software.

The U.S. Government's evolving policy toward the People's Republic of China has resulted in DoD participating in the negotiation of a China Control List in COCOM. This agreement places China in an extremely favorable position, compared with the Warsaw Pact countries, for receiving high technology exports from the West and Japan. These exports will be subjected to national licensing with only statistical reporting to COCOM. Chinese importers are required to provide Western exporters with a written import certificate verifying that the government of China has authorized the import. This is to ensure that the goods are not diverted.

DoD has an integral role in the administration of Section 5, National Security Controls and related sections of the Export Administration Act of 1979, as amended (in 1985). Amendments supported by DoD include provisions strengthening enforcement, increasing penalties for violations, upgrading COCOM operations and streamlining the licensing process.

Congress reaffirmed the need for, and the role of, the Militarily Critical Technologies List (MCTL) in amendments to the Export Administration Act. Each item must be reviewed in term of foreign availability; control of technology is to be accompanied by a reduction in control of product; a new list of keystone equipment is to be developed; and an assessment is to be made of the impact of listing items on the MCTL. Steps are being taken to assist with implementation of the MCTL into the Commodity Control List (CCL) and the Munitions List, as required by law.

The need for a U.S. Technology Security Program will continue as long as the Soviet Union is intent on continuing its military build-up, based largely on the infusion of Western technology. We are proud of the steps we have taken in the past year and are confident that our plans for the future will bring us even closer to our goal of safeguarding our national security by controlling the transfer of militarily critical technology to the Soviet Bloc.

TABLE OF CONTENTS

Preface.....i
Foreword.....iii
Executive Summary.....iv

I. INTRODUCTION - THE DEPARTMENT OF DEFENSE'S GOALS.....1
IN TECHNOLOGY SECURITY

- National Security
- Efficiency
- Predictability
- Transparency

II. INSTITUTIONALIZATION OF TECHNOLOGY SECURITY AT THE DEPARTMENT OF DEFENSE - THE DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

A. History
- Implementation of DOD Directive 2040.2.....2
B. DOD Directive 5105.51
1. Implementation.....2
2. Responsibilities of DOD Components.....3
C. Organization of DTSA.....4

III. NATIONAL SECURITY

A. The Cost of Technology Transfer
1. Soviet Assessment of the Effect of Their Program to Acquire US and Western Technology..7
2. US Assessment of the Effect of US Programs to Limit the Soviet Acquisition Effort.....10
B. Export License Review Protects National Security -- Case Studies.....17
C. Soviet Disinformation Campaign.....19
D. Role of the Intelligence Community in Technology Security.....23
E. Innovative Security Programs to Protect Unclassified Technologies.....25
F. Strategic Defense Initiative.....26
G. Space.....27

IV. EFFICIENCY - SERVING THE EXPORTER

A. Case Processing: Legal Deadlines and Actual Processing Times at DOD
1. Munitions.....28
2. Dual-Use
a. West-to-East Applications.....28
b. West-to-West Applications.....29
c. Foreign COCOM Cases.....31

B. How An Export License Application Flows Through the Department of Defense
1. Munitions....31
2. Dual-Use
a. West-to-East Applications....34
b. West-to-West Applications....34
c. Foreign COCOM Cases....35
d. Operating Committee....37
3. International Technology Transfer Panel....38
C. Automation....38
1. Foreign Disclosure and Technical Information System (FORDTIS)....39
2. West-West Case Review....40
3. Secure Data Base....41
4. Automated Impact Assessment....41
D. Reserve Units....46

V. PREDICTABILITY

A. Case Precedent System....48
B. Foreign Availability Assessment....48

VI. TRANSPARENCY

A. Status Checks - ELISA....52
B. Open Door Policy....54

VII. WORKING WITH INDUSTRY

A. Awareness....55
B. Publications Available....60

VIII. INTERNATIONAL EFFORTS IN TECHNOLOGY SECURITY

A. COCOM
1. The Ongoing List Review
a. Goals....61
b. How it Works....61
c. Recent Agreements....62
2. Evolving Policy Toward the People's Republic of China....64
3. DOD Representation at COCOM....65
4. COCOM Modernization Efforts
a. The COCOM Secretariat....65
b. Automation Efforts....65
5. COCOM and Non-COCOM Countries....66
B. Bilateral Technology Security Agreements
1. India....66
2. US/Canada Agreement on Protection of Strategic Technical Data....67

IX. MODERNIZING THE EXPORT CONTROL PROCESS.....68

X. OTHER ISSUES

A. The 1985 Amendments to the Export Administration Act of 1979.....72
B. Munitions.....74
C. Emerging Technologies Program.....75
D. Militarily Critical Technologies List (MCTL).....75
E. Foreign Capability Assessment Study.....76
F. Soviet Technology and Research Capabilities.....76

XI. TECHNOLOGY SECURITY AND THE ARMED SERVICES
A. Army.....77
B. Navy.....80
C. Air Force.....81

XII. RESOURCE REQUIREMENTS.....84

XIII. APPENDIX.....85

A. DOD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions"

B. DOD Directive 5105.51, "Defense Technology Security Administration"

I. THE DEPARTMENT OF DEFENSE'S GOALS IN TECHNOLOGY SECURITY

The Department of Defense is moving into a new phase in its efforts to control the transfer of militarily significant technology to the Soviet Bloc. having consolidated our export control and related functions in the Defense Technology Security Administration (DTSA), we are now able to pursue management objectives that will further improve implementation of United States technology security policy.

Each of our management objectives of efficiency, predictability and transparency is designed to ensure that DTSA's role in technology security will enhance our national security. Efficiency and predictability in export licensing strengthens the export competitiveness of U.S. industry which, in turn, contributes to a healthy defense industrial base. An efficient and predictable system that is open and transparent in its operations will build confidence and provide the base of support and cooperation necessary for controls to work.

The objectives we have established for DTSA are directed toward one overall goal: to protect the national security by limiting Soviet acquisition of militarily significant technology. In 1985 we found that the Soviets focused their acquisition efforts particularly on automated production and control technology, computers, deep underwater equipments, telecommunications, and sensor technologies. Significantly, the Soviets are relying more and more on illegal means of technology acquisition. The success of our COCOM program has forced the Warsaw Pact to use more difficult and more costly illegal methods.

The need for a U.S. Technology Security Program will continue as long as the Soviets are intent on continuing their military build-up. For a variety of reasons, they are dependent upon the infusion of Western technology to meet their goals. We are proud of the steps we have taken to enhance the credibility of the export control program.

Dr. Stephen D. Bryen

II. INSTITUTIONALIZATION OF TECHNOLOGY SECURITY AT THE DEPARTMENT OF DEFENSE

THE DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

A. History - Implementation of DoD Directive 2040.2

On January 17, 1984, Secretary Weinberger signed DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," institutionalizing technology security responsibilities within DoD for the first time. Directive 2040.2 established working relationships between the Office of the Under Secretary for Policy, the Office of the Under Secretary for Research and Engineering, the Organization of the Joint Chiefs of Staff, the military services, and the Defense agencies. The relationships set out in this directive continue to serve as a framework under which the initiatives and continuing actions described in this report take place.

B. DoD Directive 5105.51

1. Implementation

The most notable initiative within this framework was the May 10, 1985, establishment of the Defense Technology Security Administration (DTSA) under DoD Directive 5105.51. With the establishment of DTSA, the Office of the Secretary of Defense's (OSD) various export control and related technology security functions were pulled together for the first time under one chain of command. The Deputy Under Secretary of Defense for Trade Security Policy (DUSD/TSP) serves as the Director of DTSA and reports directly to the Under Secretary of Defense for Policy. The Deputy Director of DTSA is provided by the Under Secretary of Defense for Research and Engineering. The unification of OSD's export control effort under DTSA has enabled DoD to develop a more coherent technology security program based on national security considerations and more efficient, predictable, and transparent procedures for reviewing export licenses.

DTSA's mission, as outlined in Directive 5105.51, is to administer the DoD Technology Security Program. DTSA is therefore the focal point of DoD's effort to ensure that international transfers of defense-related technology, goods, services, and munitions are consistent with U.S. foreign policy and national security objectives. DTSA is responsible for ensuring that DoD technology security policies are implemented. In addition, DTSA coordinates the efficient rapid processing of export license applications which have been submitted to DoD for review.

2. Responsibilities of DoD Components

Although DTSA is the focal point of DoD's Technology Security Program, other DoD components also play a role in accordance with DoD Directives 2040.2 and 5105.51. The Office of the Under Secretary of Defense for Research and Engineering (OUSDRE) is directed to provide advice on the technical aspects of technology security. In addition to furnishing the Deputy Director of DTSA, OUSDRE is responsible for developing the Militarily Critical Technologies List (MCTL); overseeing implementation of DoD technology transfer policy for all research, development, and acquisitional matters; and providing and coordinating technical support for DoD's participation in COCOM. This latter responsibility includes management of DoD's support to the interagency Technical Task Groups (TTGs), which develop technical proposals for COCOM controls. (This process is explained in further detail elsewhere in this report.) OUSDRE also plays an important role in the International Technology Transfer (IT^2) Panel, which is discussed below.

The military departments support DTSA with technical, acquisitional, intelligence, and operational information. Each service designates a liaison officer from its staff to DTSA on a full-time basis to assist in coordinating service inputs. The military departments also provide DTSA with recommendations on proposed export licenses.

Directive 5105.51 also directs the Assistant Secretary of Defense for International Security Policy (ASD/ISP) to play a role in technology security functions as well. The ASD/ISP represents DoD in technology security matters before several interagency committees including: the Advisory Committee on Export Policy (ACEP), the Economic Defense Advisory Committee (EDAC), which administers COCOM cases, and the Committee on Foreign Investment in the United States (CFIUS), which monitors the impact and significance of foreign ownership of U.S.-based companies. The ASD/ISP also continues to serve as chairman of the IT^2 Panel, which resolves differences within DoD concerning technology transfer policy implementation.

The Office of the Joint Chiefs of Staff (OJCS) continues to provide support in accordance with DoD Directive 2040.2. This support includes conducting operational and military mission impact assessments on technology, goods, services, and munitions transfer issues, as requested.

Finally, DTSA is supported by the Defense Intelligence Agency (DIA). DIA provides this support in accordance with DoD Directives 2040.2 and 5105.51. Under 2040.2, DIA is directed to: a) provide assessments of the types and numbers of illegal transfers of technology, goods, services, and munitions, and the associated transfer mechanisms, b) assess foreign availability, c) conduct end-user checks, and intelligence reviews of export applications, d) provide intelligence concerning the total effect of transfers of technology, goods, services, and munitions on U.S. security, e) assess the

reliability of recipient nations to protect technology, goods, services and munitions that originate in the U.S., f) assist in identifying technologies critical to potential adversaries, and g) support export control and enforcement agencies.

C. Organization of DTSA

DTSA is divided into directorates as follows (see Figure 1):

The Strategic Trade Directorate coordinates overall DTSA policy for dual-use technologies (technologies that have both civilian and military applications) and works closely with the Department of Commerce, which is the administering agency for the Export Administration Act. This directorate has the primary responsibility for DoD participation in COCOM (the Coordinating Committee for Multilateral Export Controls). Its policy and technical experts, including engineers, review and process over 25,000 export license applications for strategic commodities and technologies referred by the Department of Commerce each year and all export requests referred to us by our allies through COCOM. In addition, the directorate's technical experts represent DTSA on the MCTL Technical Working Groups, the COCOM Technical Task Groups preparing new COCOM proposals, and the Department of Commerce's Technical Advisory Committees. The directorate works closely with U.S. industry to develop technical policy guidelines.

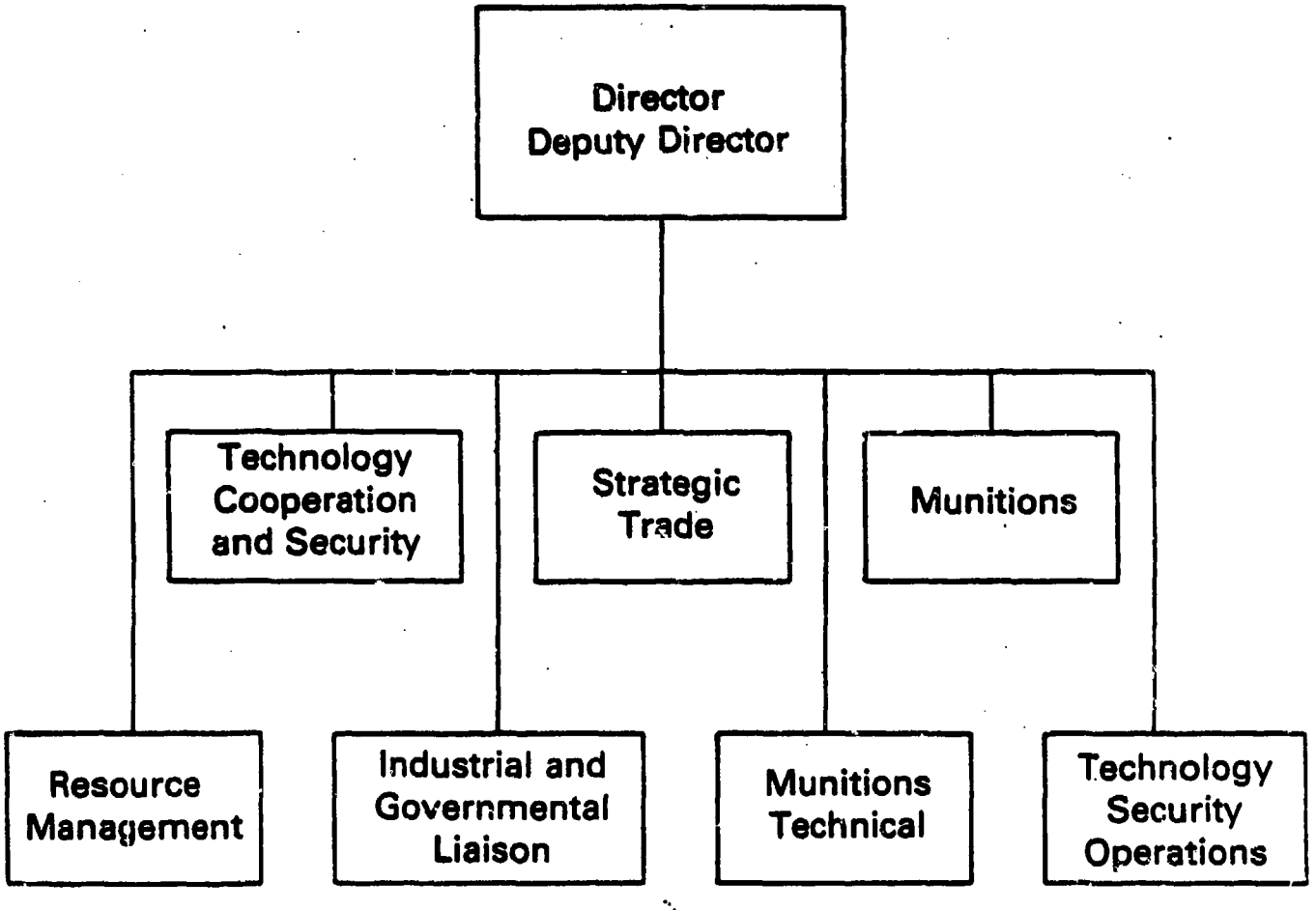
The Munitions Directorate, in coordination with the military departments and other DoD agencies, formulates the DoD final position on approximately 9,000 munitions export license requests referred to DTSA annually by the Department of State, which has primary responsibility for administering the Arms Export Control Act. The directorate reviews U.S. policy on arms exports and engages in interagency and foreign government policy discussions in this regard.

The Munitions Technical Directorate, in coordination with the Office of the Under Secretary of Defense for Research and Engineering, the Office of the Assistant Secretary for Command, Control, Communications and Intelligence, and the military departments, provides technical assessments and recommends technical positions on those munitions cases reviewed by DoD and provides this technical position to the Munitions Directorate. The Directorate also develops technical policy for the Munitions Directorate.

The Technology Security Operations Directorate (TSO) monitors diversions and works to halt them with the intelligence community and the enforcement agencies with jurisdiction over illegal exports. This directorate ensures that information about diversions is passed to the enforcement agencies in a timely manner and that policy issues arising from diversion attempts reach DoD policymakers for rapid action. In 1985 TSO assisted in halting more than 20 major diversions and identified more than 12 major

FIGURE 1

DEFENSE TECHNOLOGY SECURITY ADMINISTRATION



policy issues arising from the diversions. Diversions also provide important information about what technologies the Soviet Bloc is targeting for acquisition.

The Resource Management Directorate provides, in addition to general administrative support, expertise in the computer support systems upon which DTSA relies, increasingly, for efficient case review.

The Industrial and Governmental Liaison Directorate is responsible for keeping U.S. industry, government agencies, the Congress, the general public, and foreign governments informed about the Department of Defense's Technology Security Program. Its staff develops and carries out various programs to raise technology security awareness. Companies needing information, briefings or assistance on licensing matters may look to this directorate.

The Technology Cooperation and Security Directorate develops and coordinates Department of Defense policy and agency positions on the relationship between technology cooperation and technology security to include negotiations with allied and neutral countries.

III. NATIONAL SECURITY

A. The Cost of Technology Transfer

1. Soviet Assessment of the Effect of Their Program to Acquire U.S. and Western Technology

On September 18, 1985, Secretary Weinberger made public a report entitled "Soviet Acquisition of Militarily Significant Western Technology--An Update." The report, a product of a government-wide effort involving 22 agencies, contains previously classified information on the Soviet technology acquisition effort. According to the Soviets' own assessment, over 5,000 Soviet military research projects each year benefit from technical documents and hardware obtained from the West. The Soviets budget approximately 500 million rubles (or $1.4 billion in equivalent 1980 U.S. purchase power) each year for the legal and illegal purchase of these documents and hardware.

The Soviets have two basic goals in this acquisition effort. First, they seek to raise the technical level of both their military systems and manufacturing processes. Second, they hope to acquire dual-use manufacturing and test equipment for direct use in their outdated production lines.

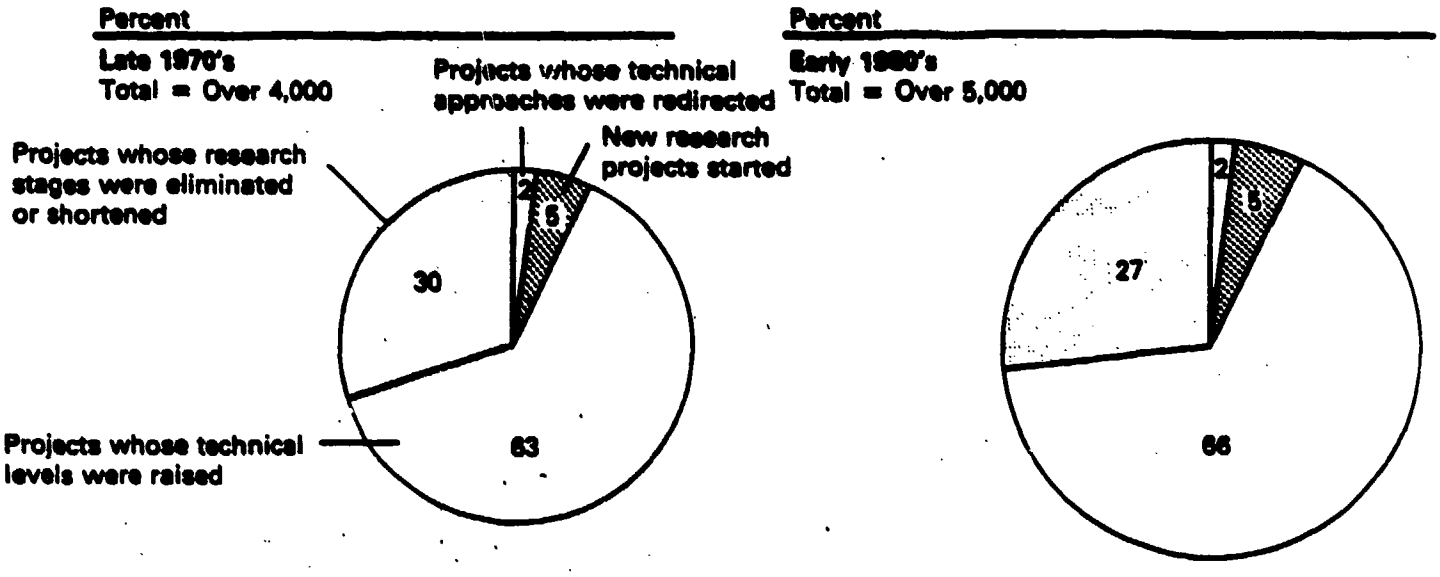
In order to acquire the desired technology, the Soviets rely upon two overlapping but separately administered acquisition systems. The first system is coordinated by the Military Industrial Commission (VPK) of the Presidium of the Council of Ministers. The VPK is the most powerful organization in the Soviet defense research establishment, coordinating the development of all Soviet weapons as well as the national program to acquire Western technology. The design bureaus of the key defense manufacturing industries prepare requests for Western hardware and documents which the VPK then translates into lists of collection requirements. In the VPK program, the Soviet Bloc intelligence services (the KGB), the Chief Intelligence Directorate of the Soviet General Staff (GRU), and their surrogates among the East European intelligence services are the collectors most often tasked and the most successful.

The Ministry of Foreign Trade and the Soviet intelligence services administer a second program which focuses on trade diversion in order to acquire relatively large numbers of dual-use manufacturing and test equipment for direct use in production lines. The equipment obtained through the Ministry of Foreign Trade's program will be used to increase the throughput of weapon-producing industries.

From 1976 to 1980, the Soviet Ministry of the Defense Industry and the Ministry of the Aviation Industry realized savings of 500 million rubles in research project costs due to the acquisition of Western technology. As Secretary Weinberger stated when releasing

FIGURE 2

TECHNICAL AND TIME BENEFITS TO THOUSANDS OF SOVIET MILITARY RESEARCH PROJECTS FROM WESTERN TECHNOLOGY



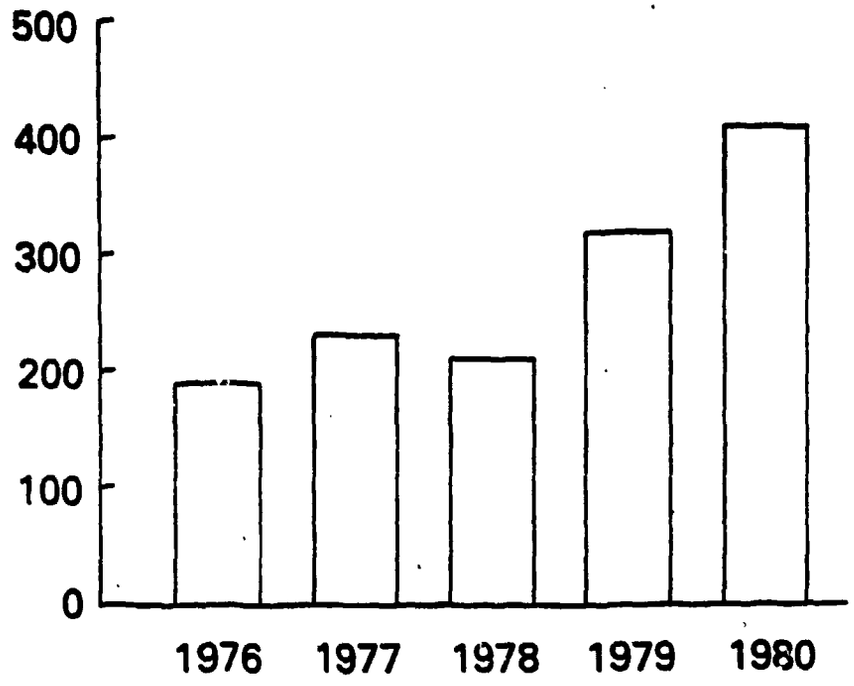
The benefits to the Soviet military research establishment from acquisitions of Western technology are far greater than previously believed. Virtually every Soviet long- and short-term research project for military systems — well over 4,000 in the late 1970's and well over 5,000 in the early 1980's — is benefiting from the documents and hardware of at least a dozen Western countries.

Projects in the VPK program are divided into the four major categories shown above. Projects with redirected technical approaches and new projects represent the most significant benefits through adoption of innovations and new directions for military systems. Major pitfalls are thus avoided. Projects whose technical levels were raised and those whose stages were eliminated or shortened represent improvements in the military state of the art of the Soviet Union and an acceleration in the time when more advanced subsystems are ready for new and future weapons.

FIGURE 5

RUBLE SAVINGS FROM ONLY A PART OF SOVIET WESTERN TECHNOLOGY ACQUISITIONS

Million Rubles
At least 1.4 billion rubles in savings on selected projects during the 10th Five-Year Plan



The above savings generally are conservative estimates by the Soviets resulting from the elimination of stages of military research and design projects, the reduction in time to carry them out, and the adoption of new technical approaches. The savings are not cumulative. That is, a 20-million-ruble annual savings from the acquisition of U.S. and other Western fiberglass plastics production technology used in manufacturing high-pressure air tanks for submarines was counted for one year only, the year of acquisition.

Roughly 400 million rubles ($640 million) were saved in 1980 for only a portion of the Western technology acquired. Most of these savings were in long-term military research projects for weapons of the late 1980's and early 1990's. They therefore were most likely given in terms of manpower savings. By this measure, several tens of thousands of Soviet man-years of scientific research effort were saved in 1980.

the September report, "This means nothing less than our subsidizing the military build-up of the Soviet Union."

More significant, perhaps, is the time savings in research and development which the Soviets are able to achieve due to the acquisition of Western technology. For example, the Soviets estimated that by using documentation acquired on the U.S. F-18 fighter, their aviation and radar industries saved five years in developing the next generation of fire-control radars for Soviet fighter aircraft. The manpower savings on this project alone translate into over 1,000 man-years of scientific research. Western documents also helped the Soviets cut by two years the time spent on researching a new generation of fuzes for munitions with a large kill radius and for self-aiming aviation cluster munitions.

The Soviets have thus been able to translate their technology acquisition into accelerated development and deployment schedules. In doing so, the Soviet Union has diminished the qualitative lead in technology which the West must maintain in order to preserve its security.

2. U.S. Assessment of the Effect of U.S. Programs to Limit the Soviet Acquisition Effort

The major goal of the Department of Defense's Technology Security Program is to inhibit Soviet access to Western technology in order to reduce the external military threat facing the United States and its allies. By doing this, our security program can significantly ease the defense cost burden which the United States must face in the future in order to maintain a military posture sufficient to protect our national interests.

This section assesses the defense cost savings associated with the DoD Technology Security Program. These cost figures represent an update of our pilot study on this subject issued a year ago (Assessing the Effect of Technology Transfer on U.S./Western Security, A Defense Perspective, Office of the Under Secretary of Defense for Policy, February 1985), and were calculated using the same techniques. The 1985 study demonstrated that it is possible to credibly quantify the costs to U.S. taxpayers of specific transfers of technology. We see continuing value both in the assessment process developed and in its results.

Our 1986 assessment indicates a continuing Soviet emphasis on acquisition of militarily critical technology which, if acquired, could have:

- Saved them additional billions of dollars in defense costs
- Significantly reduced their development times for specific military systems
- Further enhanced their defense industrial productivity, and
- Accelerated their response to new Western weapons and tactics.

Our principal findings are:

Exploitation of Western technology acquired through legal channels could have:

- o Saved the Soviet military $4.6 to $12.0 billion;
- o Cost the U.S. and its allies $5.0 to $13.2 billion;
- o Degraded the NATO/Warsaw Pact military balance, particularly in critical aspects of ASW
- o Contributed to Soviet/Pact military technology base, particularly in automated production and control, sensors, and telecommunications

The DoD Technology Security Program denies to the Soviets benefits of such technology transfer efforts and contributes to U.S. national security in three extremely important ways:

1) It reduces the technology level available to current and future Soviet weapons systems. In this way, our security efforts restrict Soviet strategic options in countering or defeating future U.S. defense initiatives.

2) It slows improvements in Soviet defense industrial productivity. Such improvements are increasingly important to the Soviets as their weapons systems become more complex.

3) It reduces the significant savings accrued to the Soviets in military research, development, and production through the infusion of critical Western technology.

This assessment of the potential impact of Soviet attempts to acquire Western technology is based on the evaluation of export requests from the Soviet Union and East European countries which were referred to DoD between April 1984 and December 1985, the period of time from the end of our 1985 pilot study to the present.

In 1985 as in previous years, the Soviet Union and its Warsaw Pact allies made major attempts to acquire militarily critical technology from the U.S. and the West. Had these attempts been successful, the resulting transfers could have caused significant damage to U.S. national security through sizable Soviet and East European military savings. These savings denied the Soviets through DoD's Technology Security Program and other government agency programs are estimated at between $4.6 and $12.0 billion. The variation in these figures comes from uncertainties we have in estimating Soviet use of Western technology since the Soviet Union is a closed society and actively seeks to deny the West this information.

Given that such Soviet defense budget savings would have been invested in new military initiatives, they would have necessitated additional U.S. defense expenditures of between an estimated $5.0 to $13.2 billion over the next ten years in order to maintain our current military posture relative to the USSR. These costs are staggering.

Significant as these savings are, they reflect the impact of only a small portion of Soviet technology acquisition efforts worldwide (i.e., through legal channels). These figures do not reflect additional Soviet efforts using illegal and clandestine channels. Also, they do not include the potentially much greater "second order" effects as savings and improved technological capabilities are distributed throughout the Soviet military-industrial complex or the unquantifiable effect of restricting future Soviet military-strategic options to those made available primarily from indigenous resources.

By closing Soviet and Warsaw Pact access to militarily critical technologies through legal channels, the U.S. Technology Security Program forces the Soviets to turn to less efficient, less reliable illegal or clandestine acquisition programs.

All cases reviewed during the time frame of our study which could have provided major defense savings to the Soviet Union or Warsaw Pact allies were denied or restricted by the DoD Technology Security Program as well as those of other U.S. Government agencies.

Soviet technology acquisition patterns using legal channels were very similar to the acquisition patterns found in our 1985 study, with 1) a continuing emphasis on acquisition of automated production and control technology, computers and telecommunications, 2) an increased emphasis on sensor technologies (especially areas relating to anti-submarine warfare capabilities), and 3) less evidence of the use of legal channels to acquire sophisticated microelectronics technology.

Several technical findings of our 1986 assessment are presented below.

Automated Production and Control (APC) Technology

In 1985, the Soviet Union officially acknowledged, as part of its strategic economic plan during the 12th five-year period (1986-1990), its goal of dramatically increasing the use of integrated systems, computer-aided-design and computer-aided-manufacturing. The Soviet and East European effort to legally acquire Western APC technology has clearly intensified over the last year. We noted, especially, repeated Soviet and Warsaw Pact requests to acquire computerized industrial program controllers, process control systems, and applications software. Such APC software was allegedly for use in several different automobile, steelmaking, machine tool, and automation research and development

facilities such as Togliatti, Volga, Ivonoskoye, the Center for Automation Technology, and others.

Perhaps because of the success of earlier technology security program efforts, we noted an increased emphasis on acquiring technology other than state of the art. This trend showed the Soviet need for less than the "top of the line" capabilities and a recognition that the U.S. Government would not release the most capable equipment. Whatever the case, it shows a continuing Soviet/Bloc emphasis on acquiring militarily critical Western APC technology.

Along with the Soviet Union, Poland, Czechoslovakia, Bulgaria, and Hungary are prominently engaged in these acquisition attempts, which is in keeping with known division of responsibilities for APC development within the Council for Mutual Economic Assistance (CEMA). It would appear that the continuation of requests from the Soviet Union for lower level APC technology may indicate that they have not yet been successful in incorporating computerized production techniques into designated areas of their industry. This would not be unusual since there seems to be substantive evidence of Soviet difficulties in assimilating previously acquired APC technology and in developing their own capability.

Because the APC technology is pervasive, Soviet defense savings from acquired Western equipment and technology can be quite large. Given their stated industrial priorities and the military significance of this technology, we believe the Soviets will continue to attempt to acquire Western APC technology.

Sensor Technology

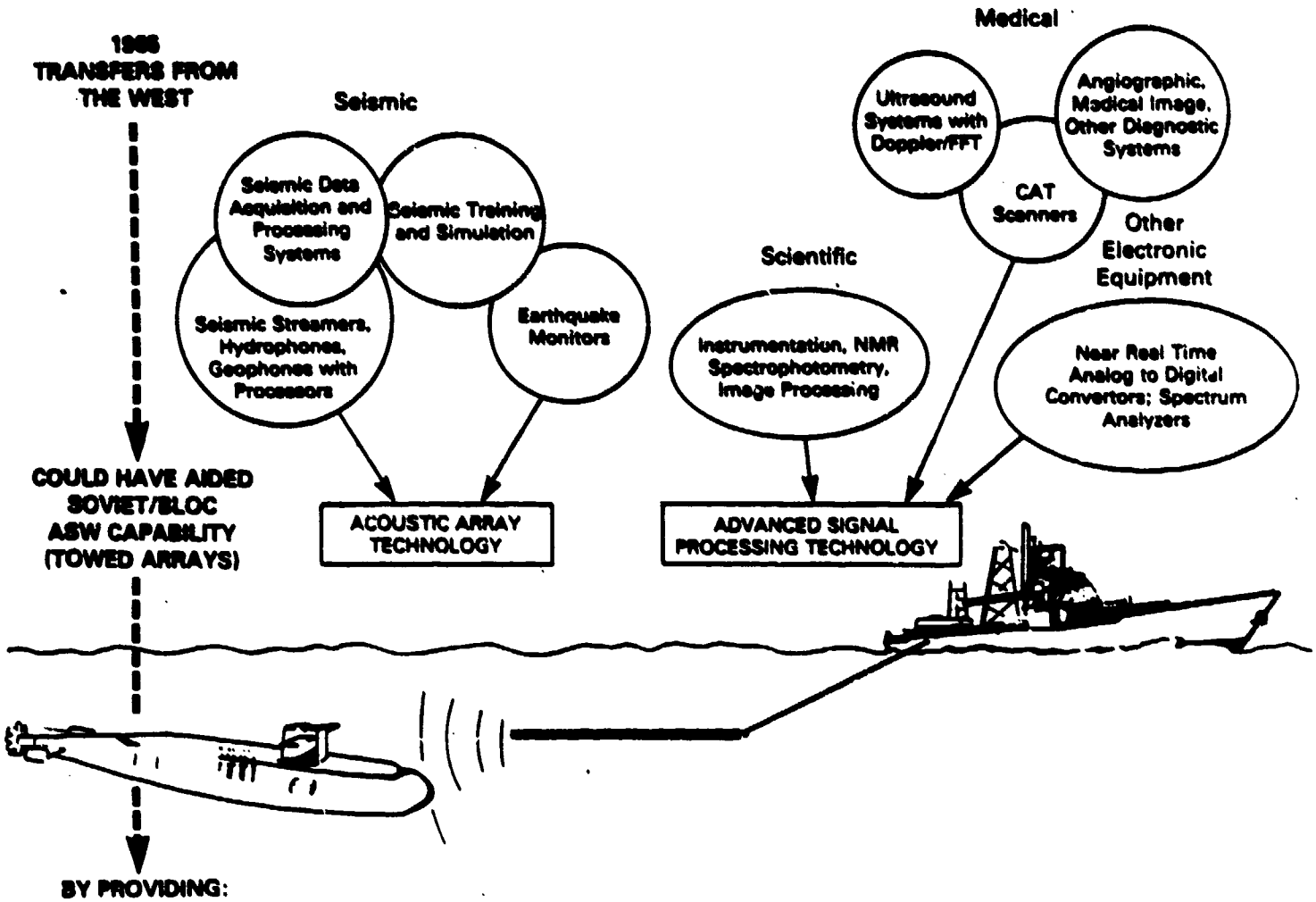
Advanced sensing and the associated digital signal processing is a second technology where there was significant activity during late 1984 and 1985. The U.S. Intelligence Community has long identified priority Soviet technology acquisition efforts in this area. Such acquisition of advanced Western know-how coupled with their indigenous technology base could provide the Soviets with the ability to launch a major challenge to the survivability and detectability of many elements of the U.S. force structure.

We see a pattern in the Soviet acquisition attempts during 1985 which appears to support their development of advanced sensors for use in anti-submarine warfare (ASW). Figure 4 portrays this pattern. Notably, we saw attempts to acquire:

- Sophisticated seismic data collection and data processing equipment
- Advanced signal and image processing systems from medical and other industries
- Advanced spectrum analyzers and analog-to-digital converters

FIGURE 4

SENSOR CLUSTER



- Design Information
- Systems Integration Know-How
- Sensor-to-Processor Interface Data
- Automatic Calibration and Adjustment
- Applications Software
- Versatile, Multiple Use Array Processors

The majority of the sensor-related cases involve embedded signal processing or array transform processors with Fast Fourier Transform capabilities, highly advanced image processing, high-speed analog-to-digital conversion capabilities, or real-time spectrum analyzers.

We believe that the Soviets and other Bloc countries would exploit the technology embedded in those systems--for system design, applications software, sensor-to-processor interfaces, automatic calibration and adjustment, and integration know-how--for use in advanced passive acoustic arrays for ASW.

These technologies, if acquired and exploited fully by military research and development efforts, could enhance substantially the Soviet ability to field an effective acoustic sensor. Such a system, once deployed, could increase the fraction of early generation Western fleet ballistic missile submarines (SSBNs) jeopardized by Soviet ASW capabilities. The cost of potential Western responses to such improved Soviet capabilities would be very high; tens of billions of dollars.

Computer Technology

Soviet and Warsaw Pact computer-related acquisition efforts in 1985 appear to have been directed at two distinct technologies: compact or personal computers and mass storage devices, particularly disk and tape drives. The large number of requests for compact or personal computers from Bloc countries indicates the level of evolution of the computer industry throughout the Bloc. It appears that Bloc nations have just entered the phase of computer use achieved some five to seven years ago in the U.S.

The other area of high interest was in mass storage devices, particularly disk and tape drives and magnetic media. Here, the Soviets appear to be attempting to improve on one of the fundamental weaknesses in their computer sector. Czechoslovakia and Bulgaria account for the majority of these requests seeking both equipment for direct end use and for manufacturing. Transfers in these areas could have provided significant cost savings to the Warsaw Pact in their attempts to produce military quality mass storage systems.

There is a notable change in the pattern of requests from the Soviet Union regarding licenses for computers other than compact or personal computers. The Soviets themselves made few requests for computer technology during 1985, with the majority of requests coming from Poland, Czechoslovakia, and Bulgaria. One way for the Soviets to mask their attempts to acquire militarily critical technology from the West is to use their East European allies as conduits since certain East European countries are treated differently, and often more favorably, than the

Soviet Union in the export licensing area. We may be seeing an expansion in the Soviets' use of other Eastern European allies to acquire computer technology through legal channels. This apparent shift in Soviet acquisition strategy may be a direct result of our technology security program.

Microelectronics Technology

As with computers, microelectronics technology remains a top priority collection requirement for the Soviet Union and its East European allies. We noted in 1985, however, a lack of major Soviet legal channel activity in this technology. This is interpreted to indicate increased use of alternate acquisition channels.

One recent Soviet microelectronics request analyzed as a part of the 1986 study was particularly revealing. This case involved the repair of some major semiconductor production equipment at one of the Soviet Union's largest military semiconductor manufacturing facilities. The Soviets requested that Western specialists come into this sensitive facility to repair broken equipment. This request probably indicates severe production difficulties at the military facility and the apparent lack of adequate domestic repair capabilities even at a major military facility. U.S. technology security efforts appear to be limiting the effectiveness of Soviet acquisition efforts of this technology, both by denying critical technology transfers and by forcing a greater reliance on illegal acquisition channels.

Telecommunications Technology

Poland, Bulgaria, Czechoslovakia, and Hungary were aggressive in their attempts to gain access to critical telecommunications products and technology during 1985. All of these countries made a major effort to upgrade their national telecommunications capabilities. Since military communications rely heavily on the use of commercial communications networks (with only special modifications for communications security and electronic counter--countermeasures), improvements in Warsaw Pact national telecommunications networks can have a direct and significant military impact.

The primary areas of requests during 1985 were in analysis and measurement equipment, which are useful both in research and development and in production of telecommunication equipment. The emphasis was on sophisticated instrumentation useful in the R&D process. Examples of such equipment include a system analyzer, impedance analyzer, waveform analyzer, and a frequency calibration standard.

A noteworthy request was for export of equipment designed to Hungarian specifications. This request covered a number of preamplifiers (74) to be manufactured in the West for use in Hungary. Approval of this request would have transferred devices using the latest state-of-the-art technology for preamplifiers

which could in turn be used for military applications. Soviet Bloc use of such specifications for the production of equipment in Western countries is seen as another way to obtain our latest technology and in a form which may, in fact, be tailored to use in their military applications.

Figure 5 summarizes the estimated Soviet defense savings associated with the cases analyzed.

The U.S./NATO defense costs associated with responding to Soviet exploitation of the cases selected for analysis in our assessment far overshadow the total value of all licenses recommended for denial by DoD during the same period. Our diligence in stopping this flow of militarily critical Western technology to the Soviets and their allies, allows us to report that none of these effects will occur.

B. Export License Review Protects National Security: Case Studies

Soviet Bloc countries have stepped up attempts to divert illegally strategic commodities denied through the licensing process. Such attempts leave little doubt of what the Soviet Bloc is targeting for military use. To obtain these commodities, they have established an elaborate array of front companies, principally in COCOM countries, with routings through transit zones of neutral nations. Items sought out for diversion include:

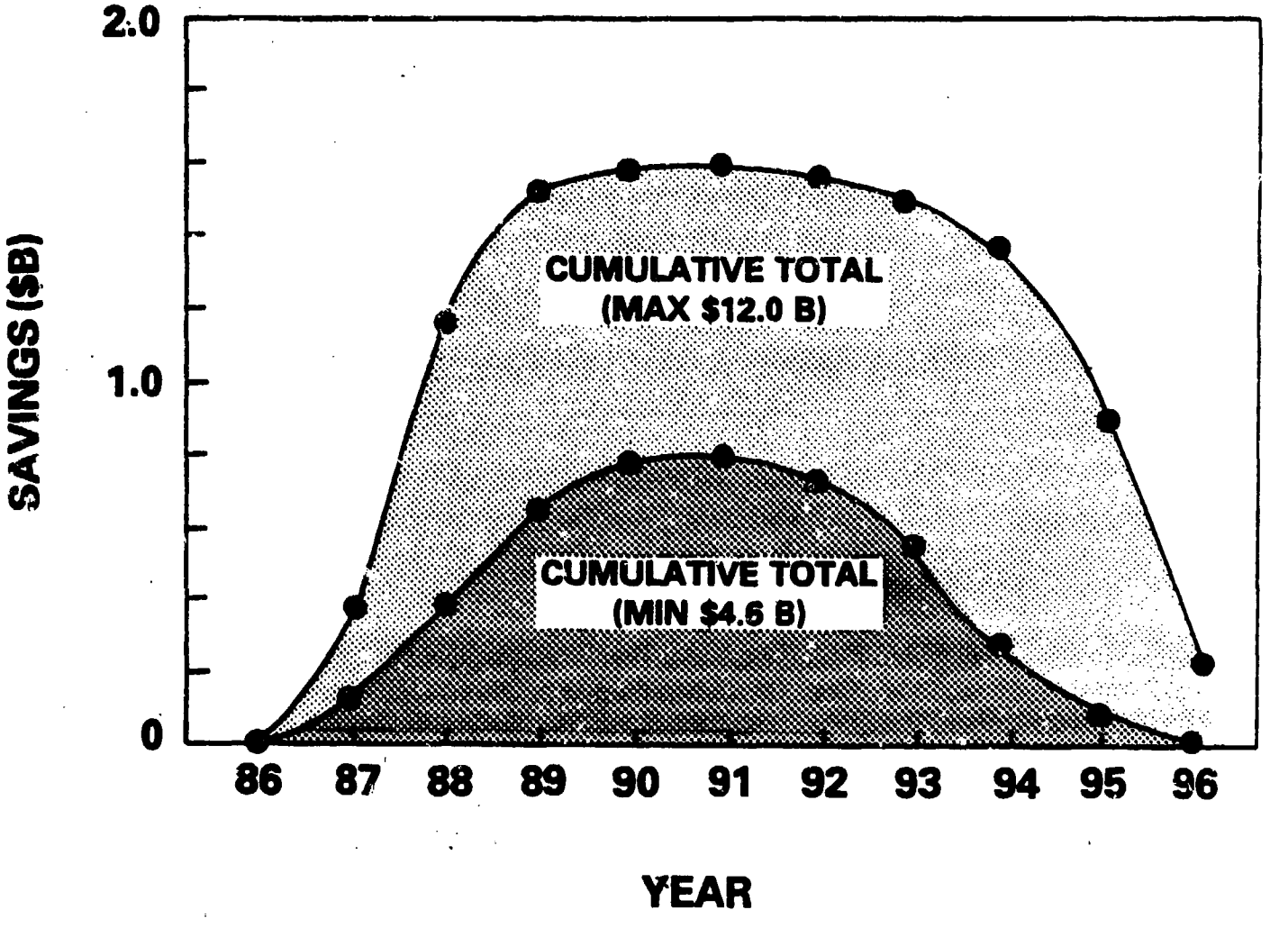
a. Computer-aided design and computer-aided manufacturing equipment
b. Hot isostatic presses for carbon-carbon and super alloy work
c. Very Large Scale Integrated Circuits manufacturing equipment
d. Disk drives
e. Electro-optics and remote sensing

From these targeted commodities, the Defense Department has had to assess the strategic consequences of these illegal acquisitions to U.S. military systems. In many cases, DoD has determined that they pose a threat to Western security. Consequently, DoD over the past year has stepped up efforts to monitor diversions and act as a catalyst and coordinate efforts to halt them. In addition, DoD has been instrumental in taking issues resulting from the diversions to policy makers at the highest government levels. Increasingly, diversion cases quickly highlight major policy issues between the United States and other governments.

Certain diversion cases this past year dramatize the increase in attempted diversions. The high level of attention given these cases reflects their importance to the various Western governments involved.

FIGURE 5

USSR MILITARY SAVINGS (1986-1996)



Carbon-Carbon Case--This case involved the attempted diversion from Great Britain of carbon-carbon manufacturing equipment. This equipment would have given a production capability to the Soviet Union to manufacture critical components for strategic missiles. The critical components would be made with durable, lightweight material able to withstand tremendous temperatures. Carbon-carbon material is a critical component of major U.S. military strategic systems. The diversion attempt drew particular attention to the lack of adequate strategic controls on this equipment among the COCOM countries. Consequently, the United States and Great Britain had to pass emergency regulations to halt the export of the equipment literally as a Soviet ship was coming into Britain to pick it up. The issue of controls and the strategic consequences of the export of the equipment was taken, respectively, to British Prime Minister Thatcher and to President Reagan.

The carbon-carbon case continues to offer major challenges to non-COCOM countries capable of producing similar equipment. It has brought about demarches to high levels of government in those countries. It also has required a complete review of COCOM controls, which proved to be deficient. Recent efforts have tightened those controls. The case also has prompted continued vigilance by U.S. Customs and the Federal Bureau of Investigation to head off any attempt to fulfill the Soviet order for this equipment. Denial of this export clearly upset a rigid Soviet timetable to install a manufacturing system and provide greater accuracy and throwweight for its strategic missiles.

Computer-Aided Design/Computer-Aided Manufacturing--Tens of millions of dollars in controlled equipment destined to a foreign embassy in a neutral country caused US officials to question a transaction. An investigation revealed that two shipments already had been allowed to be exported from a COCOM country for questionable purposes in the neutral country. The routine investigation revealed that a major diversion had been in progress over a period of time, including at least six front companies in two COCOM countries. The goods then were to be shipped through a neutral country's transit zone to the East Bloc. From the portion of the shipment that was stopped, the determination was made that the Soviet Bloc was in the process of putting together elaborate computer-aided design and computer-aided manufacturing centers. These commodities generally would be denied to the Soviet Bloc if export licenses were sought. Further investigation continues to identify other fronts which may have been used to pull off what may be the largest recorded diversion to date.

C. Soviet Disinformation Campaign

The Soviet Union and its allies are engaged in a sophisticated propaganda campaign designed to influence governments around the world that may be building new or strengthening existing technology security programs. This systematic, calculated effort is intended to weaken the U.S. by trying to divide its interests from those of

its allies, by exacerbating and maximizing differences of opinion among the allies and by ignoring or minimizing their common security interests. While intending to weaken the West on the one hand, the Soviet effort is designed also to strengthen its effort to obtain the militarily critical and advanced technology that it lacks.

The Soviet Bloc tries to accomplish these objectives through various "active measures" including the dissemination of inaccuracies or disinformation, forgeries of official documents, the development and support of foreign communist parties and international front organizations, the use of economic threats and, of course, propaganda. As the West's technology security effort has increased over the past few years, the Soviet campaign against it has intensified and spread.

Since acquiring Western technology, trade and credits is easier for the Soviets to achieve within the context of detente, one of the major foreign policy priorities of the Soviet Union now is the reawakening of the "detente spirit," particularly following the US/USSR Summit in Geneva.

The ambience the Soviets are intent on creating would foster Soviet influence, exacerbate differences within the Western alliance, and render less influential and effective those officials within the Administration who continue to pursue a prudent, realistic and long-term policy against the Soviet Union's self-proclaimed goals of world domination.

The sometimes contradictory proganda themes the Soviets continue to pursue were articulated by General Secretary Gorbachev in both his September interview with Time magazine and in his post-Geneva address to American businessmen visiting Moscow. Some of these themes are:

- The U.S. gains access to advanced technology through its imperial, cynical and exploitative use of its allies while the USSR uses its technology for benevolent and modest purposes;
- The USSR does not depend on Western technology because it is a great scientific and technological power;
- The USSR has a huge and ready market for Western business people selling Western technology;
- The US talks about the technological achievements of the USSR only when it wants to increase the defense budget, but when it wants to prohibit technology it depicts a mighty Soviet Union far advanced in its use of technology;
- Soviet economic reform will lead to a scientific and technological revolution which will leave the West in the dust;

- Removal of trade restrictions, the ban on official U.S. credits and most-favored nation trade status (all characterized by the Soviets as "discriminatory" trade restrictions) would allow the two superpowers to become natural trading partners.

Other themes consistently repeated in the East Bloc media and in public statements by East Bloc officials include:

- The liberalization of Soviet internal politics depends upon the importation of Western technology;

- COCOM is an "organization of economic terrorists," which is "an instrument of U.S."--rather than Allied--"power, and has become one of the principal factors for...subversive activity;"

- The Reagan administration is isolated from the American business community which wants to do business with the East, from the scientific community which wants to promote exchanges of scientists and information with the East, and from the Western allies who rely on trade with the East;

- The actual goal of Western export control is the complete subordination of trade and economic relations to the interests of militarization;

- The lack of consumer items in the East is a consequence of Western export controls;

- Equipment, documents and technology--which the Soviets do not need because they are so advanced--reach the East despite Western export control regulations so it would behoove the West to remove its regulations and allow its businessmen to make a decent living;

- Europe and the Soviet Union are linked through historical ties, and a common cultural foundation while America, with its inferior political culture, has not yet learned to view Europe as an equal partner.

Another constant theme involves personal attacks on Administration officials, particularly against those who are Jewish and/or who advocate a quid pro quo policy toward the Soviet Union. These people are condemned and attacked by the Soviets as "obstructionists," "warmongers," and "opponents of peace." By fabricating lies about these public figures, by alleging conspiracies among them, and by promoting anti-semitic sentiments against them, the USSR propaganda machine hopes to realize its goal of discrediting and undercutting those people who are firm in their opposition to the implementation of American policies which would further the long term goals of the Soviet Union.

FIGURE 6

WESTERN TECHNOLOGY:
THE KIND NOBODY NEEDS

An American electronic juicer:
It effectively extracts the last drop of juice from the Western allies

An Israeli steam iron:
It [op]presses occupied Lebanese villages

A German fan:
It fans ideas of revanche and 1937 borders

A sewing machine:
It tailors transparent myths about the "Soviet threat"

SOURCE: *Pravda*, March 8, 1985

The placement of misrepresentations, distortions and outright falsehoods in the non-communist Western media is critical for the success of the Soviet active measures programs for it provides a veneer of respectability and acceptability to the propaganda themes.

In furthering its propaganda campaigns, the Soviets try to use the aptly named "boomerang" principle: A news story (or a slogan or a "scientific discovery") is planted in a non-communist source. Then it is replayed in the Soviet and East European media as well as through controlled or semi-controlled front publications and organizations. This technique remains among those most favored by the Soviet disinformation specialists not only because they enjoy the irony of quoting American sources against the United States but also because the disinformation is better absorbed and therefore more effective if it is published by the Western press. Many of the articles in the Soviet media attacking the technology security program cite American press reporting, whether fringe or establishment publications.

It is expected that the Soviet active measures campaign will intensify for the foreseeable future since the acquisition of technology is of critical importance for the functioning of the Soviet military system and the Western technology security programs are increasingly effective at slowing or stopping that acquisition. While Soviet propaganda will portray Soviet technology as on par with Western technology, this claim will be belied by Soviet efforts to undermine COCOM and bilateral agreements with non-COCOM countries, to weaken domestic political support for the technology security programs in the West, and to drive a large wedge between our allies and America, and between Western scientists and businessmen and their governments.

It is increasingly obvious that the American government must, on both intra- and inter-agency levels, systematically track and devise countermeasures to Soviet propaganda and disinformation, particularly abroad.

D. Role of the Intelligence Community in Technology Security

The DoD Intelligence Community provides direct support for technology security matters to the Office of the Secretary of Defense, the Joint Chiefs of Staff, the Military Services and the Director of Central Intelligence. Within OSD the principal consumers are the Offices of the Under Secretary of Defense for Policy, the Deputy Under Secretary for Technology Security Policy, the Under Secretary for Research and Engineering, the Assistant Secretary for International Security Policy, and the Assistant Secretary for Public Affairs.

Major responsibilities for support of the Office of the Secretary of Defense (OSD) by the Defense Intelligence Agency (DIA) and the Service Intelligence Agencies are outlined in DoD Directive 2040.2, "International Transfers of Technology, Goods, Services

and Munitions," and several other pertinent Directives. The Directorate for Scientific and Technical Intelligence in DIA serves as the DoD focal point for intelligence support to technology security activities. Among the many responsibilities levied on DIA and the Service Intelligence Agencies are the following:

- Formulate and/or coordinate intelligence assessments concerning the type and number of illegal transfers of technology, goods, services, munitions and the associated transfer mechanisms.

- Conduct and coordinate intelligence reviews on assigned technology, goods, services, and munitions cases to include end-user checks on declared intermediate and ultimate consignees.

- Provide and/or coordinate the provision of intelligence expertise in interagency, national and international fora on technology security matters.

- Assess and/or coordinate assessments of the availability of technology, goods, services and munitions in foreign countries in terms of its equivalence in quality and quantity to such technology, goods, services, and munitions available from U.S. suppliers.

- Provide and/or coordinate intelligence assessments concerning the total effect of the legal or illegal transfer of technology, goods, and services on foreign capabilities.

- Provide intelligence support to the DoD International Technology Transfer Panel, Subpanels and Working Groups.

- Assist in identifying and assessing technology, goods and services critical to potential adversaries of the United States.

- Provide intelligence assessments on the ability of foreign nations to protect U.S. technology, goods, services and munitions.

- Provide intelligence support to export control and enforcement agencies regarding technology security.

Technology security support to the Joint Chiefs of Staff is usually provided in response to specific requests for intelligence support for major assessments of the actual or potential impact of technology transfer on impending or past actions. Current intelligence reporting and periodic activity reporting regarding technology security informs the JCS of day-to-day developments.

DIA and the Service Intelligence Agencies provide technology security support to the Military Services through direct liaison and numerous studies on the technological capabilities of the

Communist countries that address various aspects of the technology security problem. An intensive briefing program entitled, "The Threat to Western Technology," has been presented to thousands of US government and contractor personnel.

The Director of Central Intelligence provides community-wide intelligence assessments on technology security to support the Departments of State. Defense, Commerce, Treasury (and Customs), Justice (and the Federal Bureau of Investigation), Energy, the National Security Council, and other agencies and departments of the Executive Branch, as well as the Congress. Extensive support is provided to the Director of Central Intelligence (DCI) by DIA, the Service Intelligence Agencies and the intelligence arms of other executive departments and agencies.

To effect this support, the DCI's Technology Transfer Intelligence Committee serves as the principal coordinator of intelligence for those U.S. government entities with responsibilities for policy and action on technology security issues. In providing this support, two major subcommittees (COMEX which deals with visits and EXCON which concerns trade) have been active since 1981 to address continuing tasks. A number of ad hoc working groups with full support of the DIA and the Service Intelligence Agencies are active at all times to address time-sensitive topics requiring coordinated Intelligence Community input.

The DoD intelligence activity is in place to provide direct support to the DoD technology security program. In addition to direct DoD support, extensive indirect support is provided through the DCI's committee structure. The DoD intelligence activity has provided timely intelligence to support decision-makers on key policy issues. With recruitment and training of additional scientific and engineering intelligence personnel, the DoD Intelligence Community will respond more effectively to the continually increasing requirements for intelligence support to the technology security program.

E. Innovative Security Programs to Protect Unclassified Technologies

Very High Speed Integrated Circuits (VHSIC)

The VHSIC program is one the Department of Defense's most critical research and development efforts. Integrated circuits, already part of virtually every modern weapons system, will play an ever-increasing role on the battlefield of the future. The VHSIC program is developing more capable and reliable integrated circuits that process data considerably faster, use less power, and have less volume, weight, and system life-cycle costs.

Representatives from the U.S. defense electronics community, industry, and DoD experts designed an innovative security system to protect VHSIC without producing costly time delays which could

serve to reduce the competitiveness of U.S. defense companies in the VHSIC program. This security program provides for security classifications, application of export control regulations, and other controls to restrict certain unclassified critical technology from public disclosure. The recently published "VHSIC Security Classification Guide" (DoD Instruction 5210.25, dated 27 Nov 85) provides uniform guidance in the handling of VHSIC information and products.

DoD Instruction (5230.26, dated 17 March 1986), "VHSIC Technology Security Program," establishes VHSIC technology security policy, prescribes procedures, and assigns responsibilities for the VHSIC security program. It builds on defense contractors' existing security policies and procedures and features inspection of contractor facilities and certification as to the effectiveness of contractors' internal security procedures for their personnel, facilities and products.

The VHSIC security procedures were put into place at the onset of the VHSIC development to ensure that this critical technology is not compromised.

Data Bases

Ready transmission of data through international networks provides our adversaries with another potential source of sensitive technology in a number of important fields. Even though the information in open data banks is unclassified, it frequently has military significance when a large volume of information is acquired, compared, and analyzed. The announcement in 1981 that the U.S. government would no longer fund the International Institute of Applied Systems Analysis (IIASA) brought public attention to this problem. IIASA, an international research organization, had become a major Soviet access link to a wide range of Western data bases.

This problem of easy access to Western data banks has multiplied as computer network systems have proliferated. The Defense Technology Security Administration (DTSA) has taken the lead in raising this issue in bilateral trade security discussions with friendly countries, and is participating actively in the ongoing search for ways to protect sensitive technological data transmitted in this manner. For example, DTSA continues to study proposals which would control access to data bases while allowing a fruitful interchange of ideas and information.

F. Strategic Defense Initiative

The Allied Strategic Defense Initiative (SDI) represents the first time that DoD has successfully integrated technology security with technology cooperation objectives at the outset of a major program. In recent months, U.S. negotiators have achieved consi-

derable success in furthering the President's goal of Allied participation in SDI research. Less well-known, but equally important, is the the Administration's success in ensuring that the critical technologies being researched can be protected from Soviet acquisition efforts.

The Defense Technology Security Administration took the lead within DoD in developing a technology security approach to Allied participation in the SDI program. The approach has been adopted by the government as a whole. The SDI technology security approach builds upon established DoD procedures for transfer of technical data, classifying material, and the competitive procurement process. Consistent with this approach, DoD has concluded successful negotiations for an umbrella agreement for the United Kingdom's participation in SDI. Subsequent agreements were concluded with the Federal Republic of Germany and with Israel; further bilateral agreements are expected. The Administration hopes to expand the SDI cooperative research effort, backed by a strong Technology Security Program.

The breadth and intensity of the SDI research will considerably alter the technologies known, or expected to be, militarily critical. In this expectation, the current effort to revise the Militarily Critical Technologies List (MCTL) has been specifically augmented to examine the SDI-associated technologies.

Other efforts are continuing, both under contract and in-house, to assess foreign technical capabilities in SDI technologies. This effort will assist in MCTL development, and will provide technical support for U.S. decisions and policies on Allied cooperation in the SDI research program.

G. Space

Recognizing the unique national security importance of key space technologies, the President recently directed U.S. government departments participating in space research to implement special security procedures for space technology. Along with other DoD elements, the Defense Technology Security Administration is working to develop these security elements. For example, we are seeking a more systematic review of space information before it is released to the public or to foreign governments or companies. This procedure would be implemented to support the applicable Export Administration Regulations and International Trade in Arms Regulations. DTSA is also working with the National Aeronautics and Space Administration and other agencies on the technology security aspects of cooperation with various friendly countries on the use of a space station.

IV. EFFICIENCY

SERVING THE EXPORTER

A. Case Processing Legal Deadlines and Actual Processing Times at DoD

1. Munitions

The export licensing review process at DoD continues to be guided by the desire to reduce the potential for competitive disadvantage to U.S. industry while safeguarding national security under existing regulations.

During the past year, the Department of Defense has further improved its performance in the processing of license requests to export military items and technical data controlled under the Arms Export Control Act and the International Traffic in Arms Regulations (ITAR). The giant strides made in 1984 from 92 days at the beginning of the year to 38 days at the end were duplicated in 1985. Despite an increase of over eight percent in cases received by DoD during the calendar year, the average age of cases in process was reduced to 16 days by the end of 1985. The denial rate remained at seven percent in 1985. This was accomplished through a melding of dedicated professionalism, automation and streamlining of procedures by the Defense Technology Security Administration's Munitions and Munitions Technical Directorates, working in close coordination with the Military Services, other DoD agencies and U.S. industry. This effort was highlighted when we reduced the caseload to the point where there were no cases older than 60 days in April 1985 and none older than 45 days by mid-November 1985. We, as well as the U.S. exporting industry, are most pleased with the continued dramatic reduction in the number of days required for DoD processing of export requests.

We will strive for continued improvements in munitions case processing. Ongoing efforts to upgrade our data processing capabilities include the use of an automated end user and intermediate user name check programs. The Department initiated action to have DoD computers net with Department of State computers. Once the interface system is approved by State and activated, we can expect to further reduce the time required for State to process and refer the export license request to Defense for review and for Defense to respond. However, in order to produce even greater efficiencies in DoD case processing a more responsive data base management system is needed.

2. Dual-Use

a. West-to-East Applications

In late 1983, when Trade Security Policy assumed responsibility for managing the review of West-to-East export applications, the average age of pending cases was 70 days. This was

unacceptable to the exporting public, and a commitment was made, on the part of management and staff, to improve the performance.

Through managment methods such as assigning strict accountability for processing times to the responsible staff members, and by the employment of the automated systems, discussed elsewhere in this report, the average age of West-to-East applications in process was cut to 30 days in only 12 months. As of February 1985, the processing time was down to 15 days.

b. West-to-West Applications

On January 4, 1985, the President approved the coordinated review of export license applications by the Departments of Defense and Commerce for eight commodity control list (CCL) categories to fifteen Free World destinations. The memorandum of understanding between the two departments further directed that an electronic data link be established.

Under terms of this agreement, the Department of Defense has seven days to review electronically transmitted license applications. If during this time it wishes to review the complete file it must complete its examination within fifteen working days of referral by Commerce. Defense review takes place simultaneously with the review in the Department of Commerce.

Defense began receiving its first cases for review electronically from Commerce under this agreement on February 15, 1985. A prototype case processing system has been designed and developed for this purpose under a contract with American Management Systems. The Defense Automated Cases Review System (DACRS) receives, stores and processes cases transmitted via telephone line from the Commerce License Access Review System (LARS). By the first anniversary of DACRS operations 15,478 cases with a total value of $7.6 billion had been reviewed and processed within the established deadlines of the Presidential Directive.

During this initial start up period Defense has prided itself on a record of meticulous handling of cases. Presently, Defense's initial case review time averages less than two days. This means that simple cases where there are no questions on the commodities to be exported are taking less than 48 hours to clear the DACRS system. In instances where Defense has asked for the complete file the more complicated review is taking less than 10 days after receipt of complete case files.

From its inception the DACRS system has proven to be flexible in operation. As the data base has grown and the Defense Department has added administrative, technical and intelligence filters it has also become a useful analytical tool for case processors.

In little over a year, Defense believes it has made a number of worthwhile contributions toward improving the export control program.

It has demonstrated that an automated case review system can speed the process of export licenses. This success under Department of Defense leadership has resulted in studies by the two departments on areas where the process can be speeded further through automation.

Defense review has resulted in a reduction in the improper use of the Individual Validated License (IVL) as a multiple or bulk license. Early in its review of Free World export license applications under the Presidential Directive, Defense began to be concerned about the large number of items being considered on license applications with a vague or "for resale" end use. Bulk shipments of computers and related equipment valued at several million dollars were common. In particular, one application to export to a neutral country was for computers valued at over $156 million that even exceeded the limits of Distribution Licenses fo COCOM countries.

In another instance, Defense identified a license application that grossly exceeded annual sales projections for the applicant and ultimate consignee. Furthermore, Defense determined that the consignee had given written assurances that items could not be used for defense purposes but intelligence data revealed the principal business of consignee was with military organizations. Upon further analysis of the data readily available on DACRS, Defense found that this type of license submission was typical for a company that could not qualify for a Distribution License because of the annual number of licenses saved requirement. Defense immediately returned these cases to Commerce requesting specific end-user and end-use information.

To allay concerns for diversion through the misuse of the IVL and still remain sensitive to the needs of the exporters, Defense is working with both Commerce and the exporters to plug this loophole in our licensing system. Since the Defense initiative earlier this year, the number of bulk IVL license submissions has declined.

In two major instances, Defense review resulted in the denial of over 200 licenses to questionable end-users at Pacific Basin country destinations. One involved 119 cases totaling $7 million consisting almost entirely of computer accessories for networking or CAD/CAM application. The other involved over 100 cases totaling more than $80 million. Defense's recommendations for denial were sustained by post license checks on the ultimate consignees, several of whom are now under indictment or investigation. At the suggestion of Defense, a joint U.S. Defense/Commerce/Customs Study Team will soon visit selected Pacific Basin countries on a fact finding mission.

A general tightening up of foreign policy review to such destinations as Libya, Syria, and Iran, has been effected. Utilizing its technical and intelligence resources, Defense has recommended denials of sensitive technology to such destinations for national security reasons. Defense continues to work with the Departments

of State and Commerce to define and establish more effective controls in these areas.

The Defense DACRS system and the electronic transfer of case information has resulted administratively in improving the quality of data entered into the Department of Commerce's LARS computer system, giving both departments more complete and accurate information in the database.

c. Foreign COCOM Cases

The United States expects that its COCOM allies will take expeditious action on requests for exceptions that it presents in the COCOM forum on behalf of US exporters. Therefore, it is important that the US reciprocate and provide expeditious processing of foreign cases presented to us for review via COCOM. In 1981, processing of foreign COCOM cases in DoD averaged 50 days. Through the management and automation initiatives discussed earlier, we were able to cut that to 30 days in only one year, and to 20 days by February 1985.

B. How an Export License Application Flows Through the Department of Defense

1. Munitions

Under the authority of the Arms Export Control Act, the Department of State has statutory responsibility for administration of munition items export licensing. DoD, following its national security mandate, reviews approximaely 20 percent of these export license requests and renders its position to the Department of State.

The Munitions Directorate of DTSA is the entry point for those export requests from the Department of State. It is the responsibility of this directorate's staff to ensure that the military services, appropriate Defense agencies and the technical staff of the Office of the Under Secretary of Defense for Research and Engineering review these export requests or munitions cases in a timely manner (concurrent review). To save time, the Department of State delivers these cases concurrently to the military Departments and DoD Agencies and components it believes would have an interest in the case. The Munitions Directorate then assures that the appropriate staffing has been made and the DoD position is formulated and sent to the Department of State.

Figure 8 depicts both the input and output license flow within the Department of Defense (DoD). After receiving recommendations from the DoD elements tasked to review a particular license request, the Munitions Directorate then studies these recommendations and develops the DoD position which is sent to the Department of

FIGURE 7

AVERAGE AGE OF WEST-TO-EAST AND FOREIGN COCOM CASES

(SEPT 1983-DEC 1985)

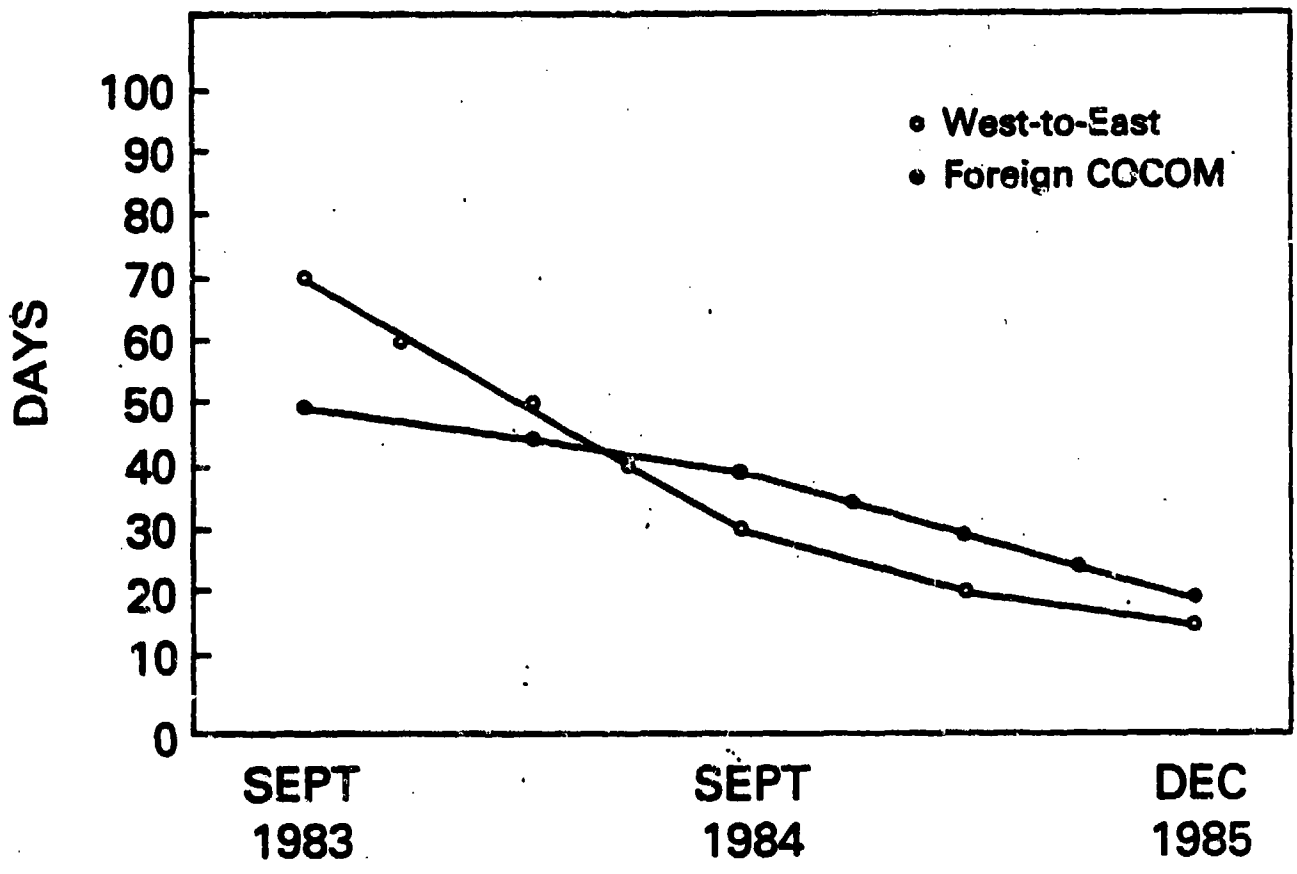
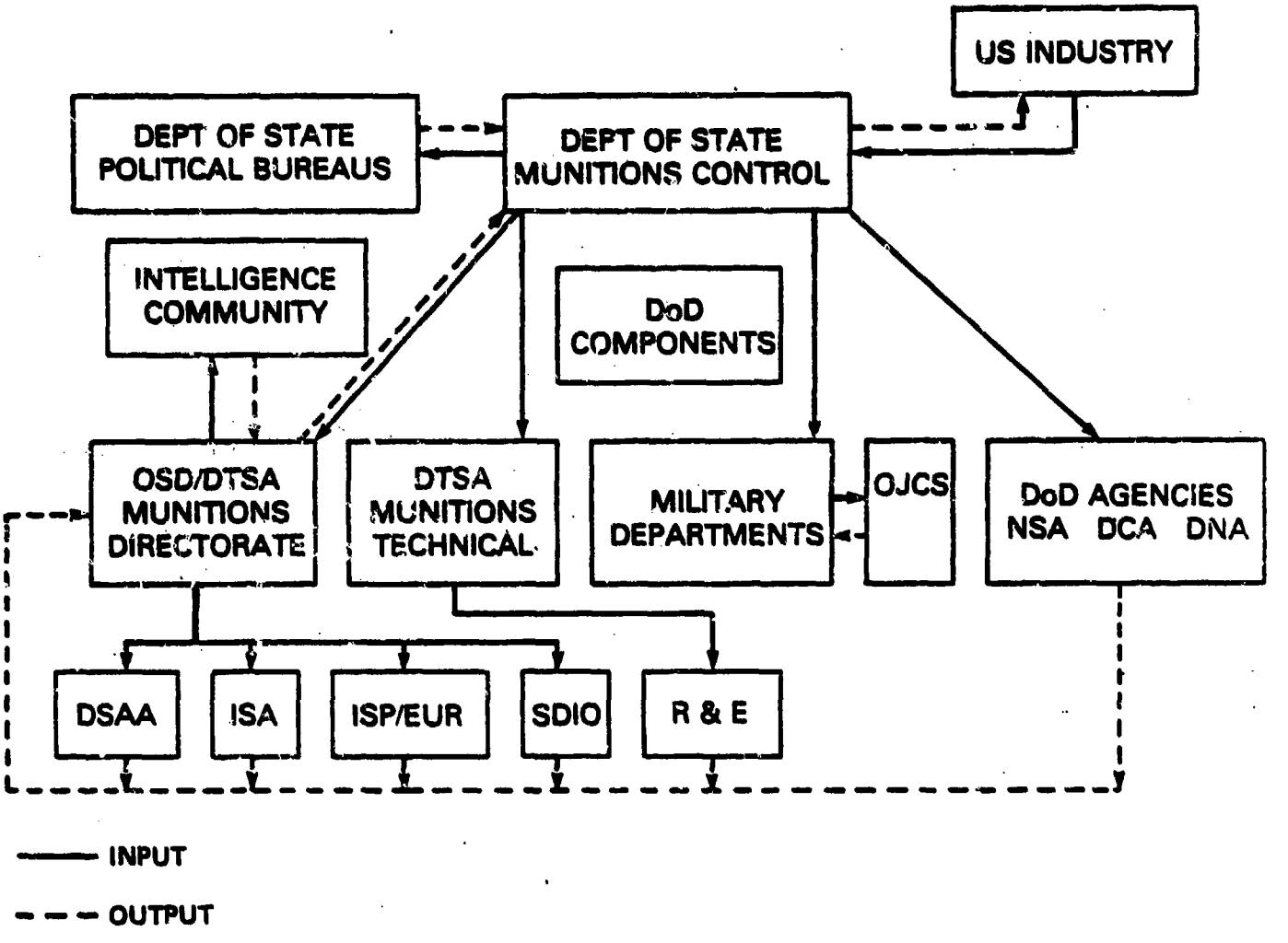


FIGURE 3

MUNITIONS LICENSE FLOW



State. Most differences within DoD are resolved at the working level. Those that cannot be so resolved are referred to the International Technology Transfer Panel for resolution.

2. Dual-Use

a. West-to-East Applications

West-to-East applications are submitted to the Department of Commerce by U.S. companies who want to export controlled commodities to proscribed destinations. After registration and review by the Department of Commerce, these cases are referred to other government agencies as required, including DoD.

Upon receipt, DoD logs the case into the Foreign Disclosure and Technical Information System (FORDTIS), capturing pertinent information including: dates, applicant name, consignee, key words, and commodities involved. The case is then assigned to a technical expert who assesses the impact of the proposed export on national security. The export regulations, COCOM agreements, technical data, personal knowledge, recommendations on previous cases, intelligence reports, and consultations with the military services and/or the applicant are all used in this assessment. The results are then documented in FORDTIS for reference and use in reviewing future cases for the same or similar commodities.

The case then undergoes a policy review which considers the technical assessment as well as other pertinent information on which a final DoD position is based. This position is also documented in FORDTIS and then transmitted by written memo to the Department of Commerce.

b. West-to-West Applications

On January 4, 1985, the President acted to limit the illegal diversion of militarily sensitive technology and equipment through Free World countries by directing the Department of Defense to review applications for some categories of exports to certain Free World countries targeted by the Soviet Bloc for illegal acquisitions. The Presidential Directive is selective. It limits Department of Defense review to applications for export to 15 countries of eight categories of critical commodities known to be of particular interest to the Soviet military.

In almost all cases, this review does not imply that a country is engaged in illegal activity as a government policy. It does mean, however, that the Soviets have targeted that country for illegal acquisition. A number of these countries are cooperating with the U.S. on a bilateral basis to provide enhanced protection of sensitive U.S. exports.

In order to implement the President's directive, DTSA developed the Defense Automated Review System (DACRS) which is discussed further

in Section IV.C.2. of this report. The use of DACRS for review of West-West cases began on February 15, 1985. A brief analysis of the results of our Free-World case review shows that between February 15 and December 31, 1985, Defense reviewed 14,303 cases. Recommendations of disposition given to the Department of Commerce were as follows:

	Number	Percent
Approved	10,556	73.8
Approved with Conditions	1,767	12.4
Returned without Action (for further information)	760	5.3
Denied	1,220	8.5
Total	14,303	100.0

In working to meet our objective of interfering as little as possible with legitimate, non-strategic trade, we recently added the capability to electronically return the results of our review to the Department of Commerce. This reduced processing time considerably. DTSA is hoping that experience gained through the electronically supported processing of these license applications can be translated into further improvements in the process throughout the Government.

DoD's updated review efforts have resulted in these improvements in the export licensing process:

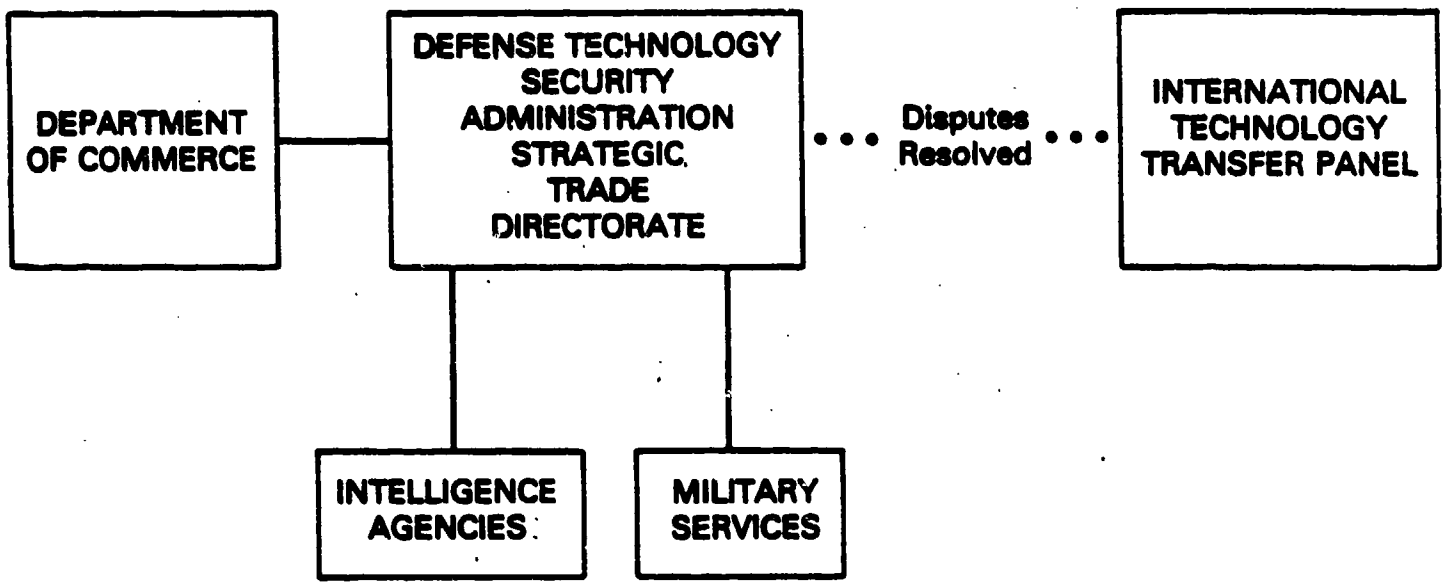
- Greater care is being taken in the front-end of processing to ensure that information entered into the system is accurate;
- Applications are being returned to the applicant via the Department of Commerce when there is insufficient end-use or end-user information;
- Ways are being examined to implement distribution license recordkeeping controls on individual licenses where the end-use is for resale.

c. Foreign COCOM Cases

COCOM procedures require member governments to submit for unanimous approval by the Committee those export licenses issued by national licensing authorities involving embargoed items proposed for export to proscribed destinations. These COCOM export licenses are classifed into seven types of cases and are provided to each country delegation represented at COCOM headquarters. Upon receipt by the U.S. delegation, the COCOM cases are then rushed by courier

FIGURE 9

DUAL-USE EXPORT LICENSE PROCESSING AT DoD



to Washington, D. C. and copies are provided to DTSA, the Department of State (Office of East-West Trade) and the Department of Commerce for review under U.S. technical and policy guidelines under the aegis of the Economic Defense Advisory Committee (EDAC).

Once a case is received at DTSA, a case folder is prepared and a case description (including case number, type of case, assigned analyst, deadline dates) is entered by the DTSA COCOM coordinator into the automated Foreign Disclosure and Technical Information System (FORDTIS) for on-line tracking, position recording and historical record purposes. A duplicate folder which includes the technical brochures is then submitted to the DTSA technical case coordinator for staffing to the technical support team for review and evaluation. If the technical support team determines that the case requires review by the Military Services and/or DoD agencies, immediate tasking is made. The Services' and components' input contributes to development of the DoD recommended position, which is based upon US DoD technology export control guidelines. The recommended position is entered into FORDTIS, reviewed for consistency with DoD and COCOM policy guidance and a DoD position is finalized.

This position is then submitted to EDAC Working Group 3, chaired by the Department of State and composed of representatives from DTSA, the Department of Commerce and other U.S. agencies involved in export control. If this working group reaches a consensus it is then submitted to the U.S. delegation in Paris for further communication to the COCOM Secretariat and, finally, to the appropriate COCOM delegation. If the working group does not reach a consensus on a case, it is referred to the Executive Committee which operates at the Office Director level. Cases not resolved by the Executive Committee are referred to the Sub-EDAC which operates at the Deputy Under Secretary level. The next referral levels are the EDAC (at the Assistant Secretary level), the National Security Council, and the President.

Foreign cases that proceed through the EDAC structure must meet a 60-day deadline for People's Republic of China (PRC) cases, and a 90-day deadline for all other proscribed destinations. If no objections to an export are raised within the time limit, the case is automatically approved by COCOM. Currently, the average age of a COCOM case within the DoD is 16 days and the vast majority of positions taken by EDAC reflect DoD recommendations.

d. Operating Committee

The Operating Committee is the first step in the interagency review process of contentious U.S. export applications. The Committee, chaired by the Department of Commerce, is a working-level group which attempts to reach agreement on major export issues, usually involving proscribed destinations. Recent Committee resolutions have involved seismic data acquisition systems to the PRC.

The Department of Defense frequently finds itself advocating its position on specific export license applications in isolation. Often the other participating agencies will challenge DoD's national security-based objections with arguments of foreign policy or commercial competitiveness. DOD positions, therefore, require the greatest possible degree of cogency and logical exposition buttressed by persuasive technical arguments.

Additional cooperation among policy-level decision makers at all participating agencies is needed to resolve these cases in an expeditious manner.

3. International Technology Transfer Panel

The DoD-wide International Technology Transfer Panel continued its work in 1985 under the provisions of DoD Directive 2040.2. Subpanel A, which deals with export control policy, was the most active.

The first sales of major defense equipment to the People's Republic of China (PRC), based on the 1984 Subpanel A's policy regarding the releasability of dual-use and military goods, services and technology to that country, were concluded in 1985. Exports of a U.S. small arms munitions facility and torpedos were approved through the interagency process, in consultation with European and Pacific allies. That policy remains the authoritative guide for technology transfer to the PRC.

Another example of Subpanel A's role in successfully coordinating export control policy issues among various players lies in the development of special security procedures for the export of "trusted" computers. Trusted computers are those with security features built in to guard against break-ins by "hackers" and to allow for compartmentalized access to the computer's stored data.

Subpanel A was convened to establish an efficient technical review procedure for proposed exports of trusted computers. An agreement was reached in Subpanel A whereby DoD obtains technical review from the National Security Agency. This agreement has resulted in establishment of a predictable threshold of trusted computer security capability under which these computers are exportable to certain destinations.

C. Automation

DTSA has a comprehensive plan for defining, developing and implementing its automation needs for the future. Called the High Technology Export Analysis and Control System for the 1990s, or HI-TRAC 90, the plan calls for further automation of present methods of processing export license applications within DTSA. HI-TRAC 90 capabilities will include furnishing analysts with on-line access to both new and existing data bases containing reference, management, and tracking information.

The software will also incorporate artificial intelligence features to streamline the process of detecting those individuals and organizations attempting to illegally export controlled commodities and high technology items. With its office automation and telecommunications capabilities, the HI-TRAC system will serve as a keystone for the integration, modernization and restructuring of the United States' export license review processes in the future.

1. Foreign Disclosure and Technical Information System (FORDTIS)

The Foreign Disclosure and Technical Information System (FORDTIS) provides DoD users with access to information needed in the technology transfer/technology security process via an interactive, secure communications network. The primary function of FORDTIS is to assist DoD decision-makers and analysts in the processing of export license applications and requests for foreign disclosure of classified information.

FORDTIS provides a basic case processing and control through tracking and assignment functions for all active cases in DoD, maintaining a historical record of prior cases and their disposition, and facilitating access to information in reference data bases that is related to case processing. It also provides an electronic mail capability. Over 300 registered users throughout the Office of the Secretary of Defense (OSD), the Military Services, and defense agencies have the capability to exchange classified information while processing export license applications. This communications network now supports 35 remote sites with 103 terminals available for DoD interactive processing.

FORDTIS is managed by a permanent organization established in the Office of the Deputy Under Secretary of Defense for Policy. The central computer site and secure communications network is operated and maintained by the 1st Information Systems Group, U.S. Air Force, which develops and maintains software with contractor assistance.

With greater DTSA management attention on the technology transfer/technology security case process, analyst efficiency and control over outstanding cases has been improved significantly. We have seen a steady decline of average case processing time in DoD. Also, better case decisions are made because the system provides a consistent frame of reference with respect to policy, technology, and historical precedence.

FORDTIS became fully operational in 1984. Now that it is maturing in the case tracking, assignment and processing functions, we are proceeding with extensive enhancements to make the system even more effective for the decision-makers. In 1985, we converted all case processing data to a state-of-the-art intelligent database machine (IDM) and added a second minicomputer. These enhancements significantly increased system capability, reliability and redundancy.

The final significant capability that FORDTIS accomplished in 1985 is the addition of a Foreign Military Sales (FMS) history database. This database, updated monthly, consists of major items that the U.S. agreed to sell to foreign countries under the FMS program since 1982. This information is useful to munitions case analysts.

Efforts scheduled in 1986 and beyond include the continued extension of FORDTIS to agencies outside of DoD. Another major enhancement area involves expansion of the reference data bases available to users.

2. West-West Case Review

When the Department of Defense was directed by the National Security Council (NSC) in 1985 to begin review of certain West-to-West export license applications, it was clear that the processing time must be efficient and fast. To meet the short deadlines established by the NSC, and in order to facilitate the review of export license applications, a prototype system called the Defense Automated Case Review System (DACRS) has been developed. The objective of the system is to screen out those cases in which there is a suspected potential for diversion of the commodity to be exported.

DACRS provides the following functions:

- Electronic downloading of cases from the Department of Commerce (DOC)
- Editing and updating of the DACRS database
- Analysis of case data
- Passing recommedations to DOC

The DACRS provides the capability to display each case on a screen, identify the consignee address, and extract the Processing Data Rate (PDR) of proposed computer exports. (The PDR is a number derived from the "average number of bits transferred per instruction" and the "processing rate of the computer." A more detailed description of PDR is contained in Part 376, Special Commodity Policies and Provisions, of the Export Administration Regulations.)

The DACRS is a microcomputer-based system that uses fourth generation language and an integrated database product called PC FOCUS. It is used to screen a selected set of Commodity Control List (CCL) items for selected destinations.

The cases are then processed through several "filters" (e.g., Dun & Bradstreet, a suspect end-users list; an export control filter for reexport checks, a technology filter to

identify high technology items for resale vs. manufacturing use, and an administrative filter).

DACRS allows historical searches for previous shipments to the ultimate consignees to identify equipment, actions taken, and quantities or values of these prior cases. This and other reports which can be generated allow the analyst to determine trends and buying patterns and flags the need for further inquiries into suspect cases.

The prescreening identifies cases that require little review. These are approved in less than three days. In cases where the hard copy is obtained from DOC, DTSA is completing its review between eight and 12 days. DACRS allows DTSA analysts and engineers to address higher priority cases through the use of this new, automated tool.

Future plans entail the expanded use of end-user checks using information available from the intelligence community, the Departments of State, Treasury and others. This information will allow DTSA to identify a larger number of "suspect" end-users and to build profile filters for additional screening of export license applications.

3. Secure Data Base

The Defense Technology Security Administration Technology Transfer Secure Data Base became operational in late 1985. It contains classified data records of known and suspected worldwide diversions of advanced Western technology to proscribed nations.

4. Automated Impact Assessment

Another method being developed to increase the efficiency of the Defense Technology Security Administration's case review process is the automated impact assessment system illustrated in Figure 10. The approach being built into this system is the microeconomic assessment of individual cases or groups ("clusters") of cases which may have some actual or potential interrelationships. One case, for example, might concern the transfer of a piece of keystone manufacturing equipment, which in and of itself may have limited impact. It may lead to a complete turnkey manufacturing capability, however, when put in the context of other transfers already taking place or requested. This larger perspective is needed for credibly estimating the impact of specific technology transfers and the potential Soviet cost savings. The principal elements of data and expert judgment to be considered are:

- Selection and clustering of CCL and COCOM cases to the USSR and the Warsaw Pact

- Identification of key aspects of these cases given the full range of recent transfers (e.g., end-user association with the military)

- Identification of potential enhancements of Soviet military production capability or of their military technology base
- Calculation of potential Soviet defense budget savings associated with these cases
- Estimation of the nature and cost of appropriate NATO/U.S. responses necessary to counter Warsaw Pact/Soviet military enhancements

Based on assessments performed to date, the technology areas targeted by the Soviets and their allies and most amenable to this type of analysis are:

- Automated Production Control
- Microelectronics
- Telecommunications
- Optoelectronics
- Transportation
- Computers
- Structural Materials
- Vehicle Power and Propulsion
- Weapons
- Guidance
- Manufacturing
- Directed Energy
- Sensors

We intend for this automated impact assessment system to have many types of users, including DoD Technology Security Program managers, case processors, and case assessment analysts. Further, it will be able to support multiple requirements--including COCOM and other policy support, refinement of the Militarily Critical Technologies List (MCTL), input to CCL, COCOM and munitions case processing, and preparation of periodic technology security reports. Each system user will have access to the system via a minicomputer or microcomputer terminal, and each will have software tailored for his or her functional needs.

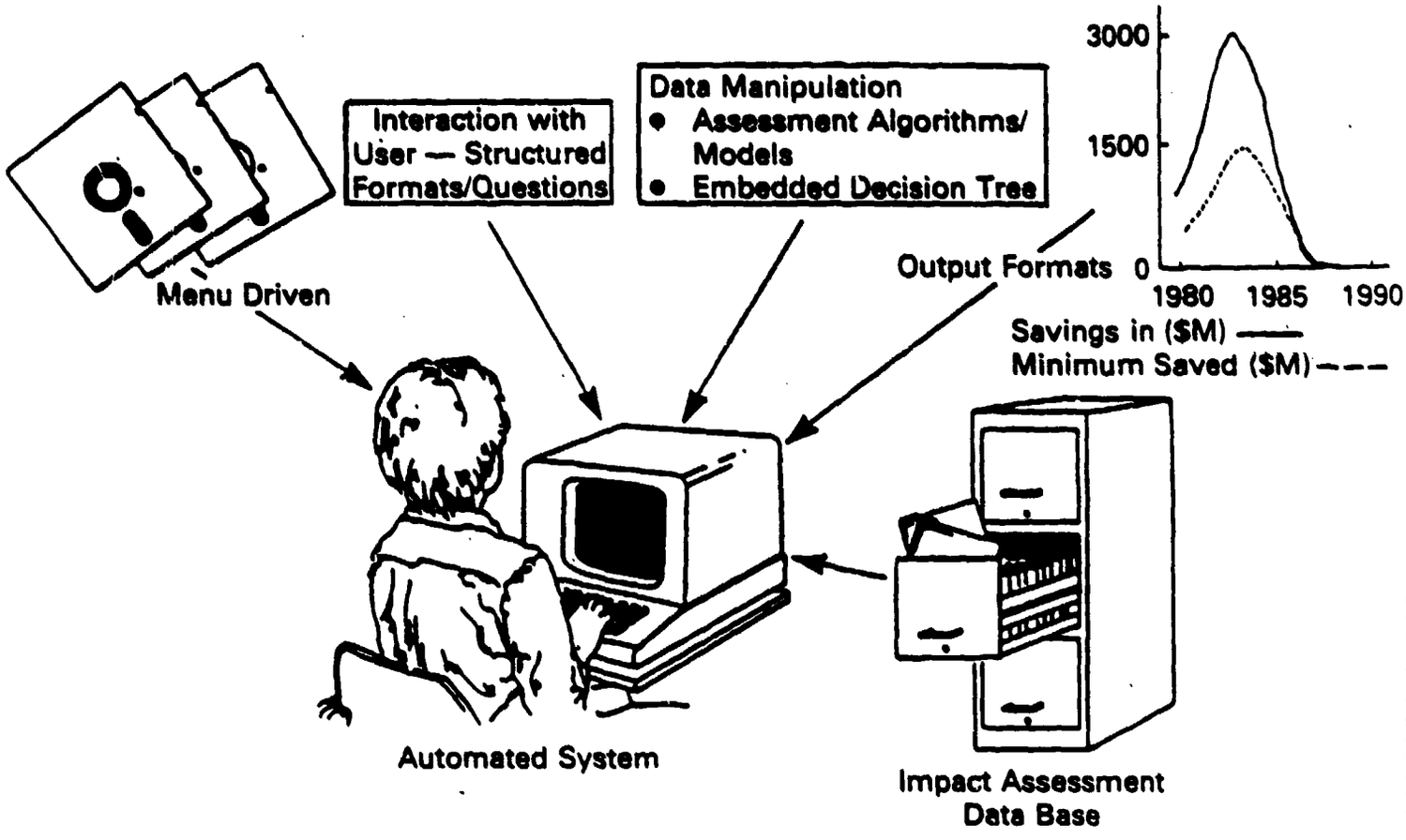
For each case, the prototype system will automatically provide the analyst with access to specialized assessment data bases and to a variety of modeling spreadsheets used for case selection, assessment scenario generation, and preparation of the final impact assessment. This process is illustrated in Figure 11 using a specific example from our 1985 study -- a request to export to Romania technical data to manufacture high quality ball bearings. This case would be entered into the automated system from the DoD case files (shown on the left in Figure 11).

Based on the case data which is input, and on very simple criteria, the system would identify whether the case is a candidate for further analysis. Given the East European recipient of the technical data and the importance of the technology, the ball bearing case would be selected for analysis.

Once selected for final assessment, the analyst would retrieve specific information relating to this case from the supporting data bases. Specific technology lead/lag data, production data for the specific facility, and technical data such as mean-time-between-failure rates of Soviet jet engines would be retrieved from the supporting data bases. The analyst would then select

FIGURE 10

AUTOMATED SYSTEM FOR ASSESSING THE IMPACT OF TECHNOLOGY TRANSFER ON WESTERN SECURITY



the most credible assessment scenario and perform the final cost assessment using economic models contained in the software. Since the Soviets have had problems in the past with jet engine reliability, the economic model for the ball bearing case is based on savings to the military for jet engines with enhanced reliability. The system gives the impact analyst complete, interactive control over each phase of the assessment.

A very important aspect of this automated system is the associated supporting data bases. These data bases are briefly described below:

Case Data

Case data is detailed information relating to the substance and status of specific export requests under review by the Department of Defense.

Product Data Related to Potential Applications (Possible "End-Uses")

Product application data is that category of information relating to possible military or industrial uses of the specific end product, services or data requested for export. The category includes product type (e.g., technical data, hardware), performance specifications (e.g., COCOM control parameters), and potential military or industrial uses or applications. The assessments system will ultimately incorporate a computerized data library of this information for manipulation by specialized software.

Soviet/East European End-User Data

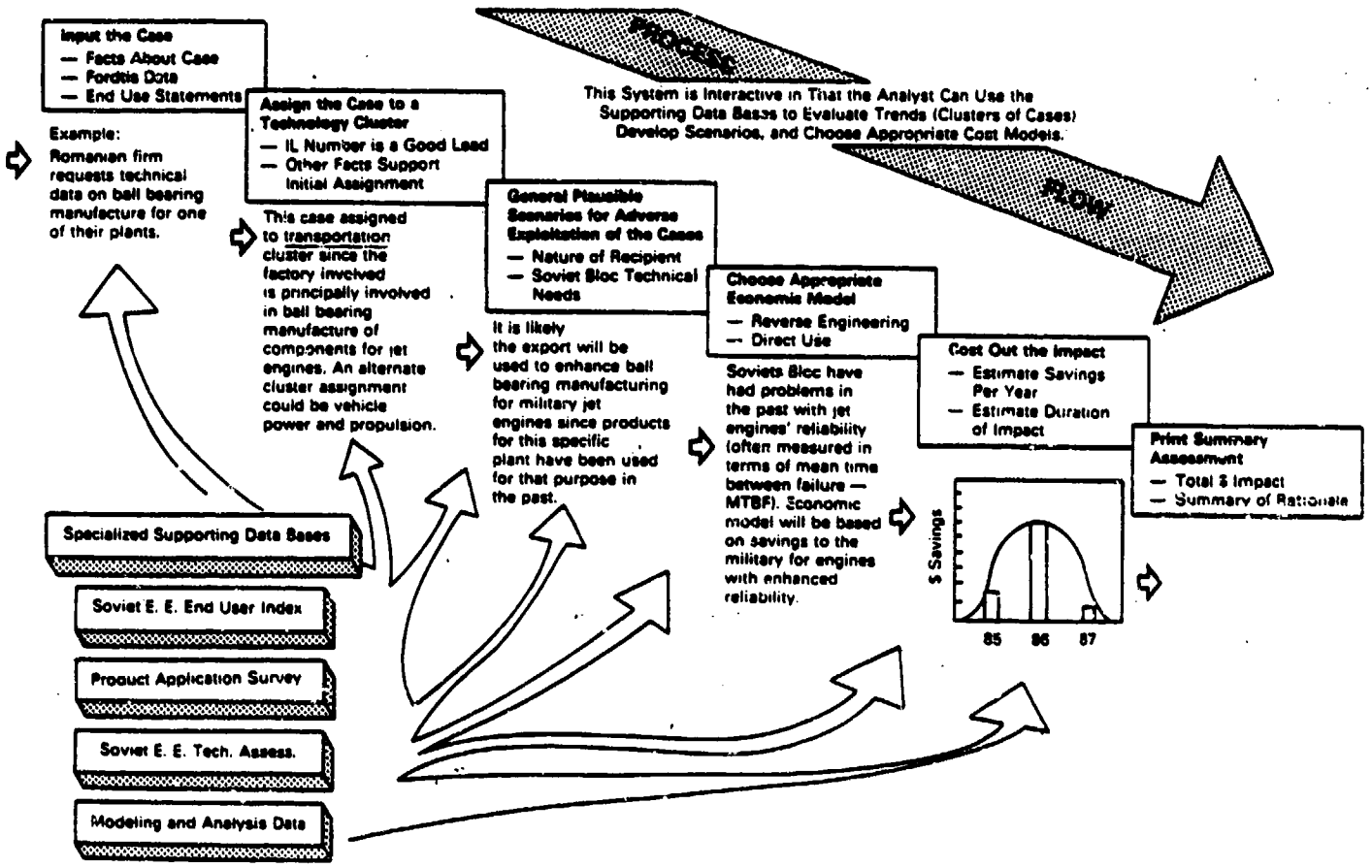
Soviet/East European end-user data is that category of information which describes the linkages of various end-users with the Soviet military (e.g., role of a facility in the production of military components) as well as past history of diversion. Much of this data will come from intelligence sources with some inputs from open sources.

Data For Soviet Technology Assessment (Clustering)

This information is used to assess the application of a specific case ' a technology cluster group in order to determine possible uses the export which might be detrimental to the security of the United States. Information for this data base would include such items as descriptions of Bloc military technology base relative to the U.S. and the West for key technology areas; long range military production goals for major tactical and strategic weapons systems; and generalized descriptions of national research and development efforts as indicators of worldwide trends as well as specific efforts.

FIGURE 11

AUTOMATED IMPACT ASSESSMENT SYSTEM



Data for Economic Modeling

Modeling and analysis data is that category of information used in the costing of impact. Examples of such data are Soviet lead/lag for a given technology cluster, defense budgetary data, facility production figures, U.S. research and development and production costs as an aid for estimating Soviet costs for comparable activity; and reverse engineering modeling data.

This system is being designed to provide maximum support to DTSA case processing activities without disruption. The proposed level of automation is consistent with what is practical for such an analytical process. The analyst or case processor will actively input to each case assessment, supported by computerized assessment tools and data bases. The prototype system we are now building is designed to evolve into a full scale system integral to other DTSA automation efforts.

D. Reserve Units

Naval Reserve OSD Technology Transfer Unit 0166 was established in March 1984 to mobilize with and support the Office of the Deputy Under Secretary of Defense (Strategic Trade Policy) and his staff. Since its inception, this unit has performed with distinction and demonstrated superb professionalism in supporting the mission of this office which is to preclude diversions of advanced militarily critical technology to proscribed nations.

The contributions by NR OSD TT 0166 have exceeded all expectations. Specifically noteworthy accomplishments during the past 24 months include:

- Providing a total of more than five man years of direct intelligence support in developing a high priority OSD/DIA all source world-wide data base of known/suspected diversions of advanced technology for use in DTSA processing of export license applications by an average of 19 unit members. This data base was created in response to a Presidential Directive to protect U.S. advanced technology and has received many favorable comments from U.S. Government officials for its key role in the successful implementation of this Directive.

- Materially assisted in performing intelligence analysis, coding data entry, and quality control on over 7,000 intelligence documents for inclusion in the data base.

- With rare skill conducted extensive in-depth analyses of intelligence materials to trace the geneological associations of known technology diverters and their pseudonym alter entities and accomplices. This effort has resulted in the exposure of over 60 foreign entities

involved in expropriating U.S. technology for the Soviet Union and its allies which would have otherwise gone undetected.

The foregoing results are impressive. They are a goal to which other Reserve Units should seek to emulate.

US Air Force Individual Mobilization Augmentee (IMA's) support for DTSA has just been approved by Air Force and OSD. The purpose of this program is to provide a cadre of 12 Air Force Reservists with technical degrees and industry experience in leading edge technologies. These personnel will serve annual active duty tours of 14 days or longer and will be responsible for presenting briefings/point papers for DTSA engineers on emerging technologies in their specialty areas. Additional Air Force Reservists will also perform active duty tours to assist with the development of an on-line emerging technologies data base to assist in case processing.

During the past eight months a number of outstanding Air Force Active Reserve Officers have performed active duty assignments with my staff in DTSA. Their superb efforts and long hours of highly professional work have been exceptionally effective in expediting the development of U.S. Government directed high priority projects for export license case processing and protection of U.S. high technology.

Specifically noteworthy accomplishments by these "Ready-to-go-Reservists" include successful design and testing of a joint DoD/Commerce-developed export license processing prototype. It is anticipated that this prototype will soon be expanded into a nationwide on-line system for authorized exporters with no record of technology diversions to quickly obtain automated approval of routinely approved Free World export licenses. The ultimate objective of this system is to give DTSA staff the necessary additional time required to process the more difficult export license cases where technology transfer is more likely.

V. PREDICTABILITY

A. Case Precedent System

A project was started in 1985 to develop an export case precedent decision-aid system based on an export case history/policy database. When completed, the database will contain policy guidance so that DoD license application officers can identify key current export control policy considerations relevant to the applications they are processing. And this flexible system will keep policy guidance and applicable licensing criteria up to date on an on-line basis. The historical licensing information in the database will ensure consistent treatment of like exports to the same destination country or country groups.

The decision support system will be built on three levels of analysis as shown in Figures 12 and 13.

The system is being designed as a rule-based system, driven by the technical parameters and rules derived from regulations negotiated at COCOM. The decision aids will include on-line access to technical information and end-user and end-use information provided by the Intelligence Community. The system is being designed to be both adaptable and flexible. If new COCOM rules are developed, these can easily be integrated into the system. Similarly, new policy direction can be quickly disseminated to system users. Further, the rules are not hard and fast; there is room for documented technical judgment and initiative on the part of the users.

We hope that this innovative, automated assistance to licensing officers and other policy makers will be initially operational in 1987. Its full implementation will depend on the availability of budgeted funds to acquire a planned-for, secure computer terminal network.

B. Foreign Availability Assessment System

Another means of increasing the predictability of export licensing under DoD's Technology Security Program is the SOCRATES foreign availabilty assessment system currently being developed by the Defense Intelligence Agency (DIA). The system is designed to track the technological capability (equipment, know-how, and materials) of all technologically significant countries worldwide in terms of years-ahead or years-behind the U.S. and the parameters of the equipment which gives the country its state-of-the-art capability. DTSA is contributing to funding support for SOCRATES.

SOCRATES is being designed to support updating reviews of the various export control lists such as the Commodity Control List (CCL), and the COCOM lists for foreign availability. SOCRATES will also support updates of the Militarily Critical Technologies List (MCTL). Analysts will be able to use SOCRATES in order to correlate the technology capabilities of past, present, and future

FIGURE 12

EXPORT LICENSE APPLICATION AUTOMATED PROCESSING SYSTEM

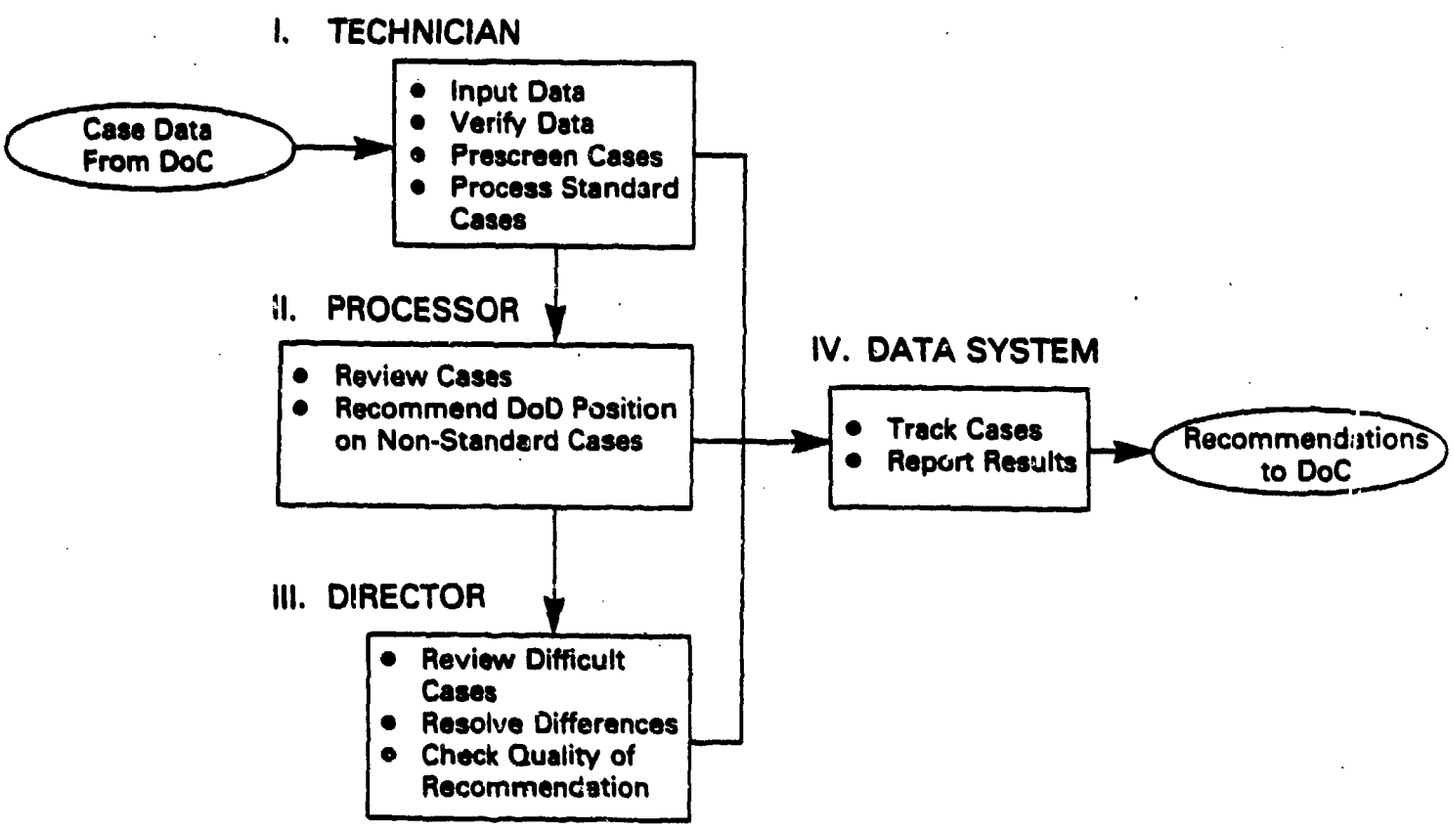
OBJECTIVE: Develop decision aids to support export case processing of both "standard" and "non-standard" cases.

DESIGN CONCEPT: Decision support needed for three levels of analysis

- Technician
  - Data Entry and Validation
  - Automated Pre-Screening
  - End-User Check
- Processor
  - Technical Parameter Check
  - End-User/End-Use Check
  - Prior Case Precedence
  - Policy Guidance
- Director
  - Verification and Review Capabilities
  - Summary Statistics and Reports

FIGURE 13

EXPORT LICENSE APPLICATION AUTOMATED PROCESSING SYSTEM



potential Free World suppliers with the needs of the proscribed countries. SOCRATES will, therefore, enable the Departments of Defense, State, and Commerce to factor foreign availabiity into the export license decision process in a way that will result in decreasing the flow of technology to potential adversaries while increasing the competetiveness of U.S. companies in the world marketplace. The SOCRATES system is being developed in FORDTIS.

VI. TRANSPARENCY

A. Status Checks - ELISA

In May of 1985, DoD's Export License Status Advisor (ELISA) became operational. This remote electronic bulletin board provides a means for exporters to conduct their own status checks on munitions and dual-use export license applications referred to DoD by the Departments of Commerce and State.

ELISA is updated automatically each day from FORDTIS and functions on a 24-hour basis (except for a 30 minute down time between 7 and 10 a.m. for updating). The system can be accessed on (202) 697-6109 from anywhere in the world by any other computer and a modem. Over 200 businesses take advantage of this simple, totally transparent means of checking the status of their export applications. The caller must have the application number assigned by the Department of Commerce or State to obtain information on the application. The screen will display the date the application was received in DoD, the date DoD action was completed, and the recommendation made to the Department of State or Commerce (approve, approve with conditions, deny, return without action, or more information needed).

DTSA also uses ELISA to transmit a variety of information to its users, both general export control information for all users and messages accessible only to specific users. The information may include such items as system changes, technology security tips, export regulation changes, or a list of available publications. Similarly, users can send information, requests, and questions to DTSA through the ELISA mail system.

Best of all, ELISA's software cost $8 using public domain bulletin board software. It is a low-cost, efficient way to be totally transparent to exporters.

ELISA 2 is currently being developed, to provide exporters even more, in-depth information on exporting and technology security. That remote bulletin board's telephone number is (202) 697-3632.

For those businesses unable to use the computer bulletin board, DTSA's Directorate for Industrial and Governmental Liaison (I&GL) will provide a status check on their export applications over the phone. Businesses needing a status check can call the I&GL office at (202) 697-7840. The I&GL staff will use ELISA to check the status of the application and call the requestor with the information. I&GL receives approximately 35 such requests each week.

FIGURE 14

DEPARTMENT OF DEFENSE
EXPORT LICENSE STATUS ADVISOR

ELISA—(202) 697-6109

REMOTE ELECTRONIC BULLETIN BOARD

OPERATES 24 HOURS DAILY
(EXCEPT 7-10 AM MON-FRI EASTERN TIME)

300 OR 1200 BAUD, NO PARITY, 8 DATA BITS, 1 STOP BIT

FOR INFORMATION ON EXPORT LICENSE APPLICATIONS FILED UNDER THE EXPORT ADMINISTRATION ACT OR THE ARMS EXPORT CONTROL ACT BEING REVIEWED BY THE DEFENSE DEPARTMENT

CALL ELISA
(202) 697-6109

The status of export license applications referred to the Department of Defense by the Departments of Commerce and State is available on-line via a remote electronic bulletin board system.

The system, known as ELISA, for Export License Status Adviser, is operational 24 Hours Daily

Upon accessing the system via the telephone number above, instructions on its use are provided. No proprietary data is displayed, only the following:

APPLICATION NUMBER	DATE RECEIVED	DATE CLOSED	STATUS OR ACTION

Callers must have the export license application number assigned by the Department of Commerce or State in order to access information. Dates and status provided refer only to processing within the Department of Defense.

The bulletin board also displays other information useful to exporters such as new publications which may be available.

ELISA provides instant information, is updated daily and operates on 300/1200 Baud, no parity, 8 data bits, 1 stop bit.

Let your computer talk to DoD—Call ELISA!

Department of Defense
Trade Security Policy
Washington, D.C. 20301-2600

B. Open Door Policy

DTSA formally initiated its open door policy in 1985, soon after the Defense Technology Security Administration opened the Technology Security Center at 1221 Fern Street (just two blocks from the Pentagon). As part of our goal of complete transparency in operations, DTSA and its operations are open to the exporting community and other interested parties.

A large number of visitors have toured DTSA headquarters, been briefed on current operations and plans for the future and met with the directors and staff. DTSA is proud of its operation and eager to show it off to Congress, the exporting community, representatives of foreign governments, and the press.

We welcome such visits and, as part of the outreach program described in Chapter VII, are planning more. We do, however, prefer to conduct tours and briefings for groups rather than individuals since these take time from export license processing and related functions. Such visits may be arranged through the Industrial and Governmental Liaison Directorate, DTSA, Pentagon 4C761, Washington, DC 20301-2600, phone (202) 697-7840.

VII. WORKING WITH INDUSTRY

A. Awareness

The first step in slowing the Western technological subsidy of the Soviet military is to increase both government and private sector awareness of the problem. Those responsible for technology security at the Department of Defense recognized this early on in this Administration's tenure and established an industrial and governmental liaison office to meet that need. Now a directorate in the Defense Technology Security Administration, Industrial and Governmental Liaison (I&GL) spearheads the awareness mission in which all DTSA personnel and many others in the DoD technology security family participate.

The Secretary of Defense's release of the publication, Soviet Acquisition of Western Technology: An Update, in September, 1985, gave the awareness program a major boost. The white paper, which was the work of the 22 government agencies involved in the Senior Interagency Group on Technology Transfer, is described in Section III. Its presentation of the Soviet acquisition program is a thorough exposition of the need for the U.S. government's efforts in technology security. It continues to garner a great deal of attention in the press and more than 30,000 copies have been printed and disseminated around the world. The pace of requests for the white paper has not slowed.

Public awareness has also been improved through industry briefings. I&GL developed the briefing, variations of which were delivered to hundreds of people in 1985. Figure 15 is a partial listing of the types of audiences reached. Although tailored to the specific audience being addressed, the basic outline of the briefing is the following:

- National Security Importance of the West's Technological Lead
- Soviet Threat to the Western Technological Lead
- U.S. Government Program to Counter the Threat
- Need for Industrial/Public Commitment

There are other aspects to industrial liaison. In 1985 these other aspects took various forms. For example, in November we hosted an interagency technical meeting with representatives of the member companies of the Semiconductor Equipment and Materials Institute, (SEMI) Inc. Industry representatives presented a mini-tutorial to bring our technical staff up to date on the state of the art in lithography, ion implantation, sputtering and coating, and other technical areas. Government representatives discussed export controls on the type of technology cited above, particularly in terms of policy toward the People's Republic of China. Industry representatives

came away with a better appreciation for government security concerns in these areas. There continues to be some disagreement, however, on the levels of technology being controlled, particularly on foreign availability issues.

This first technical meeting having been such a success, we are planning similar meetings in other critical technical areas in 1986.

We also sought industry input on our awareness briefing as it was being developed. In January 1985 we hosted a pilot briefing for selected industry representatives to obtain their feedback on a new, improved version of the briefing on the Technology Security Program. The feedback from industry representatives was important in making our basic presentation more effective. Most of the suggestions presented during the pilot briefing, and since then, have been incorporated into the final product.

Since it is vital that we in the government are aware of what our colleagues are doing, in 1985 we conducted several types of intra-DoD briefings to keep our own "family" aware of the importance and extent of the DoD Technology Security Program. For example, I&GL briefed two classes of Naval Investigative Service Investigators. These are people who, in turn, brief Navy contractors on technology security matters. Senior officers from the staff of the Army Deputy Chief of Staff for Operations were also briefed.

Several intra-US Government briefing sessions were held to make our non-DoD government "family" aware of the importance and extent of the DoD Technology Security Program. For example, in June we briefed a class of the Government Affairs Institute (GAI). GAI, run by the Office of Personnel Management. provides a series of classes for mid-level managers in all U.S. government departments and agencies.

I&GL also briefs U.S. government officials posted overseas. We briefed the incoming Science and Technology Counsellor to US Embassy Budapest and participated in technology security policy discussions during the Strategic Trade Officers' Conference in Tokyo in October. The participants were US embassy officials from posts in the Far East. We plan to brief as many Department of State and Department of Commerce personnel going to foreign postings as possible in 1986 because our own people need to be very familiar with our policies in this area while serving abroad.

Our awareness activities also include the scientific community. In December, we briefed participants in the Outlook on Issues in Science and Technology, a conference for government executives sponsored by Brookings Institution. Participants were principally government scientists, including many from the military services.

FIGURE 15
1985
TECHNOLOGY SECURITY BRIEFINGS AND PRESENTATIONS
(In Washington Unless Otherwise Noted)

08 Jan	Senate Armed Services Committee
08 Jan	Singer Marketing/Government Relations Group
10 Jan	Irish Government Export Control Delegation
10 Jan	First Secretary, Australian Ministry of Defense
11 Jan	Industry Group (Electronic Industries Association, National Security Industrial Association, American Defense Preparedness Association)
16-17 Jan	Second Annual West Coast Meeting, National Security Industrial Association, Beverly Hills
24 Jan	IBM Executives, Boca Raton
29 Jan	Naval Investigative Service Class
30 Jan	Boeing Company Executives
31 Jan	Senate Banking Committee
01 Feb	American Electronics Association Meeting
11 Feb	Inspector General Staff
13 Feb	Swedish Industrialists Group
20 Feb	Chief of Naval Operations Staff
20-22 Feb	Pacific Symposium
26 Feb	Dutch Parliamentarians
27 Feb	Head of Trade Relations, Ministry of Foreign Affairs, UK
12 Mar	Semiconductor Industries Association
12 Mar	Assistasnt Secretary, Australian Department of Foreign Affairs
13 Mar	German Industrialists
15 Mar	ITT Gillfian Executives
25 Mar	National Contract Managers' Association Meeting
25-27 Mar	Japanese Government Officials, Tokyo
27 Mar	UK Parliament Defense Committee
01 Apr	Swiss Minister of Defense
01 Apr	FRG Minister of Defense
02 Apr	National Security Industrial Association
15 Apr	South Korean Businessmen's Group
16 Apr	Department of Commerce Export Conference on Licensing
19-26 Apr	UK Export Control Team
22-23 Apr	Spanish Government Officials
29 Apr	Raytheon Marketing Executives
01 May	Canadian Defense Attache
01 May	Congressman Purcell
08 May	Group of South Korean General Officers
20 May	American Association for the Advancement of Science, National Convention
23 May	American Society for Industrial Security Meeting, Boston
28 May	Naval Investigative Service Class
03 Jun	Norden Systems Executives, Melville, NY and Norwich, CT
03-04 Jun	Norwegian Ambassador
13 Jun	Industry Coalition on Technology Transfer
18 Jun	Financial Times Seminar, London

TECHNOLOGY SECURITY BRIEFINGS AND PRESENTATIONS
(In Washington Unless Otherwise Noted)

(Continued)

24 Jun	Consultant to Australian Minister of Defense
25 Jun	Government Affairs Institute Class
25 Jun	Department of Commerce Aerospace Industry Meeting
26 Jun	Strategy '85 Conference
01 Jul	Norden Systems Executives, New Hampshire
02 Jul	Department of the Army Deputy Secretary for Operations
17 Jul	American Electronics Association Meeting, Palo Alto, CA
18 Jul	Semiconductor Equipment and Materials Institute, Inc. Meeting, Mt. View, CA
19 Jul	Symposium on National Security, McClellan AFB, CA
29 Aug	U.S. Science and Technology Counsellor, American Embassy Budapest
29 Aug	Institute for Sino-Soviet Studies Seminar, George Washington University
06 Sep	Australian Defense Industry Attache
10 Sep	Aerospace Industry Sector Advisory Committee Meeting
12 Sep	U.S. Chamber of Commerce Meeting
16 Sep	Navy Staff College, Foreign Students Class
18 Sep	Press Conference
23 Sep	LAM Research Executives
24 Sep	Digital Equipment Corporation Executives
26 Sep	Voice of America Appearance
26 Sep	Executive Leadership Seminar on U.S. Trade Policy, Brookings Institution
26 Sep	Litton Company Executives
26 Sep	International Business Council Meeting
01 Oct	Canadian Business Council Meeting
01 Oct	Benelux Desk Officer
12 Oct	Claremont McKenna College Students Class
12 Oct	U.S. Naval Academy Class
15 Oct	House Foreign Affairs Committee Staff
16-18 Oct	American Society for Public Administration Conference, Monterey, CA
17 Oct	Naval Postgraduate School, Foreign Officers' Defense Management Class, Monterey, CA
20-23 Oct	Strategic Trade Officers' Conference, Tokyo
29 Oct	South Korean Business Group, Brookings Institution
29 Oct	Chairman, President's Export Council's Subcommittee on Export Administration
30 Oct	EASCON Conference
04 Nov	Marine Resources Co., Inc. Executives
06 Nov	Austrian Government Export Control Team
06 Nov	International Management Development Institute Seminar
07 Nov	GTE Export Policy Seminar
07 Nov	President's Export Council's Subcommittee on Export Administration Meeting
19 Nov	Garrett Corporation Executives
20 Nov	National Security Industrial Society Meeting
21 Nov	German Business Group
25 Nov	Semiconductor Equipment and Materials Institute, Inc. Meeting

TECHNOLOGY SECURITY BRIEFINGS AND PRESENTATIONS
(In Washington Unless Otherwise Noted)

(Continued)

26 Nov	International Business Council Meeting
05 Dec	Department of Commerce Conference on Marketing in the Pacific Basin
09 Dec	AMPEX Company Executives
12 Dec	Outlook on Issues in Science and Technology, Conference for Government Scientific Executives
19 Dec	National Academy of Sciences Hearing
20 Dec	Foreign Service Institute Class
21 Dec	American Society for Industrial Security Meeting
22 Dec	Institute for Foreign Policy Analysis, Conference on the U.S. and the Sale of Defense Products to the Third World

Again in the area of in-house awareness, we have provided a considerable amount of input on technology security issues to Department of Defense documents and publications including the Secretary of Defense's Annual Report to the Congress, the Research and Engineering Posture Statement, Soviet Military Power, and Defense Guidance.

The electronic bulletin board system known as ELISA described in Section VI has created a great deal of goodwill with the exporting community as has our telephone back-up to ELISA. Callers frequently tell us that few government officials have been as responsive to their questions as we.

In 1986 we are planning to expand our awareness program, to increase our outreach to trade associations.

In the field of internal awareness, we want to continue briefing classes of the Defense Investigative Service, Naval Investigative Service, the Customs Academy and other similar schools. We also want to put technology security on the curriculum of the service staff schools and the National Defense University. This is well worth the effort since they train not only our own future general officers, but also those of many friendly countries.

Our liaison with officials from other governments increased in 1985 as well. The export control personnel exchange program continued with visits from Irish, British, and Austrian representatives. Under the personnel exchange program, working level export control officials from friendly countries visit with DTSA and other U.S. government agencies involved in the export control process for a few days with a reciprocal U.S. visit in their country later. Much practical information is exchanged during these visits and a better understanding of "how the other guy does it" results. In addition, the personal rapport established is beneficial for both sides. This program will continue in 1986.

B. Publications Available

We have a number of publications which describe various aspects of the Department of Defense's Technology Security Program. These are available to the general public for the asking. When a new publication is printed, we announce it on the electronic bulletin board system, ELISA. ELISA customers may request copies by leaving a message on the electronic bulletin board.

VIII. INTERNATIONAL EFFORTS IN TECHNOLOGY SECURITY

A. COCOM

1. The Ongoing List Review

a. Goals

There are a number of major goals that are being pursued in the COCOM list review. Efforts are underway to maintain the vigor of the process by means of technically sound and thorough evaluation of other members' proposals. Where they have merit, and where changes can be made in controls that accommodate other members' concerns at no loss to our national security, the U.S. has tended to accept them or modify them enough to be accepted. Efforts are also underway to strengthen the existing controls on items such as superconducting materials and metals, computer software, super-precision measuring equipment, photosensitive devices, acoustic wave devices, electronic materials, lasers, recording equipment, power sources and microwave components. We have an additional goal of securing control of other sensitive technology, such as coating processes, substrates and coating materials of a strategic nature by introducing new list items.

b. How It Works

In the Multilateral Coordinating Committee on Export Controls, COCOM, it takes unanimous approval to make any type of change to the list of controlled items. The participating countries take the entries that are scheduled for review during the year and internally staff them to their experts for analysis. We do the same. Out of this process are generated the proposals for adding new items for control, for changing existing control entries or deleting existing control entries that are no longer necessary.

The review process at COCOM is divided into two rounds with the first running from October through February and the second from April through July. The first round allows the proposing country to present the proposal for revision by the others. At times, bilateral discussions are held which allow the participants to go back for further investigation if agreement is not reached. In round two the delegations come back with new instructions for final negotiation. If agreement is not reached then the proposal is deferred.

COCOM finished the last of the list review negotiations in the Spring of 1985 under the previous three-year cycle. That type of review necessitated a grueling schedule endured by all COCOM countries' technical experts of back-to-back negotiations and did not allow COCOM to rapidly respond to the development of new technologies which might require control. This situation has changed, as a result of U.S. persuasion, to a more timely appraisal of products and technology which, if exported to the Eastern Bloc, would enhance the military build-up underway in

those countries. The new approach is a continuous, four-year segmented review with one fourth of the listed items being reviewed each year. Flexibility is built-in, however, to allow the entry of critical, new strategic technologies into the system on a timely basis if required.

The first segment of the new segmented list review started in Paris in the Fall of 1985 and continued through July 1986. In most cases the process of identifying the need for new controls and of drafting proposals began up to a year before any negotiations started. Preparatory work in the U.S. begins with the Militarily Critical Technology List Technical Working Groups (mandated by Congress) in which strategically critical technologies, keystone equipment, products and materials are identified. The strategically critical items' technical parameters and limits are established by the COCOM Technical Task Groups (TTGs) where the U.S. COCOM proposals are developed. The Department of Commerce, through its participation in the TTGs, provides U.S. industry impact assessments by coordinating the proposals with the Technical Advisory Committees (TACs), which consist of industry technical representatives. These technical proposals are then reviewed, amended and finalized at the inter-agency Working Group 1, chaired by the Department of State. After agreement is reached in Working Group 1, the proposal becomes the U.S. government's negotiating position. A team of policy and technical experts (usually drawn from the groups which developed the proposal) is assembled to negotiate the U.S. government's position at COCOM.

In 1985 there was a major effort by other COCOM countries to further participate in the list review process by submitting substantial numbers of proposals for bringing items under control or proposals for the modification of control levels.

c. Recent Agreements

In 1985, the COCOM countries approved significant new coverages in important areas.

Nautical Items

An array of equipment and technologies was added to the COCOM list, including important items such as small waterplane area twin hull (SWATH) vessels, submersibles, underwater vision systems, underwater life support systems, hull penetrators, underwater positioning systems and underwater manipulators.

Computers

The computer items, long considered the most difficult and complicated to control of all the embargoed items, account for more than 50 percent of all export license appplications. COCOM agreement on new multilateral controls for these items represented a significant achievement.

For the first time, low-level computers of limited strategic concern are now free from embargo, enabling American industry to compete with other Western countries on an equal basis. At the other end of the spectrum, ruggedized computers, superminis, and large mainframes will be uniformly embargoed by COCOM.

A major breakthrough at COCOM was achieved in the control of computer technology. It had been prior practice to decontrol the technology to produce an item when that item itself was decontrolled. As a result of the list review, the technology for making some unembargoed computers remains embargoed. The reason behind this is that the technology to produce some items is more valuable to the Soviets than the item itself, and the same technology can be used to build larger, reliable computers.

Communications Switching

More than 90 percent of the strategic and national command authorities' communications in the continental U.S. is transmitted via commercial equipment and systems. Communication networks designed especially for strategic communications commonly use off-the-shelf commercial switching equipment with enhanced software and interface capabilities. The export of significant quantities of computer-controlled communications switching systems to the Eastern Bloc for modernization of the "civil" communications base would undoubtedly provide considerable command and control benefit to military users.

Switching agreements concluded in 1985 include a total prohibition on wide area packet switching equipment; abeyance until September 1988 of exports of terminal and transit switching systems; and capability limitations on digital, time division PABX systems which significantly reduce their potential for strategic use.

Software

The new COCOM agreement defines software as a commodity, not as technical data. As a commodity, it is for the first time brought under explicit COCOM embargo. This places US software houses on an equal footing with European and Japanese companies.

The vast majority of existing commercial software is now free from control, including all of the commonly used business software. Only certain limited types of software applicable to military programs and command networks are embargoed by COCOM.

Microelectronics

Microelectronics is the basic building block of computers and is a critical technology in many advanced military applications. In this area, the United States and its Western allies have a commanding lead.

The indexing scheme that was implemented in the 1980 list review negotiations was discarded in 1984. It was replaced, in 1985, by controls based on existing Soviet capabilities in microelectronics manufacturing. The 1980 indexing scheme is a good example of how shortsighted the West was about Soviet military objectives in the 1971-1981 time period. Indexing microelectronics was tantamount to assisting the Soviet military to obtain parity in this vital field whose application ranges from strategic to tactical systems.

Robotics

Robots and associated technology were brought under export control for the first time in January 1985 after a three-year period of negotiation. Advanced robotics is considered a critical technology with applications in military and defense-industrial sectors. The export controls apply to robots with general purpose industrial applications and with specialized military missions. The embargo also includes the controllers, related software and certain specialized equipment pertaining to robot systems.

Air Traffic Control

COCOM recognized the significance of the relationship between air traffic control systems (ATCS) and air defense systems (ADS). In general, both ATCS and ADS have the same generic make-up: radars (long range and short range), control centers with corresponding hardware and software, and a netting system. Agreements were reached on the control of radars, based on their value to the air defense role. In the computer sections of the COCOM agreements, both hardware and software limitations were placed on the types of computer equipment and networking that could be associated with ATCS. Most critical to the operation of ATCS is the speed of the computers and the type of software used for control networking.

2. Evolving Policy Toward the People's Republic of China

During the spring and summer of 1985, the Department of Defense played a leading role in negotiating a China Control List with our COCOM partners. As a member of an interagency team, DoD policy and technical representatives travelled to COCOM capitals and labored through five weeks of negotiations in Paris to forge a final agreement. This agreement placed China on an extremely favorable footing, compared with the Warsaw Pact countries, for receiving high technology exports from the West and Japan. In all, 27 categories of technologies, including computers and microelectronics, have been made available to China on roughly the same basis as exports to other non-allied countries. These exports will be subjected to national licensing with only statistical reporting to COCOM. China, for its part, is required to provide exporters with a written import certificate verifying that the government of China has authorized the import. This is to ensure that goods intended for China are under government authority

and will not be diverted. It is expected that up to 50 percent of current high technology trade with China will fall under the new list and procedures.

At the conclusion of COCOM agreement on China, it was understood that COCOM will periodically review the China list.

3. DoD Representation at COCOM

Through the years it has become increasingly obvious that there was a legitimate need for a Defense Department representative to be permanently established in the U.S. COCOM Delegation. A DoD representative is needed to coordinate Defense positions on a wide array of issues related to the COCOM List Review.

It is expected that during 1986 the DoD representative will be assigned to the Organization for Cooperation and Development (OECD) in Paris. OECD hosts the US delegation to COCOM.

4. COCOM Modernization Efforts

a. The COCOM Secretariat

The COCOM modernization drive, sponsored by the U.S., made considerable progress in 1985. The COCOM budget was increased to help accommodate a larger, formally organized Secretariat staff. The new COCOM chairman, Mr. Raineri Tallarigo, of Italy, supports the modernization effort. In addition, a professional data base manager joined the Secretariat staff in 1986, advancing the automation upgrading efforts. Other additional staff positions include translators, a case processing administrator, a librarian and security administrator. These improvements can be attributed to the efforts made by the Department of Defense.

b. Automation Efforts

Through a grant from the Department of Defense, COCOM received a new computer system with a number of terminals and two large memory storage disk drives. A special computer room was also constructed to house the computer equipment. Additional efforts sponsored by the Department of Defense resulted in the development of customized software to enable the Secretariat to efficiently process COCOM cases, the weekly agenda, personnel matters, as well as to track the List Review negotiations. For the first time, it will be possible for countries to submit their exception requests to COCOM on a computer-compatible medium, such as floppy diskette. This will save time by eliminating the paper system currently used in the COCOM secretariat. For example, if the Department of Commerce were to take advantage of this system, instead of taking weeks for cases to reach COCOM and further weeks to process them in the COCOM system, it could take as little as a few minutes to transmit electronically US license requests to the COCOM computer.

Finally, thanks to the Department of Defense's initiative, the COCOM meeting rooms will soon be upgraded. Plans involve the remodeling and enlargement of the present conference room. A microphone and speaker/headset system will soon be added to the conference room as well. This will provide simultaneous translations during negotiation sessions.

5. COCOM AND NON-COCOM COUNTRIES

In 1985, the COCOM countries agreed to seek comprehensive trade security arrangements with friendly, non-COCOM nations that produce sensitive goods or are the site of diversion attempts. While details of approaches to these "third" countries are kept confidential, it can be said that this unique, multilateral effort to bring non-COCOM countries into the Free World's technology security family is successful.

B. Bilateral Technology Security Agreements

1. India

Outside of the COCOM arena, and in the wake of the National Security Directive on India, substantial changes in US-India relations were made in 1985 in the areas of defense cooperation and sales of military and dual-use equipment and technology. Following agreement on a US-India Memorandum of Understanding (MOU) on technology transfer in November 1984, the two governments successfully negotiated a follow-on agreement in 1985 to implement the procedures delineated in the MOU, together with assurances regarding nuclear and missile applications. Completion of these agreements resulted in immediate release of a large number of technologically advanced exports. Another milestone was reached with the establishment of mission area discussions between defense establishments of the two countries with the goal of increasing military cooperation and sales of military equipment and technology. A DoD technicial delegation visited India in early 1986 to explore specific areas of cooperation.

With the conclusion of the government-to-government agreements, sales of controlled dual-use technology surpassed the $1.2 billion mark in 1985. DoD processed more than 3,000 Indian cases in 1985, with an approval rate of 92 percent.

Of note were DoD's efforts in paving the way for the first coproduction agreement with India for the manufacture and distribution of computers.

2. U.S./Canada Agreement on Protection of Strategic Technical Data

The President of the United States and the Prime Minister of Canada, in a joint declaration made at the Quebec Summit in March 1985 agreed to strengthen cooperation in exchanging and protecting strategic technology.

A memorandum of understanding concerning the exchange of sophisticated technical information has been negotiated and formalized through diplomatic channels. This memorandum is unique in that it will facilitate access to unclassified strategic technical data of both countries for qualified contractors from each country on an equally favorable basis. This memorandum also pledges each government to ensure that effective and appropriate controls and enforcement mechanisms are in place to protect the information exchanged.

Moreover, and perhaps most important, the memorandum provides for a common, jointly staffed system for certifying participating contractors in each nation. This procedural framework will, in our judgement, stimulate further cooperation between our respective defense industries and our military acquisition establishments.

IX. MODERNIZING THE EXPORT CONTROL PROCESS

In spite of the many improvements we have made in the U.S. export control system in the past five years, there is no doubt that it is in need of an overhaul. As it presently stands, it is too cumbersome and it fails to achieve its main objective to weed out those who dishonestly trade away our high technology to the Soviet Union, the Warsaw Pact countries, or nations hostile to the United States--for example, Libya and Nicaragua.

Many ideas have been put forward which are aimed at improving the existing export licensing system. Most of these proposals seek to "shorten" the export control lists. Some add that the list should be focused even more on "technology" and manufacturing know-how rather than products, on the theory that controlling technology better safeguards national security. Others propose to do away with licensing among the COCOM countries; to set up a special "fast track" for reliable companies or to expand the system of Bulk and Distribution Licenses. Virtually all serious proposals--many of them containing one or more of the ideas mentioned here--argue that a "streamlined" export control system will be more enforceable. Most serious students of export controls favor increasing the penalties for those who violate the export control laws.

To achieve a more efficient, purposeful and effective system the United States Government as a whole must take a number of necessary steps. Among the domestic changes that ought to be initiated right away are the following:

- Creation of a fully integrated automated data processing system linking all the agencies involved in export control

- Adoption of a new system of warranted end-users of American and COCOM countries' technology

- Extension of the warranted end-user system to friendly countries where a sufficiently strong enforcement system is in place and there is the political will to use it

- Compilation of a single list of controlled technology to be treated as "war material"

- Annotation of the control list to describe to the public the reasons why a technology or product is included on the control list

Each of these proposals warrants further elaboration.

Automated Data Processing

At the Department of Defense we have demonstrated that automated data processing can vastly improve the export licensing system. Now that our automated system is in full operation, the

average age of the dual-use export license applications in the system is less than 20 days. This is a tremendous improvement over the situation some years ago when license applications would languish for month upon month in the Department of Defense without resolution.

Obviously, automation alone will not assure discipline in the export license system. But it is possible to fold a number of effective management tools into the automated system in order to get the desired results: rapid turnaround and thoughtful, responsible review.

In the Department of Defense our automated system now includes a number of databases and, as described elsewhere in this report, we are working toward integrating these into an improved system that can be queried by the action officer processing a license application. We believe that this will improve the consistency of license review and assure checks and crosschecks on data being evaluated.

To improve the system across the board, the first logical step is to extend the automated system to all the export control agencies and, in the future, to link it directly to COCOM. While this is an expensive undertaking, it would be cost effective for both government and for industry. Export licensing would be speeded up, thereby reducing the cost of licensing to American companies, while its efficiency would help assure that America does not lose export opportunities to competition from abroad. Additionally, government would quickly recoup the investment in such a system by the increase in tax revenues resulting from export earnings.

A properly integrated system will assure that enforcement authorities can immediately check whether an item crossing a border point is correctly identified and has a proper export permit. A link to a fast scan system, such as bar codes (which, today are used to label everything from soup to nuts), will allow Customs inspectors in every country to identify items legitimately in transit. This can have the result of minimizing unnecessary detentions of goods and making the work of the "techno-bandits" much more difficult.

A modern automated data processing system would integrate fully intelligence information and police data to aid in the enforcement effort and help make it impossible for the Soviets and others to operate front companies and play other shell games on a wide scale. Our automated system for review of West to West license applications has such characteristics. With it we have been able to detect a number of obviously phony end-users in a remarkably short period of time. Over the course of the next few months we expect to perfect this system. Such a system should be an integral part of a fully automated export license system across the government.

Similarly, firms should be able to submit license applications electronically and receive authorization in the same manner.

Such a possibility is at our doorstep and could be a way to ease the paper burden.

Certified End-Users

Automation is not the solution to all problems. The Department of Commerce is processing between 140,000 and 150,000 validated export licenses each year. Many of these "individual" permits are individual only in name. Warehouses are being filled based on single validated licenses. Add to these the genuine bulk licenses and distribution licenses and it is rapidly clear that the system cannot function well under such demand.

There is no sound reason why certain customers who regularly buy U.S.-made equipment must, each time, be cleared by the system. Many customers are 100 percent reliable. It does not make sense that the export of computers to an established firm such as Volkswagen in West Germany must receive a separate permit in each instance. In addition, West Germany is a COCOM member and can be relied on to share our national security concerns.

Working with us, the Department of Commerce recently issued draft regulations for a new type of license based on this concept After a 60-day comment period, Commerce may amend the draft regul tions prior to putting them into effect.

In order to be certified as reliable end-users, foreign entities would have had to have proven their reliability and cooperativeness over time. The certification, then, would be a form of special treatment that will allow them more expeditious access to U.S. technology. A U.S. company exporting a national security-controlled item to a certified end-user would not have to apply for an individual validated export license; he could simply ship on the strength of the certification because the certified party would have agreed in advance to protect the equipment and technology.

Such an approach has the virtue of rewarding those who deserve rewards rather than simply handing out export permits in a shotgun approach, hoping for the best. Most firms--in the United States and abroad--are honest and reliable. Accordingly, they should get top treatment and not have to be delayed. In addition, the certified end-user system will reduce the burden on the Department of Commerce and other agencies substantially allowing us to focus our scarce resources on the difficult, precedent-setting cases rather than on the routine.

A Single List of Export-Controlled Items

Such an approach is far superior to the idea of "reducing" the control lists. Reducing the lists implies controlling fewer items rather than improving the licensing system and its enforcement.

The problem is that the control list is not, and has never been, an actual list of items. It is, more accurately, a list of

technologies and technological products defined by performance. The number of items "caught" by the control list varies, therefore, on a daily basis, depending on what is being produced. In addition, the control list we use is, by and large, negotiated internationally. Often it is already refined and aggregated. Certainly, any list can be changed--but most of the changes that can be contemplated are not going to either reduce the export license burden in any massive way or improve the enforceability of the embargo in a demonstrable manner. This is not to say we should not press ahead in refining and improving the list and aiming it as accurately as we can on items of the most importance to our national security and the security of our friends and allies.

X. OTHER ISSUES

A. The 1985 Amendments to the Export Administration Act of 1979

After several years of deliberations, the Export Administration Act of 1979 (EAA) was reauthorized with amendments during the summer of 1985. The amendments were achieved with broad congressional support, interagency collaboration, and private sector cooperation.

The Department of Defense plays an integral role in the administration of Section 5, National Security Controls, and related sections, of the amended EAA. Other changes supported by the DoD include the provisions for strengthening enforcement, increasing the penalties for violations, upgrading the operations of COCOM and streamlining the licensing process.

Controlling Technology Transfers to Embassies and Affiliates of Controlled Countries

As was documented in "Soviet Acquisition of Militarily Significant Western Technology: An Update," released by Secretary Weinberger, September 1985, the United States faces a very well organized and motivated effort by Warsaw Pact Governments to acquire advanced technology within the United States. In anticipation of the public release of the report, EAA Section 5(a)(1) was amended to provide the US Government with the express statutory authority to control the transfer of goods or technology "to embassies and affiliates of controlled countries" located in the United States. This closes a very dangerous legal loophole through which high technology had passed.

Moreover, the Administration recently moved by regulation to tighten the travel privileges of East European personnel. This regulatory change was made after the October 1985 hearings on Warsaw Pact technology espionage operations conducted in the US before Senator Roth's Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs. The Department of Defense significantly contributed to the progress made in House hearings through the testimony of Mr. Richard Perle, Assistant Secretary of Defense for International Security Policy, who argued in favor of strict numerical parity of diplomatic representation between the United States and members of the Warsaw Pact Treaty Organization.

Factors for Determining the Composition of the List of Controlled Countries

Section 5(b)(1) was amended to provide for more diverse grounds to justify including a country on the list of countries to which exports are controlled for national security purposes. While the President retains the discretion to consider "other

factors" he deems "appropriate," the grounds have now been broadened to specifically include "nuclear weapons capability," compliance with multilateral nuclear weapons agreements, and "the extent to which the country's policies are adverse to the national security interests of the United States." This reconfirms and broadens the pre-existing statutory authority to apply national security export controls to non-Warsaw Pact states for reasons other than East-West relations.

Elimination of Licensing Requirement for Export to COCOM Members

The amendment to Section 5(b)(2) eliminated the licensing requirement to COCOM members for goods and technologies subject to the Administrative Exception Notes (AEN) of the COCOM International Control List. Exporters can identify AEN goods and technologies as they are accompanied by the following language in the "Notes" to the Export Administration Regulations (EAR), Part 399.1 of the Commodity Control List:

> "Licenses are likely to be approved for export to satisfactory end-users in Country Groups QWY. . ."

This new procedure will allow for greater speed and predictability for the sale to COCOM countries of technologies and goods which are not of the gravest concern. These AEN goods and technologies, however, remain militarily critical and as such are still controlled for export to members of the Warsaw Pact.

Negotiations with Non-COCOM Countries

Section 5(k) was amended to specifically allow the United States government to grant COCOM-like treatment, e.g., Sections 5(b)(2) and 10(o), to non-COCOM members with whom the United States has negotiated "agreements on export restrictions comparable in practice to those maintained by the Coordinating Committee." It is hoped that this provision can be used as a powerful incentive for non-COCOM countries to develop with the United States and other COCOM members effective export control agreements to facilitate international trade in high technology between and throughout non-controlled countries. This "Third Country Initiative" is considered to be one of the most important non-COCOM policy objectives which the United States has undertaken. We have enjoyed considerable success to date but are determined to continue building an international system of interrelated bilateral and multilateral export control agreements.

Export to Members of COCOM

Section 10(o) was added to the EAA to provide for shortened licensing times and automatic approval for legitimate high technology trade with members of COCOM. The licensing deadline for the U.S. Government to issue an individual validated license

was shortened to fifteen working days after receipt of the export license application by the Department of Commerce, with the potential for an additional fifteen working days where more time is required to analyze a complex case.

The Role of the Department of Defense in the Export Control System

Section 15(b) was amended to provide for mandatory review by the Secretary of Defense of any proposed changes to the EAR having an effect on national security export controls. It is recognized that export controls must be flexible to respond to the changing international security environment of the U.S. and our allies. The Department of Defense has the chief responsibility for defending the country. It is wise management, therefore, that the Congress should allow the government to profit on a consistent basis from the national security analyses which the Department of Defense can bring to the administration of the EAR.

Furthermore, the President's Declaration in January 1985 to allow the Secretary of Defense to examine export licenses to certain non-proscribed countries obviated the need for statutory change to Section 10(g). As legislative history, the Conference Report (House Report Number 99-180) clearly supports this interpretation and the previous declaration by the President. The cumulative effect of the amendment Section 15(b), and the Presidential Declaration and legislative history with regard to Section 10(g) firmly establishes the principal that the Department of Defense, as the principal national defense agency, has the responsibility to ensure that the broad national security interests, as defined by the President within the authority of Section 5(b)(1), are properly addressed in the course of administering the export control system of the U.S.

B. Munitions

Now that a year has passed since the revised International Traffic In Arms Regulations (ITAR) has been in place, it is time to review it to refine and clarify the regulations, based on a year's experience in the spirit of improving the regulatory scheme established under the Arms Export Control Act. In the year since the revised ITAR was published, some ambiguities and omissions have been identified by both industry and the Department of Defense. In order to maintain the ITAR's currency and effectiveness, we will work to establish a joint Department of State/Department of Defense team to continually monitor problems that arise and to propose modifications as needed.

C. Emerging Technologies Program

In 1985 the Office of the Deputy Under Secretary of Defense for Research and Advanced Technology inititated a program to develop a directory of emerging technologies with potential military significance. A preliminary list has been developed and is now being evaluated by the Technical Working Groups for possible inclusion into the 1986 version of the Militarily Critical Technologies List (MCTL).

D. Militarily Critical Technologies List (MCTL)

In the 1985 amendments to the Export Adminstration Act of 1979, Congress reaffirmed the need for and the role of the Militarily Critical Technologies List (MCTL). A further statutory requirement was added that each item must be reviewed in terms of foreign availability. Also, control of technology is to be accompanied by a reduction in control of product, a new list of keystone equipment is to be developed, and an assessment is to be made of the impact of listing items on the MCTL. The MCTL continues to be a basic building block of the DOD Technology Security Program.

Significant progress has been made to meet these requirements. The annual review has been formalized with the formation of 30 Technical Working Groups and subgroups consisting of technical personnel from the Military Services, the Defense agencies, the Intelligence Community, and industry to review the list to delete or add items as appropriate. This study has been enlarged to determine what products may be removed from the list as technologies are added. Over 100 technological areas have been reviewed, and significant changes made in the areas of biotechnology, the Strategic Defense Initiative, and composites. A program has been initiated to make the list a more useful document to those responsible for export control license review by identifying the most critical items, linking the items to various weapons systems and developing a series of handbooks, cross-references and indices in this regard.

Steps are being taken to assist with implementation of the MCTL into the Commodity Control List (CCL) and the Munitions List, as required by law. Each item on the MCTL is identified as to where it is controlled or what steps are being taken to accomplish control. Each technical array of know-how is being compared with the export control lists to determine the degree of existing controls and to develop new technical proposals for control if necessary.

An assessment of the impact of critical technologies currently on the list is being prepared in terms of generic technology areas. Initial efforts have begun to identify items for the new category of keystone equipment, as required by Congress.

E. Foreign Capability Assessment Study

The Office of the Deputy Under Secretary for International Programs and Technology is continuing the study of the capability of non-COCOM countries in high technology areas identified in the Militarily Critical Technologies List (MCTL). This study responds directly to the 1985 Amendments to the Export Administration Act which require evaluation of the foreign availability of the MCTL entries. The study is being conducted by the Technical Working Groups. Items for which foreign capability has been established by the Technical Working Groups will be subjected to an independent evaluation by the intelligence community.

F. Soviet Technology and Research Capabilities

Continuing assessment of Soviet technology is made in the course of the MCTL review and in the preparation of technical proposals for COCOM submission. Intelligence support is provided by the Director of Central Intelligence, Defense Intelligence Agency, intelligence resources of the major agencies and the military science and technology intelligence centers.

XI. TECHNOLOGY SECURITY AND THE ARMED FORCES

A. Army

In 1985 the Army concentrated its focus on the Technology Security Program. The application by Army staff (ARSTAF) and major command (MACOM) program managers of an Army technology transfer decision-making structure to the increasing number of Army international programs has proven a success. Technical assessments of these systems have been completed, providing Army leadership with necessary information pertaining to system criticality, sensitivity of production methods involved and other crucial factors that must be considered when weighing the benefits and drawbacks of exporting the systems. This process is illustrated in Figure 18.

The Army reported in last year's Report to the Congress a requirement for developing technical assessments for some 78 major systems. (The 78 were consolidated into a total of 57 in 1985.) Well into that effort, six have been produced thus far as follows:

- M-1
- Stinger
- SINCGARS
- Copperhead
- TOW-2
- AN/TPQ-37

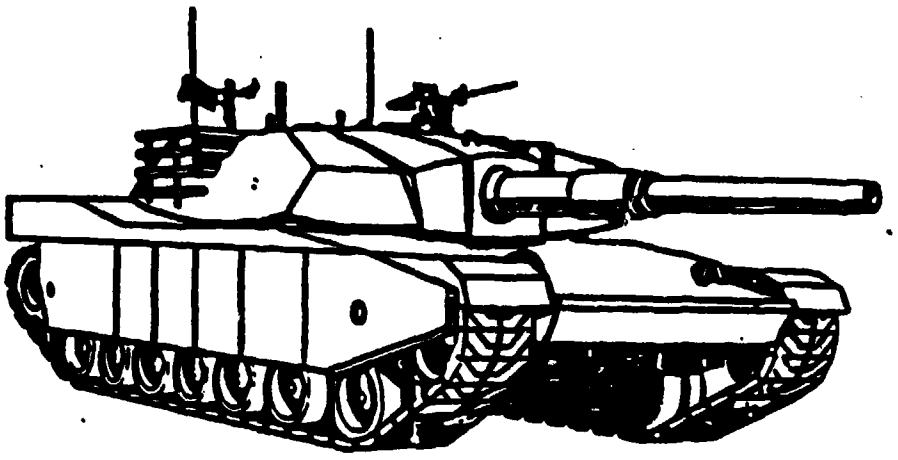
Completion of the remaining 51 is anticipated by the end of 1987.

Continuous review of the decision process has identified an important concept that was previously ill-defined. Although the validity of well developed technical assessments has been demonstrated, they are not an end in themselves. The larger issue involved in decisions to export concerns the incorporation of the technical assessments into a comprehensive disclosure plan. This would enable the Army program manager to identify major subsystems and develop a disclosure schedule that puts potential release to security assistance customers in priority order.

The effectiveness of Army technology security efforts is directly related to the resources dedicated to the program. Last year the Army reported 77 man-years of effort expended on the technology security program by various offices across the Army staff and Army Materiel Command, but only two full-time manpower spaces dedicated to the effort. The Army commitment to the Technology Security Program has resulted in renewed resource efforts in both manpower and in automation. Four civilian and military professional manpower spaces have been added to the Office of the Assistant Chief of Staff for Intelligence, Technology Transfer Division where they perform essential tasks in review of the Militarily Critical Technologies List, COCOM issue resolution,

FIGURE 16

TECHNICAL ASSESSMENTS OF WEAPONS SYSTEMS



The System . . .

- Executive Summary
- System Description
- System Comparisons
  - — Free World-Warsaw Pact
- Controlled Technologies
- Critical Technologies
- Intelligence Factors

Use . . .

- Foreign Military Sales
- Coproduction
- Cross Reference
  - — Militarily Critical Technology List
  - — Commodity Control List

dual-use and munitions license review, National Disclosure Policy management, as well as foreign visits and accreditation issues. Army hopes to have these positions assigned to these tasks on a permanent basis.

Future manpower considerations must address the larger issue of consolidating technology security functions throughout the Army. Accordingly, in compliance with Defense Guidance, Army has introduced a budget initiative to identify 18 professional spaces in support of technology security. If approved, such an Army-wide, cross-headquarters staff will provide an effective operational team to implement national policy in support of technology security.

Developments in automation have progressed significantly as well. The Foreign Disclosure Technical Information System (FORDTIS) has provided Army disclosure managers a tool to track developments in the accreditation of foreign representatives, document and information disclosure to foreign governments, and data tabulation regarding exceptions to National Disclosure Policy for release of classified military information to foreign governments. With the increasing availability of FORDTIS hardware, Army disclosure managers will be more readily able to develop timely, responsive recommendations to Defense leaders regarding technology security imperatives.

Initiatives

Significant Army initiatives have been introduced to enhance the DoD Technology Security Program.

Technology Sharing--In September 1985, the Assistant Secretary of the Army for Research, Development and Acquisition extended fullest support for Secretary Weinberger's initiative to improve the US conventional defense through armaments cooperation. The following issues are taken into account in this regard:

U.S. TECHNOLOGY PROVIDED TO ALLIES
Issues:

- Once released, it is beyond our control
- Each release is calculated risk
- Informed decision
- Case by case assessment of pros and cons
- Codevelopment process
  -- Most efficient
  -- Most vulnerable
- Phased release of information
  -- Not desirable
  -- Not practical

Broadly speaking, the Army is pursuing two parallel and complementary approaches. First is an attempt to revitalize international cooperation in research, development and acquisition of appropriate foreign equipment. The second is a commitment to develop common user requirements with our allies for future

capabilities which can result in common, or at least interoperable, equipment and organizations.

The Army will continue to protect sensitive technology while facilitating technology transfer when appropriate. Army Material Command (AMC) is responsibile for assessing the impact of sharing critical military technology with allies. Recently, the Army Staff established a Technology Control Panel for timely resolution of technology transfer matters. The panel has developed a methodology to facilitate consistent decisions on these issues.

Foreign Military Sales Considerations in the Acquisition Process--Since the Army may not want to release all critical technologies in weapons systems currently being developed, portions of such systems may be developed to meet the needs of an allied nation. The Army Plan, 1988-2002, dated December 1985, which establishes Army guidance states that one Army goal is to "...identify critical technologies which the U.S. would not want to release abroad during the research and development process so the system can be modified to enable foreign military sales without compromise of critical technologies." Army regulations will be modified to reflect this new guidance.

Summary

Army efforts in support of the Technology Security Program have their genesis in the DoD policy initiatives. An effective program balances the quid-pro-quo of security assistance and legitimate needs to protect national security resources. The Army is moving in the right direction in developing the technical assessments that provide the data base for decisionmaking and in implementing the DoD policy to promote effective bilateral and multinational armaments cooperation programs.

B. Navy

1985 was a year of transition for the Navy Technology Security Program. With an increase in the number and complexity of export cases and much shorter deadlines mandated by the Export Administration Act, the Navy expanded its dedicated resources and sharpened its focus to better support the DoD Technology Security Program. Three significant initiatives were taken to strengthen Navy's technology security efforts.

First, and foremost, six new billets were authorized for the Chief of Naval Operations Technology Transfer Policy and Control Division. With the increased manpower, the Navy's capability to review assigned cases within the prescribed deadlines has improved significantly.

Second, although the Naval Material Command (NAVMAT) was disestablished in 1985, the NAVMAT responsibility (and personnel)

for management of the technology security program element was transferred to the Office of the Chief of Naval Research. As a result, continuity of budget ($2.227M representing 22 man-years) and technical support for the Navy's Technology Transfer Program was maintained.

The third initiative was the consolidation of all the various Navy technology security intelligence functions in one location at the Naval Intelligence Support Center, Chesapeake Beach, Maryland. This provides a single focal point for intelligence support for the program.

In addition, the Naval Security and Investigative Command expanded its Technology Security Program training for Naval Investigative Service agents, with the objective of increasing their awareness of real and potential threats to the security of U.S. high technology.

The Navy priority ordering of the Militarily Critical Technologies List (MCTL) reported in last year's report to Congress was continued in 1985 with the completion of the revised MCTL. This effort was expanded in 1985 to include Air Force priority ordering as well. Through this effort, a combined list was created reflecting the most critical technologies supported by both Services.

Another on-going program in which the Navy has played a key role involves the protection, via secrecy orders, of critical technologies disclosed in patent applications.

With a strong commitment on the part of its technology security management and support staffs, and newly strengthened and focused organization, the Navy will continue to provide strong, in-depth, and timely support for the Department of Defense Technology Security Program.

C. Air Force

New Expertise Required

1985 was a year in which the Air Force was confronted with the necessity of having to deal with Third World requests for updates on their existing fleets of aircraft--frequently of Soviet manufacture--as opposed to normal requests to purchase U.S. aircraft with which we are already familiar. Pakistan and China are two good examples of this problem, though others exist. In servicing these requests, USAF technicians have been forced to provide opinions as to whether the requested U.S. equipment was even compatible on a form, fit and function basis with a Soviet manufactured airframe. Other kinds of cases which have opened up are software requests for multitudinous usages, some of which may be releasable and some of which may not be. These new kinds of cases have required special consideration and thought and are indicative of some of the changing problems being faced today in the export licensing field.

1990s Aircraft

The Air Force is witnessing a growing demand for advanced U.S. technology in the aircraft/avionics field, as country after country attempts to come up with its own version of a 1990s fighter aircraft. The Israeli LAVI program was probably the forerunner of this type of situation in which Israel requested access to U.S. composite technology for construction of specified portions of their LAVI aircraft. More recently we have experienced requests from Taiwan for U.S. corporate technological assistance with their Light Weight Indigenous Fighter (LWIDF). India has requested similar assistance for their desired Light Combat Aircraft (LCA) of the 1990s. The avionics suites are probably the areas of most interest to countries such as this as it is probably the hardest area to duplicate by a country which has not built a world leading fighter. Sweden has also shown interest in certain areas for their follow-on to the current JAS fighter. Yugoslavia had indicated an earlier desire for specified U.S. assistance on certain areas of the Orao II. USAF is also beginning to address Japan's needs for the 1990s.

Case Handling

Air Force received a total of 3705 munitions, Commodity Control List (CCL) and Coordinating Committee (COCOM) cases during 1985, a new record which was 13.8 percent over the 1984 total of 3256. The 1985 figure comes out to a total of 706 cases each, for the 5.25 persons the Air Force had in the Munitions and Export Control Section during that year. With a total of six persons on board in that section as of 1 October 1985, our current budget effort is one of converting a temporary position into a permanent one in order to maintain timely processing of incoming cases.

Critical Technology Linkage to System

To date, much of the Air Force specifying and monitoring of critical technologies has been aimed at generic technologies, and little has been done to link identified critical technologies to specific Air Force systems and subsystems. However, in 1985 the Air Force began to cross-index specific Air Force systems components to previously identified critical technologies from the Militarily Critical Technologies List (MCTL). These cross-indexing or linking reports are made available to dual-use and munitions case processors to help them determine relative sensitivity of material subject to export. The first report issued details air-to-air missile critical technologies. Reports to follow will cover electronic warfare, air-to-ground missiles and guided bombs, and software. These topics were chosen as they represent Air Force systems or subsystems subject to sale/export questions or requests.

Air Force Prioritization of the MCTL

During 1985 the Air Force surveyed over 100 of its leading technologists and developed a priority listing of the MCTL based

on relative "need to control" and "ability to control" each item. The Office of Naval Technology and the Naval Research Laboratory, which have performed a similar study, provided valuable assistance to the Air Force study. The prioritized listing will allow the Air Force to concentrate its control, protection, and counter-intelligence resources where they will do the most good. The prioritized listing can also provide guidance that the MCTL does not provide on cases of proposed exports to non-Warsaw Pact countries.

XII. RESOURCE REQUIREMENTS

FY 1987

Personnel

Civilian	84
Military	51
Total	135

Operations and Maintenance Funds	$ 5,255,000
ADP Procurement Funds	2,040,000
Research, Development and Evaluation Funds	1,759,000
	$ 9,054,000

The majority of funding requirements, other than those related to personnel, are to provide for a modern automated system to process export license applications. This system will enhance national security by providing a predictable, transparent and efficient review of export license applications. It will utilize technical data available from government and non-government sources, pertinent data from previous government decisions, as well as national and multi-national control lists to assist in processing applications. This system will, in most cases, produce in days a DoD recommendation that will be electronically transmitted to either the Department of State or Commerce. DTSA and Commerce are developing a prototype system to evaluate the concept of granting, at the time of application, an export license for certain commodities destined to certain end-users.

Department of Defense
DIRECTIVE

MAY 10, 1985
NUMBER 5105.51

ASD(C)

SUBJECT: Defense Technology Security Administration

References: (a) Title 10, United States Code
(b) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984
(c) DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976
(d) Under Secretary of Defense for Research and Engineering, "DoD Militarily Critical Technologies List (U)" (Secret Noforn), October 1, 1982
(e) DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980

A. PURPOSE

Under the authority vested in the Secretary of Defense by reference (a), this Directive establishes the Defense Technology Security Administration (hereafter referred to as "DTSA") and defines its mission, functions, authorities, and relationships.

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Organization of the Joint Chiefs of Staff (OJCS), the Military Departments, the Inspector General (IG) of the Department of Defense, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

C. DEFINITIONS

The terms used in this Directive are defined in enclosure 1.

D. MISSION

1. The DTSA shall:

a. Administer the DoD Technology Security Program to review the international transfer of defense-related technology, goods, services, and munitions consistent with U.S. foreign policy and national security objectives.

b. Ensure the implementation of DoD technology security policy relative to the international transfer of defense-related technology, goods, services, and munitions.

c. Assure expeditious processing of export license applications consistent with national security objectives, making the fullest use of automation and other techniques.

d. Support actively, intelligence and enforcement activities of USG Departments and Agencies to restrain the flow of defense-related technology, goods, services, and munitions to potential adversaries.

e. Provide support to the Under Secretary of Defense for Policy (USDP) and the Under Secretary of Defense for Research and Engineering (USDR&E) in carrying out their responsibilities assigned under DoD Directive 2040.2 (reference (b)).

E. ORGANIZATION AND MANAGEMENT

1. DTSA is established as a DoD field activity under the direction, authority, and control of the Under Secretary of Defense for Policy (USDP).

2. DTSA shall consist of a Director, a Deputy Director, and such subordinate organizational elements as are established by the Director within resources assigned by the Secretary of Defense.

3. The Deputy Under Secretary of Defense for Trade Security Policy in the Office of the USDP shall serve as the Director, with responsibility for overall supervision of the DTSA.

* 4. The USDR&E will select, in consultation with USDP, and provide a staff representative to serve as the Deputy Director, with further responsibility to serve as principal DTSA official on technical matters. *

F. RESPONSIBILITIES AND FUNCTIONS

1. The Under Secretary of Defense for Policy shall:

a. Develop, coordinate, and issue policies relating to technology security.

b. Provide policy direction and overall management for the DoD Technology Security Program in accordance with reference (b).

c. Represent the Department of Defense in interagency, national, and international fora concerning policy for technology security and enforcement matters.

2. The Under Secretary of Defense for Research and Engineering shall:

a. Provide advice and support for the technical aspects of the DoD Technology Security Program in accordance with reference (b).

b. Ensure the technical review of strategic trade, Coordinating Committee of the Consultative Group (COCOM), and munitions export license applications, and establish the DoD technical positions with supporting rationales, regarding the national security implications of the proposed transfer of technology, goods, services, and munitions in accordance with reference (b).

#First Amendment, Ch 1, 1/24/86

c. Provide technical advisors and consultants as needed to support the USDP in the development of DoD technology security policy.

d. Develop and administer programs to identify and define lists of militarily critical technologies that should be controlled for export, including necessary guidelines.

e. Provide technical support of DoD views in interagency, national, and international forums of technology, goods, services, and munitions transfer matters.

3. The Secretaries of the Military Departments shall:

a. Provide technical, intelligence, and operational support of the DoD Technology Security Program in accordance with reference (b).

b. Designate a liaison officer from the service staffs to the DTSA, on a full-time basis, of sufficient rank to facilitate the resolution of matters pertaining to the security of technology, goods, services and munitions.

4. The Assistant Secretary of Defense for International Security Policy shall:

a. Serve as the DoD representative to the Advisory Committee on Export Policy (ACEP) and the Economic Defense Advisory Committee (EDAC).

b. Serve as the DoD representative to the Committee on Foreign Investment in the U.S. (CFIUS).

c. Provide input to the DoD Technology Security Program in accordance with reference (b).

5. The Chairman of the Joint Chiefs of Staff shall:

a. Designate a senior officer from the OJCS to provide operational expertise and military judgment on technology security matters within DoD, interagency, national, and international fora.

b. Provide support to the DoD Technology Security Program in accordance with reference (b).

6. The Director, Defense Intelligence Agency shall:

a. Conduct reviews and provide intelligence support to the Director, DTSA on technology security matters.

b. Provide intelligence expertise on technology security matters for DoD, interagency, national, and international fora.

c. Designate a point of contact to represent DIA on technology security matters.

d. Assist in identifying and assessing critical technology.

e. Provide support to the DoD Technology Security Program in accordance with reference (b).

7. The Heads of DoD Components shall:

a. Assure the prompt processing of export license applications consistent with national security objectives and provide sufficient staff to facilitate the resolution of matters pertaining to technology security.

b. Designate a point of contact in their respective Component for technology security matters.

8. The Director, Defense Technology Security Administration shall:

a. Organize, direct, and manage the DTSA and all assigned resources. Establish subordinate offices necessary to fulfill assigned missions.

b. Periodically review DoD Directive 2040.2 (reference (b)), and other issuances as required, and recommend appropriate changes to the USDP and USDR&E.

c. Supervise, administer, implement and evaluate policies and procedures for the Technology Security Program.

d. Provide support for DoD contacts with foreign governments, international agencies, other federal agencies, interagency groups, industry, and DoD Components concerning technology security matters.

e. Act as the DoD receiving point for all cases concerning technology security including, but not limited to strategic trade, COCOM, and munitions export license applications.

f. Support the development of all DoD positions on COCOM, strategic trade, and munitions license applications.

g. Provide DTSA representation at meetings and deliberations of the International Technology (IT^2) Panel and Subpanels.

G. RELATIONSHIPS

1. In the performance of assigned functions, the Director, DTSA shall:

a. Coordinate actions with other DoD Components having collateral or related functions in the field of assigned responsibility.

b. Maintain appropriate liaison with DoD Components and other governmental and nongovernmental agencies for the exchange of information and advice on programs in the field of assigned responsibility.

c. Make use of established facilities and services in the Department of Defense and other governmental agencies to avoid duplication and achieve maximum efficiency and economy.

2. Heads of DoD Components shall coordinate with the Director, DTSA on all matters relating to DTSA functions and responsibilities.

H. AUTHORITY

The Director, DTSA is authorized to:

1. Obtain such information, consistent with the policies and criteria of DoD Directive 5000.19, (reference (c)), advice, and assistance from other DoD Components as necessary to carry out DTSA programs and activities.

2. Communicate with appropriate personnel in the Military Departments and other DoD Components on matters related to DTSA programs and activities.

3. Communicate with other government agencies, representatives of the legislative branch, and members of the public, as appropriate, in carrying out the functions assigned under this Directive.

I. ADMINISTRATION

1. DTSA shall be authorized such personnel, facilities, funds, and other administrative support as the Secretary of Defense considers necessary.

2. The Military Departments shall assign military personnel to DTSA in accordance with approved authorizations and established procedures for assignment to joint duty.

3. Administrative support required for the DTSA will be provided by the Director, Washington Headquarters Services.

J. EFFECTIVE DATE

This Directive is effective immediately.

William H. Taft, IV
Deputy Secretary of Defense

Enclosures - 1
1. Definitions

DEFINITIONS

1. Critical Technology. Technologies that consist of (a) arrays of design and manufacturing know-how (including technical data); (b) keystone manufacturing, inspection, and test equipment; (c) keystone materials; and (d) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (also referred to as militarily critical technology).

2. Goods. Any articles, materials, supplies, or manufactured products, including inspection and test equipment. The term excludes technical data.

3. Items of Intrinsic Military Utility. End items other than those identified in the "DoD Militarily Critical Technologies List" (reference (d)) whose transfer to potential adversaries shall be controlled for the following reasons:

a. The end product in question could significantly enhance the recipient's military or warmaking capability either because of its technology content or because of the quantity to be sold; or

b. The product could be analyzed to reveal U.S. system characteristics and thereby contribute to the development of countermeasures to equivalent U.S. equipment.

4. Keystone Equipment. Includes manufacturing, inspection, or test equipment and is the required equipment for the effective application of technical information and know-how. Keystone materials have the same significant application.

5. Know-how. Includes both the know-how of design and manufacturing and the know-how and related technical information that is needed to achieve a significant development, production, or use. The term know-how includes services, processes, procedures, specifications, design data and criteria, and testing techniques.

6. Militarily Critical Technology. See critical technology.

7. Munitions. Includes:

a. Arms, ammunition, and other implements of war.

b. Any property, installation, commodity, material equipment, supply, or goods used to make military items.

c. Any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing repair, servicing, storage, construction, transportation, operation, or use of any article listed above.

d. Technical data related to State Department munitions list items.

8. Services. Includes any service, test inspection, repair, training, publication, technical or other assistance, or defense information used to furnish military assistance, including military education and training activities.

9. Strategic Trade Cases. Cases involving technology and goods that are dual-use in nature, that is, capable of being used either for legitimate civilian purposes or capable of being used or diverted to increase a nation's military potential.

10. Technical Data. Classified or unclassified information of any kind that can be used, or adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of goods or munitions; or any technology that advances the state of the art or establishes a new art in an area of significant military applicability in the United States. The data may be tangible, such as a model, prototype, blueprint, or an operating manual, or may be intangible, such as a technical service or oral or visual interactions.

11. Technology. The technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software. The term does not include the goods themselves.

12. Transfer Mechanisms. The means by which technology, goods, services, and munitions are transferred, including but not limited to:

a. Commercial and government sales.

b. Scientist, engineer, student, and academic exchanges.

c. Consulting agreements.

d. Licensing and other data exchange agreements.

e. Codevelopment and coproduction agreements.

f. Commercial proposals and associated business visitors.

g. Trade fairs, exhibits, and airshows.

h. Sales to third-party nations.

i. Multinational corporation transfers.

j. Foreign technical missions.

k. International programs (such as fusion, space, and high-energy).

l. International meetings and symposia on advanced technology.

m. Patents.

n. Clandestine or illegal acquisition of military or dual-use technology or equipment.

o. Dissemination of technical reports technical data, whether published or by oral or visual release.

p. Dissemination of technical reports under DoD Directive 5400.7 (reference (e)).

q. Diversion or evasion of control procedures.

r. Smuggling.

s. Dummy corporations.

t. Acquiring an interest in U.S. industry, business, and other organizations.

January 17, 1984
NUMBER 2040.2

Department of Defense Directive

ASD(ISP)

SUBJECT: International Transfers of Technology, Goods, Services, and Munitions

References: (a) Public Law 96-72, "The Export Administration Act of 1979," as amended (50 U.S.C. 2401 et seq.)
(b) Public Law 94-329, "The Arms Export Control Act," as amended (22 U.S.C. 2751 et seq.)
(c) National Security Decision Directive Number 5, "Conventional Arms Transfer Policy," July 8, 1981
(d) through (q), see enclosure 1

A. PURPOSE

This Directive:

1. Implements relevant portions of references (a) through (c) by establishing policy, assigning responsibilities, and prescribing procedures for international transfer of defense-related technology, goods, services, and munitions.

2. Establishes the DoD International Technology Transfer (IT^2) Panel and Subpanels, whose charters are at enclosure 2.

3. Cancels DoD Directive 2030.4, DoD Directive 5030.28, and the Secretary of Defense Memorandum of December 29, 1983 (references (d), (e), and (f)).

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense, the Organization of the Joint Chiefs of Staff (OJCS), the Military Departments, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

2. This Directive applies to all technology transfer mechanisms and shall be implemented through such processes as strategic trade licensing, munitions licensing, security assistance, and DoD research, development, and acquisition activities.

3. The policies, procedures, and responsibilities contained in NDP-1 and DoD Directive 5230.11 (references (g) and (h)) concerning disclosures of classified military information are not affected by this Directive.

C. DEFINITIONS

The terms used in this Directive are defined in enclosure 3.

D. POLICY

It shall be DoD policy to treat defense-related technology as a valuable, limited national security resource, to be husbanded and invested in pursuit of national security objectives. Consistent with this policy and in recognition of the importance of international trade to a strong U.S. defense industrial base, the Department of Defense shall apply export controls in a way that minimally interferes with the conduct of legitimate trade and scientific endeavor. Accordingly, DoD Components shall:

1. Manage transfers of technology, goods, services, and munitions consistent with U.S. foreign policy and national security objectives.

2. Control the export of technology, goods, services, and munitions that contribute to the military potential of any country or combination of countries that could prove detrimental to U.S. security interests.

3. Limit the transfer to any country or international organization of advanced design and manufacturing know-how regarding technology, goods, services, and munitions to those transfers that support specific national security or foreign policy objectives.

4. Facilitate the sharing of military technology only with allies and other nations that cooperate effectively in safeguarding technology, goods, services, and munitions from transfer to nations whose interests are inimical to the United States.

5. Give special attention to rapidly emerging and changing technologies to protect against the possibility that militarily useful technology might be conveyed to potential adversaries before adequate safeguards can be implemented.

6. Seek, through improved international cooperation, to strengthen foreign procedures for protecting sensitive and defense-related technology.

7. Strive, before transferring valuable defense-related technology, to ensure that such technology is shared reciprocally.

E. PROCEDURES

1. In all technology transfer cases referred for review, the DoD Components concerned shall:

a. Consider proposed transfers of technology, goods, services, and munitions on a case-by-case basis.

b. Conduct policy reviews, technical evaluations, operational and military mission impact assessments, and intelligence assessments of proposed transfers.

c. Ensure that transfers of technology, goods, services, and munitions:

(1) Are consistent with U.S. national security and foreign policy objectives.

(2) Do not constitute an unreasonable risk to U.S. security in the degree to which they reduce technological leadtime.

(3) Receive positive consideration when such transfers will result in tangible and direct benefits to the defense objectives of the United States and its allies or to the defense industrial base. Such benefits should be at least equivalent to the value of the technology transferred.

d. Make sensitive transfers conditional upon agreements with allied and other nations that restrict the transfer of technology, goods, services, and munitions that harm or may harm the security of the United States and the security of U.S. allies and other friendly nations.

e. Oppose transfers of sensitive technology, goods, services, and munitions through multinational organizations in which potential adversaries participate.

f. Assess whether recipient nations:

(1) Restrict their transfer or export of U.S. technology, goods, services, and munitions to other nations who use, or may use, such technology, goods, services, and munitions against the best interests of the United States.

(2) Secure written U.S. Government agreement before reexporting U.S. technology, goods, services, and munitions.

(3) Maintain control over U.S. technology, goods, services, and munitions.

(4) Report promptly and fully to the U.S. Government any known or suspected transfers of U.S. technology, goods, services, and munitions that do not have U.S. Government approval.

(5) Transfer non-U.S. critical technology, goods, services, and munitions harmful to U.S. security.

g. Assess annually the total effect of transfers of technology, goods, services, and munitions on U.S. security, regardless of the transfer mechanisms involved.

h. Support approved DoD programs designed to inform government, Congress, industry, academia, and the public on the dangers of the loss of Western technological leadership.

2. In strategic trade cases, the DoD Components concerned shall:

a. Assess whether proposed transfers of technology and goods through actual or potential military use could threaten U.S. security, regardless of the stated end use or end user of such technology and goods.

b. Ensure that potential transfers of technology and goods are assessed with a primary consideration to control of critical technology as described by Pub. L. 96-72 and the "DoD Militarily Critical Technologies List" (references (a) and (i)).

c. Disapprove exceptions to the Coordinating Committee of the Consultative Group (COCOM) lists that are disadvantageous to the security of the United States and its allies.

d. Support North Atlantic Treaty Organization (NATO) efforts to control technology and goods.

e. Provide support to, and cooperate with, non-COCOM countries to control the transfer of militarily relevant technology and goods to the Warsaw Pact nations.

f. Assess whether recipient nations support U.S. objectives in COCOM and the COCOM embargo.

3. In munitions licensing cases, the DoD Components concerned shall:

a. Give favorable consideration to transfers of services and munitions to U.S. allies and friendly nations that are intended to achieve specific U.S. defense objectives.

b. Ensure that transfers of munitions and services involving critical technology receive special scrutiny, taking into account the importance of arms cooperation with NATO and other close friendly nations and allies, potential third-party transfers, and the protection of advanced military operational capabilities and associated technology.

c. Ensure that decisions on munitions license applications that involve or may lead to the disclosure of classified military information are in compliance with NDP-1 and DoD Directive 5230.11 (references (g) and (h)).

4. The DoD Components concerned shall submit unresolved technology security cases and issues to the appropriate DoD IT^2 Subpanel for resolution.

5. Two subcommittee reports to the DoD Steering Committee on National Security and Technology Transfer (references (j) and (k)), when approved, may provide additional procedural guidance affecting publications and technology monitoring.

F. <u>COORDINATING COMMITTEE OF THE CONSULTATIVE GROUP (COCOM)</u>

1. COCOM, founded in 1949, is an informal multinational organization made up of the NATO nations (except Iceland and Spain) and Japan. COCOM'S mission is to maintain a uniform export control system among its member nations in order to protect Western security.

2. DoD Components concerned with strategic trade policy shall seek to strengthen COCOM by:

a. Promoting the development of a professional secretariat.

b. Promoting the tightening of the strategic control list.

c. Encouraging enforcement of COCOM controls.

d. Promoting a threshold on the COCOM list beyond which technology and goods cannot be transferred to potential adversaries.

e. Promoting broader membership of free-world nations in COCOM and associate agreements with COCOM for advanced, industrialized nations.

f. Promoting the establishment of a military committee to consider strategic issues related to the control programs.

g. Providing full-time DoD policy representation to COCOM.

h. Supporting and promoting other measures that strengthen the COCOM organization and function and that support U.S. objectives.

G. RESPONSIBILITIES

1. The Under Secretary of Defense for Policy (USD(P)) shall:

a. Develop, coordinate, and issue policies relating to technology transfer control in accordance with DoD Directive 5111.1 (reference (1)).

b. Prepare technology transfer control and enforcement policy guidance and coordinate overall application of DoD policy.

c. Represent the Department of Defense in interagency, national, and international forums concerning policy for technology transfer control and enforcement matters.

d. For technology transfer policy matters, serve as DoD point of contact for foreign governments, international agencies, other federal agencies, interagency groups, industry, and DoD Components.

e. Act as the DoD receiving point for all strategic trade, COCOM, and munitions license cases.

f. Conduct policy reviews on technology, goods, services, and munitions transfer cases.

g. Prepare the coordinated DoD position for strategic trade, COCOM, and munitions license cases. If the projected recommendation differs from recommendations of the DoD Components concerned, advise the DoD Components of the recommendation and supporting rationale in sufficient time to permit submission of the issue to the DoD IT^2 Subpanel A before issuing the position.

h. Issue coordinated DoD recommendations on strategic trade, COCOM, and munitions transfer cases to the Commerce and State Departments.

i. Develop and maintain comprehensive reference data bases on technology, goods, services, and munitions transfer matters that are accessible to all DoD Components.

j. Provide to DoD Components a weekly update of the disposition of significant transfer cases.

k. Provide executive direction of the DoD IT^2 Panel in accordance with enclosure 2.

l. Develop, review, and negotiate international agreements under this Directive, DoD Directive 5530.3, and DoD Instruction 2050.1 (references (m) and (n)).

m. Assess, with the support of the Director, Defense Intelligence Agency (DIA), and the Chairman, National Disclosure Policy Committee, recipient nations':

(1) Laws, regulations, and internal operating procedures to determine their ability to enforce technology security and control provisions of applicable U.S. export license stipulations, specific cooperative program agreements with the U.S. Government, COCOM embargoes, and other industrial and government agreements.

(2) Reliability in maintaining control over technology, goods, services, and munitions that originate in the United States and whose transfer to other nations may be against the best interests of the United States.

(3) Reliability in securing prior written U.S. Government approval before exporting technology, goods, services, and munitions originating in the United States to other nations.

(4) Reliability and promptness in reporting known or suspected transfers of U.S. technology, goods, services, and munitions that were not approved by the U.S. Government.

(5) Support of U.S. objectives in COCOM and the COCOM embargo.

(6) Cooperation and support for the principle of sharing technology of comparable value with the United States.

(7) Reliability in preventing transfer to potential adversaries of non-U.S. critical technology, goods, services, and munitions harmful to the U.S. security.

n. Request the Under Secretary of Defense for Research and Engineering (USDR&E) to provide technical advisors and consultants necessary to support development of DoD technology transfer policy.

o. Assess annually the total effect of technology, goods, services, and munitions transfers on the security of the United States, regardless of the transfer mechanism involved.

p. Support the U.S. intelligence and enforcement communities in their efforts to halt or control the flow of technology, goods, services, and munitions to potential adversaries.

q. Establish, through the appropriate DoD IT^2 Subpanel, working groups and task forces to develop ways and means to protect technology from exploitation by potential adversaries.

2. The Under Secretary of Defense for Research and Engineering shall:

a. Manage overall DoD technical and acquisition efforts related to technology, goods, services, and munitions transfer in accordance with DoD Directive 5129.1 (reference (o)).

b. Oversee implementation of DoD technology transfer policy for all research, development, and acquisition matters.

c. For research, development, and acquisition matters, act as DoD point of contact with industry, other federal agencies, interagency groups, DoD Components, academia, and appropriate international forums.

d. Coordinate the technical review of strategic trade, COCOM, and munitions cases and establish the DoD technical positions, with supporting rationales, regarding the proposed transfer of technology, goods, services, and munitions.

e. Develop and administer programs to identify and define lists of militarily critical technologies that should be controlled for export, including necessary guidelines.

f. Manage technical efforts in support of DoD participation in and implementation of studies and analyses of COCOM, U.S. export controls, and related technology, goods, services, and munitions transfer matters.

g. Develop the DoD technical portion for the "DoD Militarily Critical Technologies List" (reference (i)) revisions and COCOM negotiations.

h. Provide technical advisors and consultants as needed to support the USD(P) in the development of DoD technology transfer policy.

i. Provide technical support of DoD views in interagency, national, and international forums of technology, goods, services, and munitions transfer matters.

j. Provide technical support for USD(P) assessments of the foreign availability of technology, goods, services, and munitions.

k. Develop, review, and negotiate international agreements in accordance with this Directive, DoD Directive 5530.3, and DoD Instruction 2050.1 (references (m) and (n)).

l. Develop and maintain a comprehensive technical data base for technology, goods, services, and munitions transfer cases.

m. Participate on the DoD IT^2 Panel and Subpanels in accordance with enclosure 2.

n. Support the U.S. intelligence and enforcement communities in their efforts to halt or control the flow of technology, technical data, goods, services, and munitions to potential adversaries.

o. For technology transfer research cases:

(1) Serve as the receiving point in the Department of Defense.

(2) Obtain a policy position from the USD(P).

(3) Conduct reviews and prepare coordinated DoD recommendations, with supporting rationales.

(4) Advise DoD Components if the projected recommendation differs from their recommendations and provide an opportunity for the DoD Components to submit the issue to the DoD IT^2 Subpanel B before issuing a DoD position. If a case is appealed, within 15 days the case shall be decided and all interested parties notified or the case shall be referred to the Deputy Secretary of Defense or Secretary of Defense for a final decision.

(5) Issue, after the appeal process is completed, the coordinated DoD recommendation.

3. The Assistant Secretary of Defense (International Security Policy) (ASD(ISP)) shall:

a. Monitor compliance with this Directive through the Deputy Assistant Secretary of Defense (International Economic, Trade, and Security Policy) (DASD(IETSP)).

b. Chair the DoD IT^2 Panel and participate on the DoD IT^2 Subpanels in accordance with enclosure 2.

4. The Chairman of the Joint Chiefs of Staff shall:

a. Conduct and provide operational and military mission impact assessments on technology, goods, services, and munitions transfer issues, as requested.

b. Provide operational expertise and military judgment in interagency, national, and international forums on technology, goods, services, and munitions transfer matters.

c. Participate on the DoD IT^2 Panel and Subpanels in accordance with enclosure 2.

5. The Director, Defense Intelligence Agency, shall:

a. Formulate DoD coordinated intelligence assessments concerning the types and numbers of illegal transfer of technology, goods, services, and munitions and the associated transfer mechanisms.

b. Designate a point of contact to represent the DIA on technology, goods, services, and munitions transfer matters.

c. Conduct and provide intelligence reviews on technology, goods, services, and munitions transfer cases.

d. Assess foreign availability of technology, goods, services, and munitions proposed for transfer.

e. Conduct end-user checks on the declared ultimate consignee on technology, goods, services, and munitions transfer cases.

f. Provide intelligence expertise in interagency, national, and international forums on technology, goods, services, and munitions transfer matters.

g. Provide intelligence concerning the total effect of transfers of technology, goods, services, and munitions on U.S. security.

h. Participate on the DoD IT^2 Panel and Subpanels in accordance with enclosure 2.

i. Assist in identifying and assessing critical technology.

6. The Heads of DoD Components shall:

a. Designate a point of contact in their respective Component for technology, goods, services, and munitions transfer matters.

b. Conduct assessments of proposed technology, goods, services, and munitions transfer cases as required and provide coordinated positions.

c. Assist in identifying and assessing critical technology and in supporting DoD participation in export control list reviews.

d. Participate on the DoD IT^2 Panel and Subpanels in accordance with enclosure 2.

e. Consistent with this Directive, DoD Directive 5530.3, and DoD Instruction 2050.1 (references (m) and (n)), coordinate the development and negotiation of international agreements pertaining to technology, goods, services, and munitions transfers.

f. Assure the calculation of nonrecurring cost recoupment charges in accordance with DoD Directive 2140.2 (reference (p)).

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Assistant Secretary of Defense (International Security Policy) within 120 days.

Caspar W. Weinberger
Secretary of Defense

Enclosures - 3
1. References
2. DoD International Technology Transfer (IT^2) Panel and Subpanels
3. Definitions

REFERENCES (Continued)

(d) DoD Directive 2030.4, "DoD Support for the Strategic Trade Control Program," December 11, 1962 (hereby canceled)
(e) DoD Directive 5030.28, "Munitions Control Procedures for U.S. Munitions List Export License Applications Referred to DoD by Department of State," March 10, 1970 (hereby canceled)
(f) Secretary of Defense Memorandum, "DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," December 29, 1983 (hereby canceled)
(g) "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations" (NDP-1), September 9, 1981
(h) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," March 2, 1979
(i) Under Secretary of Defense for Research and Engineering, "DoD Militarily Critical Technologies List (U)" (Secret Noforn), October 1, 1982
(j) Report when approved of the Subcommittee on Publications to the DoD Steering Committee on National Security and Technology Transfer, November 9, 1983
(k) Report when approved of the Subcommittee on Technology Monitoring to the DoD Steering Committee on National Security and Technology Transfer, September 19, 1983
(l) DoD Directive 5111.1, "Under Secretary for Policy," October 27, 1978
(m) DoD Directive 5530.3, "International Agreements," December 6, 1979
(n) DoD Instruction 2050.1, "Delegated Approval Authority to Negotiate and Conclude International Agreements," July 6, 1977
(o) DoD Directive 5129.1, "Under Secretary of Defense for Research and Engineering," November 29, 1978
(p) DoD Directive 2140.2, "Recoupment of Nonrecurring Costs on Sales of USG Products and Technology," January 5, 1977
(q) DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980

DOD INTERNATIONAL TECHNOLOGY TRANSFER (IT^2) PANEL AND SUBPANELS

A. THE DOD IT^2 PANEL

1. Functions. The DoD IT^2 Panel shall:

a. Identify and address technology transfer policy issues.

b. Resolve differences within the Department of Defense concerning program administration, interagency issues, and coordinated DoD recommendations on transfer cases referred by the DoD IT^2 Subpanels.

2. Organization and Management

a. The DoD IT^2 Panel shall be chaired by the ASD(ISP) or, in his absence, by the vice-chair.

b. The vice-chair shall be the Principal Deputy USDR&E (PDUSDR&E) or, in his absence, a person designated by the ASD(ISP) shall serve as chair.

c. In addition to the chair and the vice-chair, the Panel consists of representatives of the Office of the Deputy USD(P) (ODUSD(P)), the Office of the ASD(ISP) (OASD(ISP)), the Office of the USDR&E (OUSDR&E), the OJCS, the Defense Security Assistance Agency (DSAA), the DIA, the National Security Agency (NSA), the Defense Advanced Research Projects Agency (DARPA), and the Military Departments.

d. Panel members, excluding representatives of the NSA, DSAA, DARPA, and DIA, shall have one vote, and all voting members shall be polled on any decision. The NSA shall vote on matters having a potential impact on the cryptologic (communications security (COMSEC) and signals intelligence (SIGINT)), computer security, and electronic warfare (EW) mission areas. The DSAA shall vote on matters concerning security assistance. The DIA and DARPA shall serve in an advisory capacity.

e. Other DoD Components and other agencies and individuals may be invited to participate as necessary, but will have no vote.

f. Issues may be referred to the Panel on the recommendation of any voting member or from the DoD IT^2 Subpanels.

g. The Panel shall meet quarterly and at other times subject to the call of the chair.

h. On matters not concerning the resolution of DoD positions on specific transfer cases, a two-thirds majority vote shall resolve any differences.

i. In resolving differences concerning coordinated DoD recommendations on transfer cases, a unanimous vote is required to recommend approval of a proposed transfer.

j. Appeals shall be resolved by the Secretary of Defense or Deputy Secretary of Defense and may be made by any voting member of the Panel.

B. DOD IT^2 SUBPANEL A, EXPORT CONTROL POLICY

1. Functions. The DoD IT^2 Subpanel A shall:

a. Resolve differences within the Department of Defense on matters referred to it concerning the transfer of technology, goods, services, and munitions; IT^2 program administration and interagency technology transfer issues; and transfer cases requiring a coordinated DoD recommendation.

b. Identify and recommend solutions to technology transfer policy issues.

c. As required, form working groups drawn from member organizations and agencies to address specific issues raised by the DoD IT^2 Panel, by member organizations or agencies, or as deemed appropriate by the chair to address high-priority technology transfer policy issues.

2. Organization and Management

a. The DoD IT^2 Subpanel A shall be chaired by the DASD(IETSP), OASD(ISP).

b. The vice-chair shall be the Deputy Under Secretary of Defense (International Programs and Technology) (DUSD(IP&T)), OUSDR&E.

c. In addition to the chair and vice-chair, the Subpanel consists of representatives of the ODUSD(P); the ODASD(IETSP), OASD(ISP); the ODUSD(IP&T), OUSDR&E; the OJCS; the DSAA; the NSA; the DIA; DARPA; and the Military Departments.

d. Each member, excluding representatives of the DSAA, NSA, DIA, and DARPA, shall have one vote. All voting members shall be polled on any decision. The DSAA shall vote on matters concerning security assistance. The NSA shall vote on matters having a potential impact on the cryptologic (COMSEC and SIGINT), computer security, and EW mission areas. The DIA and DARPA shall serve in an advisory capacity.

e. Other DoD Components and other agencies and individuals may be invited to participate as necessary, but will have no vote.

f. Technology transfer issues may be referred to the Subpanel by any member when the issue requires resolution by establishing a precedent for critical or sensitive technology or when intelligence or political information dictates a policy review for specified countries.

g. On issues not concerning the resolution of DoD positions on transfer cases, a two-thirds majority vote shall resolve any differences. When a two-thirds majority decision cannot be reached, the matter under consideration shall be referred to the DoD IT^2 Panel for disposition.

h. Issues concerning coordinated DoD recommendations on transfer cases shall be referred to the Subpanel only after an attempt has been made to resolve the differences at the working level or if a DoD position on a case must be issued within 15 working days and the differences have not been resolved.

i. In resolving differences concerning coordinated DoD recommendations on transfer cases, a unanimous vote is required to recommend approval of a proposed transfer. Appeals on the cases under consideration may be made by any DoD Component having a voting member. The chair shall refer the cases to the DoD IT^2 Panel for review.

j. The chair of the Subpanel A shall chair the DoD IT^2 Panel if the Panel chair and vice-chair are unable to attend the Panel meeting.

k. Subpanel A shall meet monthly and at other times subject to the call of the chair. When a specific transfer case is appealed to Subpanel A, the Subpanel shall meet to resolve the case within 10 working days.

l. Administrative support for Subpanel A shall be provided by the Office of the DASD(IETSP), OASD(ISP).

C. DOD IT^2 SUBPANEL B, RESEARCH AND DEVELOPMENT

1. Functions. The DoD IT^2 Subpanel B shall:

a. Address issues and resolve differences in the Department of Defense regarding technical standards and definitions and the dissemination and exchange of technical information.

b. Consider appeals on recommendations in technology transfer research cases.

c. As required, form working groups drawn from member organizations and agencies to address specific issues raised by the DoD IT^2 Panel, by member organizations or agencies, or as deemed appropriate by the chair to address high-priority technology transfer research cases.

2. Organization and Management

a. The chair shall be the Deputy Under Secretary of Defense for Research and Advanced Technology (DUSD(R&AT)), OUSDR&E.

b. The vice-chair shall be the DASD(IETSP), OASD(ISP).

c. Other members of Subpanel B shall be representatives from the ODUSD(P), USD(P); ODASD(IETSP), OASD(ISP); ODUSD(R&AT), OUSDR&E; the Assistant Secretaries of the Army (Research, Development, and Acquisition), the Navy (Research, Engineering, and Systems), and the Air Force (Research, Development, and Logistics); the DSAA; the DIA; DARPA; and the NSA.

d. Each member, excluding representatives of the DSAA, DIA, DARPA, and NSA, shall have one vote, and all voting members shall be polled on a decision. The DSAA shall vote on issues concerning security assistance. The DIA shall serve in an intelligence advisory capacity. DARPA shall vote on issues affecting fulfillment of DARPA's mission. The NSA shall vote on issues concerning its

missions in cryptology (COMSEC and SIGINT), computer security, and EW.

e. Additional DoD Components and other agencies and individuals may be invited by the chair or vice-chair to participate as necessary, but will have no vote.

f. Issues may be referred to the Subpanel by any member, including representatives of the DSAA, DIA, DARPA, and NSA.

g. A two-thirds majority vote shall resolve differences. Any member voting on a particular issue may appeal a decision to the DoD IT^2 Panel.

h. Administrative support for Subpanel B shall be provided by the Office of the DUSD(R&AT), OUSDR&E.

i. The Subpanel shall meet monthly and at other times as determined by the chair. When a research technology transfer case is appealed to Subpanel B, the Subpanel shall meet within 10 working days to resolve the case.

DEFINITIONS

1. Critical Technology. Technologies that consist of (a) arrays of design and manufacturing know-how (including technical data); (b) keystone manufacturing, inspection, and test equipment; (c) keystone materials; and (d) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (also referred to as militarily critical technology).

2. Goods. Any articles, materials, supplies, or manufactured products, including inspection and test equipment. The term excludes technical data.

3. Items of Intrinsic Military Utility. End items other than those identified in the "DoD Militarily Critical Technologies List" (reference (i)) whose transfer to potential adversaries shall be controlled for the following reasons:

a. The end product in question could significantly enhance the recipient's military or warmaking capability either because of its technology content or because of the quantity to be sold; or

b. The product could be analyzed to reveal U.S. system characteristics and thereby contribute to the development of countermeasures to equivalent U.S. equipment.

4. Keystone Equipment. Includes manufacturing, inspection, or test equipment and is the required equipment for the effective application of technical information and know-how. Keystone materials have the same significant application.

5. Know-how. Includes both the know-how of design and manufacturing and the know-how and related technical information that is needed to achieve a significant development, production, or use. The term know-how includes services, processes, procedures, specifications, design data and criteria, and testing techniques.

6. Militarily Critical Technology. See critical technology.

7. Munitions. Includes:

a. Arms, ammunition, and other implements of war.

b. Any property, installation, commodity, material equipment, supply, or goods used to make military items.

c. Any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing repair, servicing, storage, construction, transportation, operation, or use of any article listed above.

d. Technical data related to State Department munitions list items.

8. Services. Includes any service, test, inspection, repair, training, publication, technical or other assistance, or defense information used to furnish military assistance, including military education and training activities.

9. Strategic Trade Cases. Cases involving technology and goods that are dual-use in nature, that is, capable of being used either for legitimate civilian purposes or capable of being used or diverted to increase a nation's military potential.

10. Technical Data. Classified or unclassified information of any kind that can be used, or adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of goods or munitions; or any technology that advances the state of the art or establishes a new art in an area of significant military applicability in the United States. The data may be tangible, such as a model, prototype, blueprint, or an operating manual, or may be intangible, such as a technical service or oral or visual interactions.

11. Technology. The technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software. The term does not include the goods themselves.

12. Transfer Mechanisms. The means by which technology, goods, services, and munitions are transferred, including but not limited to:

a. Commercial and government sales.

b. Scientist, engineer, student, and academic exchanges.

c. Consulting agreements.

d. Licensing and other data exchange agreements.

e. Codevelopment and coproduction agreements.

f. Commercial proposals and associated business visitors.

g. Trade fairs, exhibits, and airshows.

h. Sales to third-party nations.

i. Multinational corporation transfers.

j. Foreign technical missions.

k. International programs (such as fusion, space, and high-energy).

l. International meetings and symposia on advanced technology.

m. Patents.

n. Clandestine or illegal acquisition of military or dual-use technology or equipment.

o. Dissemination of technical reports and technical data, whether published or by oral or visual release.

p. Dissemination of technical reports under DoD Directive 5400.7 (reference (q)).

q. Diversion or evasion of control procedures.

r. Smuggling.

s. Dummy corporations.

t. Acquiring an interest in U.S. industry, business, and other organizations.