

# TECHNOLOGY TRANSFER, EXPORT CONTROLS AND INTERNATIONAL PROGRAMS SECURITY

## INTRODUCTION

Security assistance is a group of programs, authorized by law, that allow the transfer of military articles and services to friendly foreign governments via sales, grants, leases, or loans. These are authorized under the premise that they are essential to the security and economic well-being of allies and international organizations, and are equally vital to the security and economic well-being of the United States (U.S.). The courses at the Defense Institute of Security Assistance Management (DISAM) are geared to teach you how to transfer technology to help in the vital security, economic well-being, national security, and foreign policy objectives of the U.S. The key to this chapter is to understand that a technology transfer is an export and must be accomplished in a controlled way to assure U.S. national security objectives. To accomplish this, the chapter will cover international programs security requirements.

The Global War on Terrorism is on the forefront of our national security and the protection of critical military technology and information is critical. There is general agreement now that a broader approach to security is needed, embracing political, economic, social, ecological, and other factors.

As domestic and world markets for military equipment continue to shrink, competition based on leading edge technology has caused a significant increase in economic espionage vice military espionage for U.S. technology. Although economic security has become an important part of American foreign policy, military strength will remain an essential instrument of foreign policy. It is Department of Defense (DoD) policy to treat defense related technology as a valuable and limited national security resource. Which technologies should be controlled and to what extent? First we must understand that the U.S. policy on international trade consists of two seemingly conflicting elements:

- Free trade - the importance of international trade to a strong U.S. defense industrial base
- National security - the need to restrict the export of technology, goods, services, and munitions that would otherwise contribute to the military strength of target countries that affect U.S. national security

Keeping in mind the balance between free trade and national security, it is the responsibility of those that control technology to understand the laws, regulations and directives that guide the transfer. Traditional security assistance programs are mechanisms through which technology transfer may occur. International armaments cooperation programs with allies and friends are another means of transferring technology, especially through co-development, co-production, and commercially licensed production programs.

Once technology transfer is discussed and the methods used to transfer and control that export are covered, one still needs to know how to transfer technology by secure means. Controlling the

level of technology transferred to U.S. allies and friends is just a subset of the concept of international programs security (IPS). We start with a definition of an international program and the security of the program.

- An international program is a lawful and authorized government or commercial effort in which there is a contributing or receiving foreign participant and information or technology is transferred from one country to another
- International programs security is the total effort that safeguards information and technology identified as requiring control that is generated by, provided to, or transferred in international programs

This chapter will discuss nine main topics concerning technology transfer and export control policy and international programs security requirements:

- The concept of technology transfer and export controls
- Controlled unclassified information (CUI)
- Foreign disclosure and the national disclosure policy (NDP)
- Export approval and license process
- International visits and assignments
- International transfers
- Defense Security Service (DSS) role in international programs
- Foreign government and North Atlantic Treaty Organization (NATO) information
- Committee on Foreign Investment in the U.S. (CFIUS) and foreign ownership, control or influence (FOCI)

## **THE CONCEPT OF TECHNOLOGY TRANSFER AND EXPORT CONTROLS**

Technology transfer is the process of transferring, from an industry in one country to another or between governments themselves, technical information and know-how relating to the design, engineering, manufacture, production, and use of goods. To comply with U.S. policy, technology transfer is regulated by a myriad of U.S. government (USG) agencies, and is ultimately controlled through a government-to-government agreement that can take the form of a memorandum of understanding, general security agreement, letter of offer and acceptance (LOA), export license, or other form agreed to by both governments. The *Security Assistance Management Manual (SAMM)*, C3, “Technology Transfer and Disclosure,” is a key reference when working with security assistance that deals with technology transfer. It must be noted that the transfer policies addressed in this chapter are concerned with those that relate to militarily critical technology. Also addressed in this chapter are the policies and controls for the transfer of classified information, i.e., national disclosure policy as well as the transfer of defense articles and services.

The policy and controls discussed herein do not normally apply to common or “public domain” reference material such as military standards, specifications, handbooks, or commercial counterparts to these documents. U.S. industry representatives can determine if their materiel is within public domain by submitting documents to the director for freedom of information and security review (OASD-PA/DFOISR).

## Department of Defense Policy on Technology Transfer

The primary policy governing the process of technology transfer is contained in DoDD 2040.2, *International Transfers of Technology, Goods, Services and Munitions*. This directive institutionalizes technology security responsibilities within DoD. The directive establishes working relationships among the Joint Staff, the services, and the defense agencies. Selected U.S. technology laws and other appropriate DoD and military services directives are listed in Attachment 7-2 to this chapter.

DoDD 2040.2 states 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, DoD shall apply export controls to minimally interfere with the conduct of legitimate trade and scientific endeavor. This policy applies to DoD components.

Before we can understand how to control the transfer of technology we must define “defense articles.” Per the International Traffic in Arms Regulations (ITAR), Part 120.7:

Defense article means any item or technical data designated in Section 121.1 of this subchapter. Section 121.1 of the ITAR is:

The United States Munitions List (USML). The USML documents articles that have a primarily military utility. So the USML has the “Items”, but what is “technical data?” Again, per the ITAR, Section 120.10, Technical Data means, for purposes of this subchapter: (1) Information, other than software as defined in Section 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation, (2) Classified information relating to defense articles and defense services.

The ITAR goes on to state:

(5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities or information in the public domain . . .

### Technology Transfer Mechanisms

Within the context of security assistance, foreign military sales (FMS) and direct commercial sales (DCS) are normally thought of as the primary means by which technology, goods, services and munitions are transferred; however, as the following list (which is not all inclusive) from DoDD 2040.2 shows, there are many different means for effecting transfers:

- Commercial and government sales
- Scientist, engineer, student, and academic exchanges
- Licensing and other data exchange agreements
- Co-development and co-production agreements
- Commercial proposals and associated business visitors
- Trade fairs, exhibits, and air shows
- Sales to third-party nations

- Multinational corporation transfers
- International programs (such as fusion, space, and high energy)
- International meetings and symposia on advance technology
- Patents
- Clandestine or illegal acquisition of military or dual-use technology or equipment
- Dissemination of technical reports and technical data, whether published or by oral or visual release
- Dissemination of technical reports under DoDD 5400.7, DoD Freedom of Information Act Program
- Dummy corporations
- Acquiring an interest in U.S. industry, business, and other organizations

### **The Basics of International Programs Security**

To protect technology that is being transferred, one must understand the legal and national policy basis for DoD's international programs and the principal security considerations prior to pursuing an international program. The three primary documents that form the framework for national disclosure policy are the Arms Export Control Act (AECA), executive order (E.O.) 12958, as amended 25 March 2003, and the National Security Decision Memorandum (NSDM) 119. Each of these will be covered in more detail below. The final topic will be a discussion of the government-to-government principle. Information for the remainder of this section comes primarily from the *International Programs Security Handbook*, ODUSD (Technology Security Policy and National Disclosure Policy), February 1995 (Revised January 1, 2006).

#### ***Access and Protection***

The conditions and criteria established by the basic laws and policies require that two fundamental decisions be addressed prior to sharing U.S. defense articles with another country or international organization: whether their access is in the best interest of the U.S. and whether the articles or information will be afforded the proper protection.

#### ***Legal and Policy Basis for Program Security***

The three principal documents that provide the legal and national policy basis for security in most DoD international programs include the AECA, E.O. 12958, and National Security Decision Memorandum (NSDM) 119.

The AECA governs the export of defense articles and defense services to foreign countries and international organizations and includes both commercial and government programs. It authorizes a list of controlled articles, the USML, which is contained in the ITAR published by the Department of State (DoS). The ITAR is available on the internet at <http://www.pmdtc.gov/reference.htm#ITAR>. The AECA forms the legal basis for the security requirements of most DoD international programs. The AECA states that foreign sales (i.e., access) should be consistent with U.S. foreign policy interests, strengthen the security of the U.S., and contribute to world peace. The AECA also requires the president to provide Congress assurances that the proposed recipient foreign country or international organization has agreed to certain security conditions regarding the protection of the articles or information. The

three security-related conditions that must be satisfied to provide export controlled defense articles and information to a foreign country or international organization are:

- The recipient country or organization agrees not to transfer title or possession of the articles or related technical data to anyone who is not an officer, employee or agent of the country or organization without prior USG consent
- The recipient country or organization agrees not to use the articles or related technical data or permit their use for other than the purpose for which they were furnished without prior USG consent
- The recipient country or organization agrees to maintain security and provide substantially the same degree of security as the USG

Executive Order 12958, as amended 25 March 2003, establishes the executive branch's classified national security information program. Section 4 of this order states that access may be granted only when required in order to perform or assist in a lawful and authorized governmental function. This is the basis of the need-to-know principle. Further, persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch. The executive order also states that classified information cannot be transferred to a third party without the consent of the originator. It also provides for the protection of foreign government information. The executive order is implemented by Office of Management and Budget (OMB) directive number 1, 32 CFR, Part 20001, and the presidential directive on safeguarding classified national security information and within DoD by DoD 5200.1-R.

NSDM 119 provides the basic national policy governing decision-making on the disclosure of classified military information (CMI) to foreign governments and international organizations. NSDM 119 reiterates the basic requirements of the AECA and the executive order (E.O.) 12958 and emphasizes that classified military information is a national asset and the USG will not share it with a foreign government or international organization (i.e., permit access) unless its release will result in a clearly defined benefit to the U.S. and the recipient government or organization will provide substantially the same degree of protection.

### ***Government-to-Government Principle***

Classified information is shared with foreign governments and international organizations based on the government-to-government principle. This principle is defined by two activities relating to international programs. It applies to export and disclosure decisions, and to transfers of classified information and material.

- In keeping with the AECA, E.O. 12958, and NSDM 119, the decision to be made is whether the USG will release classified information to another government or international organization
- If the answer is yes, then the second part of the transfer must be made either through official government-to-government channels (e.g., military postal service or government courier service) or through other channels approved by the responsible governments, i.e., a government-to-government transfer

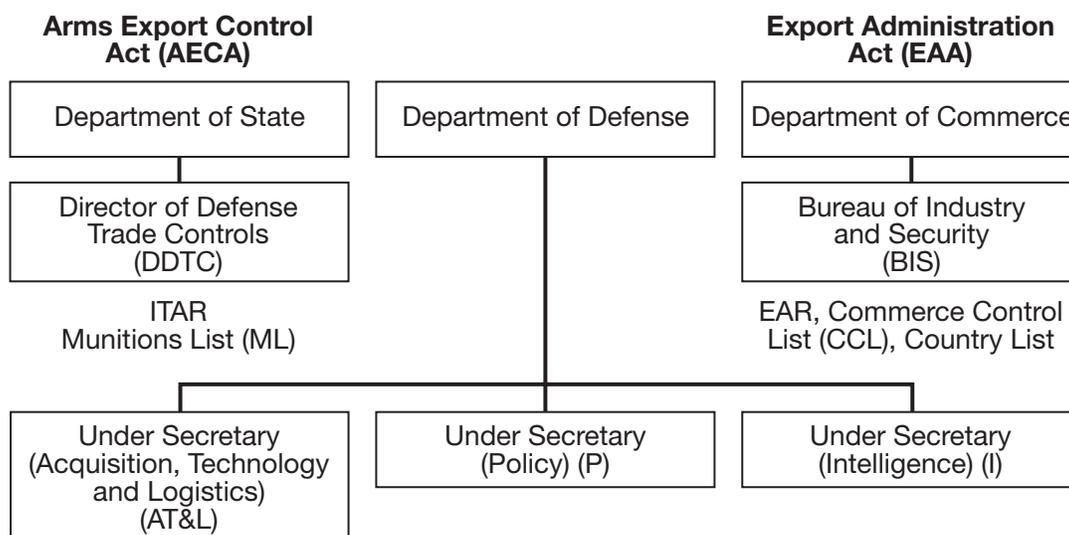
The transfer via government channels transfer is necessary so that government accountability and control can be maintained from the point-of-origin to the ultimate destination and custody is officially transferred to the recipient government that assumes responsibility for the protection of the article

or information. Transfers normally occur between designated government representatives (DGRs). A security assurance must be obtained prior to transferring classified material to a representative of a foreign government or international organization and a receipt must be obtained for classified information in material form.

### Key Department of Defense Security Organizations

Before the fundamental security considerations required in a government-to-government agreement are discussed, a review of the key USG organizations that manage technology transfer is necessary. Figure 7-1 provides a macro-overview of the key players within the Executive Branch for technology transfer and international program security. The under secretary of defense for policy [USD (P)] is responsible for international security matters. The deputy under secretary of defense (technology security policy and national disclosure policy) [DUSD (TSP&NDP)] is responsible for day-to-day decisions on NDP and the Defense Technology Security Administration (DTSA). More specifically the office is responsible for the security policy for international programs. This responsibility includes security policy and arrangements for international programs, international security agreements, the NDP, and NATO security policy. When the DoS and the Department of Commerce require DoD input to decide if a license for export should or should not be approved, the request goes to DTSA. DTSA’s responsibilities will be covered in further detail under the topic of “exports” later in this chapter.

**Figure 7-1**  
**Key Players in Technology Transfer and International Programs Security**



The under secretary of defense for intelligence [OUSD (I)] is responsible for DoD counter-intelligence, security, and intelligence programs and staff supervision of the DSS. This includes intelligence, counterintelligence, and security support for program protection planning for DoD acquisition programs. The [USD (I)] also has staff supervision responsibility for the DSS and for publication of the *National Industrial Security Program Operating Manual* (NISPOM). With the DSS field offices [USD (I)] assures that companies that manufacture military items adhere to the same laws and regulations concerning technology transfer as do individuals working for the USG.

The under secretary of defense (acquisition, technology and logistics) [USD (AT&L)] is responsible for defense procurement and international armaments cooperation programs (IACP). These functions are performed by the director, defense procurement and the director, international cooperation. The

Defense Contract Management Agency (DCMA) also reports [USD (AT&L)]. In addition to its normal management of DoD contracts, DCMA provides industrial security support at those defense contractor facilities where a DSS representative is not available.

The Joint Staff provides support that includes conducting operational and military mission impact assessments on technology, goods, services, and munitions transfer issues, as requested.

The Defense Intelligence Agency (DIA) performs the following functions in the support of U.S. defense technology security:

- Provides assessments of the types and numbers of illegal transfers of technology, goods, services, and munitions, and the associated transfer mechanisms
- Designates a point of contact to represent DIA on technology transfer matters
- Conducts end user checks and intelligence review on technology, goods, services, and munitions transfer cases
- Assesses foreign availability of technology, goods, services, and munitions proposed for transfer
- Provides intelligence concerning the total effect of transfers of technology, goods, services, and munitions on U.S. security
- Provides intelligence expertise in interagency, national, and international fora on technology, goods, services, and munitions transfer matters
- Assists in identifying and assessing critical technologies

The DoD export control responsibilities and participating organizations are further depicted in Table 7-1.

<b>Table 7-1 DoD Organizational Export Control Responsibilities</b>	
<b><u>Organization</u></b>	<b><u>Responsibility</u></b>
[USD (AT&L)]	Technical oversight for national security and nonproliferation  Vice Chairman International Technology Transfer Coordinating Committee (ITTCC)  National Economic Council representative  Economic security balance
[USD (P)]	Policy overlay
Joint Staff	Strategic rationale and validation
Intelligence community	Threat assessments of foreign nations
Military departments	Experts input from labs and commands
Institute for Defense Analysis	Federally-funded research and development (R&D) center providing [USD (AT&L)] with technical support and economic security assessments
Industry and academia	Participate in technical working groups and multilateral negotiation

## **Exports through the Department of Commerce**

Under the Export Administration Act of 1979 (EAA), the Department of Commerce has licensing jurisdiction over all commodities and unclassified technical data except for certain specified items handled by other government agencies, such as USML items by the DoS, or atomic energy material by the U.S. Department of Energy. The EAA applies to the following:

- Exports of commodities and technical data from the U.S.
- Re-exports of U.S.-origin commodities and technical data from foreign destinations
- U.S.-origin parts and components used in a foreign country to manufacture a foreign end product for export and in some instances, a foreign product produced as a direct product of U.S.-origin technical data

The Export Administration Regulations (EAR) (15 CFR Parts 368 through 399) issued by the Department of Commerce, Bureau of Industry and Security (BIS), prescribe licensing procedures for items under its jurisdiction. Controls on the issue of export licenses are based on considerations of national security, the fostering of U.S. policy and international responsibilities, the necessity for protecting the domestic economy from an excessive drain of scarce materials, and the reduction of the serious inflationary impact of abnormal foreign demand. The Commerce Department and BIS home page is at <http://www.bis.doc.gov>.

Items controlled by the Department of Commerce for export are listed on the commerce control list (CCL). The list is very detailed and lists items that may be exported to a certain country.

Dual-use items are items that were designed with no intrinsic military function but which may have a potential military application, i.e., computers, jeeps, trucks, light aircraft, and global positioning system (GPS). The Department of Commerce is charged with coordinating requests for such items that fall into this category of dual-use. However, once a dual-use item is modified for specific military use, the DoS, DoD, and Department of Commerce resolve the commodity jurisdiction of the article, and DoS notifies DoD and Department of Commerce that the article falls under the DoS control and is listed on the USML.

## **Exports through the Department of State**

Section 38, AECA, authorizes the president to control the import and export of defense articles and services, to designate such items as constituting the USML, and promulgate implementing regulations. By executive order (E.O. 11958), the president has delegated his responsibilities to the secretary of state, except that the designation of items as defense articles and services for export control requires the concurrence of the secretary of defense. Those responsibilities related to the control or regulation of imports of defense articles and defense services are delegated to the Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives except that designation of items as defense articles and services for import control require concurrence of the secretaries of state and defense.

The ITAR, 22 CFR Parts 120-130, implements the AECA statutory authority to control the export and import of defense articles and services. By virtue of delegations of authority by the secretary of state, these regulations are primarily administered by the Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs, Department of State. The ITAR is available on the Internet at <http://www.pmdtc.gov/reference.htm#ITAR>.

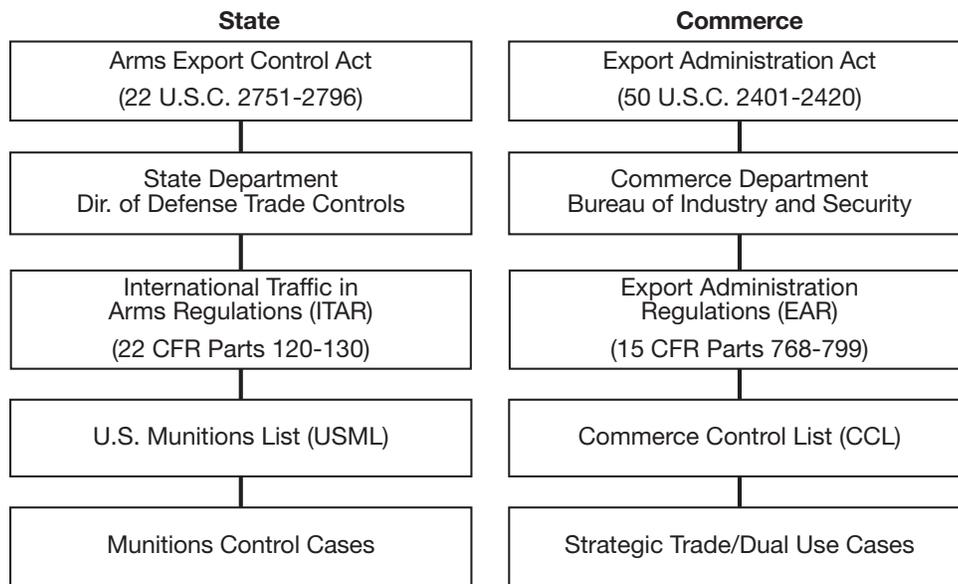
DDTC is responsible for issuing export licenses for those items on the USML. The USML can be found in Section 121.1 of the ITAR and is also discussed in SAMM, C4.3. While not a list of specific

items (e.g., M-16, M-1A1, F-4, etc.), the USML generically designates articles, services, and related technical data as defense articles and defense services in accordance with Section 38, AECA. Those defense articles preceded by an asterisk on the USML are designated significant military equipment (SME) that Section 120.7 of the ITAR defines as articles for which special export controls are warranted because of their capacity for substantial military utility or capability. Anything that is classified is considered to be SME.

The Directorate of Defense Trade Controls processed approximately 67,000 defense-related license requests in fiscal year 2006 from U.S. contractors. The numbers of license requests are increasing each year. Approximately 20 percent of these are forwarded to DTSA and the military departments (MILDEPs) for further review. The DoS regulates permanent exports, temporary exports, and temporary imports of defense articles into the U.S., and the Department of Justice regulates permanent imports of defense articles (22 CFR Parts 47, 178, and 179).

Figure 7-2 provides a comparative review of the legislative and regulatory authorities for the DoS and Department of Commerce in regulating exports.

**Figure 7-2  
Comparing Department of State and Department of Commerce**



### **CONTROLLED UNCLASSIFIED INFORMATION**

Controlled unclassified information (CUI) is a DoD term used to describe collectively all unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations. For the U.S., CUI is official government information that is unclassified, but that has been determined by designated officials to be exempt from public disclosure under the Freedom of Information Act (FOIA), which is designed to make government information available to the public and thus requires openness in government. It is not designed to protect information. It provides that the public is entitled to access to agency records, unless the record is exempt from disclosure. There is no executive order to implement FOIA. Government agencies apply their own unique markings to identify the information. Consequently DoD has several policy directives covering the disclosure of official information.

- DoDD 5230.9 contains policies and procedures for the release of information for publication or public release
- DoDD 5200.21, 5230.24, and 5230.25 govern the release of DoD technical information
- DoD 5400.7-R contains the DoD policies and procedures governing FOIA requests. Official information that meets the standards for security classification is classified and protected in compliance with E.O. 12958 and DoD 5200.1-R
- DoDD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, provides procedures for the dissemination and withholding of unclassified technical data

### **Freedom of Information Act**

Congress has stated the U.S. public generally has the right to know what its government is doing. FOIA requires government information to be made available to the public unless the information falls within one of nine exemption categories described in the Act and the appropriate USG official determines it should be withheld from disclosure.

- Exemption 1 is classified information. The FOIA permits the withholding of any information properly and lawfully classified under the provisions of E.O. 12958. The other eight exemption categories deal with unclassified but generally sensitive information.
- Exemption 2 permits the withholding of information which pertains solely to the internal rules and practices of a government agency.
- Exemption 3 permits the withholding of information that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld.
- Exemption 4 permits withholding information such as trade secrets and commercial and financial information obtained from a company on a privileged or confidential basis which, if released, would result in competitive harm to the company.
- Exemption 5 protects inter- and intra-agency memoranda which are deliberative in nature.
- Exemption 6 provides for the withholding of information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of personal privacy of individuals.
- Exemption 7 permits withholding records or information compiled for law enforcement purposes that could reasonably be expected to interfere with law enforcement proceedings; would deprive a person of the right to a fair trial or impartial adjudication; could reasonably be expected to constitute an unwarranted invasion of personal privacy of others; disclose the identity of a confidential source; disclose investigative techniques; or could reasonably be expected to endanger the life or physical safety of any individual.

- Exemption 8 permits withholding records or information contained in or relating to examination, operation or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.
- Exemption 9 permits withholding records or information containing geological and geophysical information and data (including maps) concerning wells.

For many years, it has been DoD policy to place distribution statements on documents containing unclassified scientific and technical information which was produced either within DoD or on its behalf by others. Until recently, however, this policy was only marginally directed toward restricting the disclosure of such information to the public and thus to foreign persons. Moreover, although it was the policy to apply such distribution markings, the practice did not always conform to the policy. The result was that sensitive scientific and technical information occasionally found its way into the public domain, including the foreign public. Public Law 98-94, 24 September 1983, provided the secretary of defense with the authority to withhold from the public critical technologies under above described exemption three of the FOIA. For more specific information on FOIA as it relates to LOAs and FMS procurement contracts, refer to SAMM, Section C3.4, Release of Information.

### **FOREIGN DISCLOSURE AND THE NATIONAL DISCLOSURE POLICY**

Specific policies and controls have been established and remain in place for the transfer of classified military information (CMI) and CUI militarily critical technology, defense articles, and defense services.

The NDP establishes a framework for the approval or denial for the transfer of CMI to foreign governments. Basic authority and policy for transferring classified information are contained in NSDM 119, which is implemented by the classified publication, *National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations*, short title NDP-1.

Effective implementation of NDP-1 is the responsibility of the [USD (P)]. Disclosure officials are authorized (but not automatically obliged) to disclose information up to the classification levels indicated in the NDP annex for each category of information. And most importantly, each disclosure decision is made on a case-by-case basis.

#### **Classified Military Information and Disclosure Decisions**

Under the NDP, classified information that has been developed by or for the DoD or is under its jurisdiction or control. There are three criteria that must be satisfied prior to making a disclosure decision. The release must satisfy U.S. foreign policy towards the intended recipient government, and toward other governments in the region. Release must not jeopardize U.S. military security. The third criteria is there must be an evaluation of the proposed recipient government's capability and intent to provide substantially the same degree of protection the U.S. gives to the information or material.

#### **National Disclosure Policy Committee/Exceptions to National Disclosure Policy**

NSDM 119 and DoDD 5230.11 require the establishment of a national level interagency, national disclosure policy committee (NDPC), to formulate, administer, and monitor national disclosure policy. General members of the NDPC include the secretary of state, secretary of defense (chairman), secretary of the army, secretary of the navy, and secretary of the air force, and the Joint Staff. These general members have a broad interest in all committee operations and vote on all issues that come before the committee. Other organizations such as the Central Intelligence Agency (CIA), DIA, and many

others may vote on issues in which they have a direct interest. When an exception to NDP (E-NDP) is required, because disclosure criteria cannot be met within the previously authorized classification level, such exceptions can be granted only by the NDPC, the secretary of defense, or the deputy secretary of defense. A request for an E-NDP must be sponsored by a NDPC member, normally the cognizant MILDEP.

The NDP-1 annex states only the maximum classification level of information that can be released and in itself does not authorize disclosures. The secretaries of the MILDEPs have generally been delegated authority by the NDP-1 to decide if CMI under their control can be released. The policy and guidance for implementing NDP-1 is contained in the DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*. This directive states that the MILDEPs will release CMI in accordance with the NDP-1 annex only if all of the following five conditions or criteria, originally outlined in NSDM 119, are met:

- Disclosure is consistent with U.S. foreign policy and national security objectives, e.g., in support of defense objectives
- Disclosures, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology or operational capabilities
- The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the U.S. The intent of a foreign government to protect U.S. CMI is established in part by the negotiation of a general security of military information agreement (GSOMIA) or other similar international agreement
- Disclosure will result in benefits to the U.S. at least equivalent to the value of the information disclosed.
- The disclosure is limited to information necessary to accomplish the purpose for which disclosure is made.

One further point must be emphasized. If the classification of the information proposed for disclosure exceeds the country's eligibility in the NDP-1 annex, or if the policy criteria cannot be met, then the proposed disclosure must be denied or an exception to policy must be obtained from the NDPC. Moreover, even if the U.S. disclosure official has determined that eligibility in the NDP-1 annex exists and that all policy criteria have been met, disclosures of classified military information may not be made until the affected originator's approval has been obtained or appropriate authority to disclose has been received. All disclosure authority rests in the first instance with the head of the department or agency which originates the information. In addition, all disclosure officials must be certain that they possess the required authority to disclose the information in question. The secretary of defense and the deputy secretary of defense are the only officials who may grant unilateral exceptions to the NDP. Under DoD Directive 5230.11, the secretary of defense has delegated disclosure authority to the secretaries of the MILDEPs and other DoD officials whose decisions must be in compliance with NDP-1. They are required to appoint a principal disclosure authority at component headquarters level to oversee the disclosure process and a designated disclosure authority at subordinate command and agency is delegated. SAMM, Section C3.3, "Disclosure of Classified Military Information," provides additional information on the national disclosure process as it relates to security assistance.

## **Security Survey**

To assist the NDPC and those with disclosure authority to make decisions on disclosure of military technology to other governments, international security agreements agreed to and signed at the

government-to-government level must be developed. Before these agreements can be written, security survey teams are sent to the respective countries to review and evaluate the foreign governments and industries ability to protect USG information. The teams are usually made up of members of the DoS and DoD. The primary areas reviewed by the teams are personnel security, information security and physical security to make sure that if the respective government is allowed access to USG information, it will be able to protect the information at least at the same level as it would be protected in the U.S.

### **International Security Agreements**

Before classified information is released outside the executive branch of the USG, E.O. 12958 requires that written assurances must be obtained that the information will be afforded proper protection. In situations where classified information is being made available to foreign governments, these assurances may be secured in several ways. First, they are included in the standard terms and conditions of FMS LOA, Section 2, “Conditions - General Purchaser Agreements.” See later Chapter 8, “FMS Contractual Agreements,” of this textbook for further information. They may also be the subject of diplomatic notes, memoranda of understanding and similar correspondence. Separate international agreements known as GSOMIAs have been concluded with over sixty countries. Since they are government-to-government agreements, the other governments send teams to the U.S. to ensure U.S. compliance with the agreements just like the USG would send survey teams to their countries. GSOMIAs typically include the following topics:

- Protection, third-party transfer, and intellectual property rights provisions
- Classified information transfer mechanism (government-to-government)
- Definition of classified information
- Reciprocal provision for security expert visits
- Requirements for investigations in case of compromise
- Industrial security procedures
- Visit request procedures
- Limitations on level of classification

### **Disclosure Planning**

DoD Directive 5230.11 requires that planning for possible foreign involvement should start at the beginning of the weapon system acquisition process to facilitate decisions on disclosure in support of foreign sales or cooperative programs. The key documents developed in the system acquisition process that relate to potential technology transfer are covered in Chapter 9, “System Acquisition Documents Associated with Foreign Military Sales” of the DoD Directive 5230.11.

### **False Impressions**

It is the policy of the U.S. to avoid creating false impressions of its intention to provide classified military material, technology, or information. Lack of strict adherence to this policy may create problems. Much military hardware is unclassified; however, this same unclassified hardware, if sold, may require the release of sensitive classified information for its operation or maintenance, or for the foreign recipient to receive training on it. Therefore, the disclosure decision must be made based on the classification level of all information which may be required for release if the system were to be acquired. If the proposed foreign recipient is not authorized to receive the highest level of classified

information required, no information, not even unclassified information, may be released or discussed until the required authority is obtained. This means that there can be no weapon specific information, and no release of FMS price and availability (P&A) data until authority is obtained to release the highest level of classified information ultimately required for disclosure.

Thus, designated disclosure authorities, in order to avoid false impressions, must authorize in advance proposals to be made to foreign governments that could lead to disclosure of classified military information, technology, or material.

## **EXPORT APPROVAL AND LICENSE PROCESS**

Before discussing the approval and license process for the authorized export of a military article or service we first must define the term “export.” To paraphrase the ITAR Section 120.17 an export is sending or taking defense articles out of the U.S. in any way. That includes transferring registration, ownership, or control of an item on the USML to a foreign person. It also includes disclosing orally or visually any defense article to a foreign person in the U.S. or abroad. That means if you discuss U.S. military technology anywhere with a foreign person that does not have a need to know the information and you do not have a license to do so, this is an illegal transfer. Part 127 of the ITAR covers violations and penalties of unlawful export, re-export or re-transfer or attempt to re-transfer of any defense article or technical data for which a license or written approval is required from the DoS.

### **Licenses for the Export of Defense Articles**

Part 123 and 125 of the ITAR provides for the licensing requirements for the export or temporary import of defense articles into or out of the U.S.. Any person who intends to export or to import temporarily a defense article must obtain the approval of the State Department’s Directorate of Defense Trade Controls (PM/DDTC) prior to the action unless there is a regulatory exemption.

Section 123.10 provides for the form DSP-83 to certify the non-transfer and use assurance certificate required for the export of significant military equipment and classified articles and technical data. A license will not be issued until a completed Form DSP-83 has been received by DDTC. The form is to be executed by the foreign consignee, the foreign end-user, and the applicant. Application for export license for the export or import of classified defense articles and services must be made on DoS form DSP-85 [see SAMM, Figure C3.F3]. Application must be made by a U.S. national in accordance with the provisions of Sections 125.3, 125.7, and 125.9 of the ITAR.

Table 7-2 shown on the next page, provides a guide as to which form is required for the export of munitions list items through either FMS or direct commercial sale.

### **Export License Applications Staffing within Department of Defense**

The License Directorate of DTSA is the entry point for export requests from the DoS and Department of Commerce. It is the technical responsibility of this directorate’s staff to ensure that the MILDEPs, appropriate DoD agencies, and the technical staff of the under secretary of defense for acquisition technology and logistics review applicable export requests or munitions cases. To expedite the licensing process, the DoS delivers these cases for concurrent review by those military services and DoD agencies and components which the DoS believes have an interest in the cases.

After receiving recommendations from the DoD review, the DTSA License Directorate develops the DoD position in concert with DTSA technical and policy staffs, and forwards the position to the DoS. Most differences within DoD are resolved at the working level. Those that cannot be so resolved are referred to the International Technology Transfer Panel (ITTP) for resolution.

**Table 7-2  
Forms to Be Used for Export of Munitions List Items**

<u>Activity</u>	<u>Foreign Military Sales</u>	<u>Commercial Sales</u>
Registration statement	N/A for gov't shipment	DS-2032
Permanent export of unclassified defense articles and related unclassified technical data	LOA and DSP-94	DSP-5
Permanent/temporary export or temporary import of classified defense articles and related classified technical data	DSP-85 and DSP-94	DSP-85 (with DSP-83)
Temporary export of unclassified defense articles	DSP-73	DSP-73
Temporary import of unclassified defense articles	DSP-61	DSP-61
Non-transfer and use assurances for export of defense articles and services	N/A (Already included in LOA)	DSP-83
Shipper's export declaration	Department of Commerce Form 7525-V	Department of Commerce Form 7525-V

### **Foreign Military Sales License Exemption**

To paraphrase Section 126.6(c) of the ITAR, when using the FMS program a license from the DoS is not required if the defense article or technical data or a defense service to be transferred was sold, leased or loaned by the DoD to a foreign country or international organization using the LOA as authorization.

### **Commercial Agreements Requiring Approval by Department of State**

Besides regular export licenses, the ITAR provides for commercial agreements that, when approved, provide authorization to export certain types of technical information and services. These differ from regular export licenses in that they are broader in scope, more flexible, and remain in effect for longer periods of time. These agreements are typically for ongoing projects rather than a one-time export. The ITAR recognizes three categories of such agreements:

- Technical assistance agreement (TAA). An agreement (e.g., a contract) for the performance of defense services or the disclosure of technical data, as opposed to an agreement granting right of license to manufacture defense articles [22 CFR 120.22]
- Manufacturing licensing agreement (MLA). An agreement (e.g., a contract) whereby a U.S. person grants a foreign person an authorization or a license to manufacture defense articles abroad and which involves or contemplates the export of technical data or defense articles or the performance of defense services or the use by the foreign person of technical data or defense articles previously exported by the U.S. person [22 CFR 120.21]

- Distribution agreement. A contract between a U.S. person and a foreign person to export unclassified defense articles to a warehouse or distribution point outside the U.S. for subsequent resale. These agreements contain conditions for special distribution, end-use and reporting [22 CFR 120.23]

The use of the term person means a natural person as well as a corporation, business association, partnership, society, trust or any other entity, organization or group, including governmental entities [22 CFR 120.14]

## **INTERNATIONAL VISITS AND ASSIGNMENTS**

### **Visit Procedures**

DoDD 5230.20, *Visits and Assignments of Foreign Representatives*, sets forth standard procedures concerning requests for visits, certification of liaison officers and personnel exchange programs. SAMM, Section C3.5.5. “Visits, Assignments and Exchange of Foreign Nationals,” provides further discussion relating to security assistance.

Foreign representatives, i.e., foreign nationals or U.S. citizens or nationals who are acting as representatives of a foreign government, firm, or person, may be authorized to visit DoD components or U.S. defense contractor facilities only when the proposed visit is in support of an actual or potential USG program (e.g., FMS, USG contract, or international agreement). The DoD and U.S. defense contractors receive over 230,000 foreign visitors annually on matters related to mutual security and cooperation. These visits play a vital part in the exchange of information and technology as a part of U.S. international commitments. These visits account for more transfer of CMI and CUI than all other transfer mechanisms combined.

The International Visits Program (IVP) established policy and procedures to control international visits and the information to be transferred during those visits. DoD policies and procedures pertaining to foreign visits are designed to achieve three objectives.

- To facilitate administration arrangements and otherwise plan visits
- Provide a vehicle for consideration of proposed export/disclosure decisions related to the visit and record the decision(s)
- To provide a vehicle for obtaining the required security assurance regarding the security clearance, need-to-know, and sponsorship from the visitor’s government if classified is involved

There are three types of visits that may be authorized:

- A one-time visit (normally less than thirty days)
- For recurring contacts for a period of time, normally not exceeding one year
- For an extended period of time, e.g., certifications of liaison officers, normally up to one year or term of contract or applicable export license

For an emergency, a one-time visit may be submitted for approval less than twenty-one working days before the visit start date. Emergency visits may only be authorized if failure to make the visit would jeopardize performance on a contract or program, or cause the loss of a contract opportunity. These authorities may not be used to employ foreign nationals.

Although security assistance offices (SAOs) do not approve visit clearances, they do serve as coordinators of contractor and DoD component requests to visit abroad, e.g., for security assistance or cooperative research, development, test, and evaluation (RDT&E) programs. In coordinating such visits, DoD 4500.54-G, DoD *Foreign Clearance Guide*, and the *Defense Attaché Manual* prepared by the DIA provide useful guidance.

Except for those visits approved by the MILDEPs, the National Security Agency/Central Security Service, and the immediate Offices of the Secretary and Deputy Secretary of Defense; the Director, DIA administers requests for visits and extended visits for the OSD, the Joint Staff, defense agencies, and their contractors. The MILDEPs approve or deny, or decline to render a decision on visits, liaison officer certifications and exchange personnel and for their own departments and their applicable contractors. An international agreement is necessary for personnel exchange programs and on-site assignments of liaison officers. Correspondence with DoD contractors relative to approved foreign visits shall be forwarded to the cognizant DSS regional office for transmittal to the contractor.

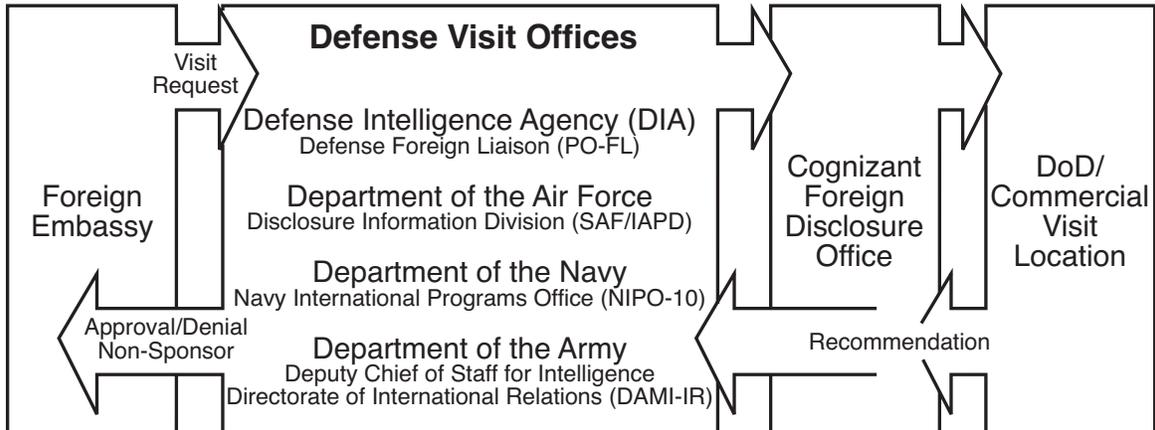
Requests by foreign embassies shall normally be submitted at least thirty days in advance for visits and ninety days in advance for liaison officer certifications. Visits carried out under the terms of an approved certification, extended visit authorization, or one-time visit may take place after coordination with the office to be visited and at least seventy-two hours advance notice. Requests for visits and certifications submitted by foreign embassies should follow the examples contained in DoDD 5230.20. Standardized notifications shall be used to advise foreign embassies of final action on requests for visits and accreditations as contained in DoDD 5230.20. As noted above, the security policy automation network (SPAN) processes and records visit requests it receives and decisions on such requests. This part of SPAN is called the foreign visit system (FVS). The FVS was developed to enhance security and provide consistent application of policy in dealings with other governments.

Visit requests are sent to one of four defense visit offices (DVO) located in Army, Navy, Air Force, and the DIA. The DVOs staff out the visit requests to foreign disclosure offices in the field that contact the organizations to be visited to see if they will accept the visits. The DVO reviews the comments from the field and renders a decision which is returned over the same electronic path used for submission to the embassy of the country submitting the visit request. Figure 7-3 provides an overview of the international visit program within DoD. At any time, participating activities have immediate access to all visit request status information. For point of contact and further information on FVS, users should contact the Director, Policy Automation Directorate at commercial (703) 697-5495 or DSN 227-5495.

Notification of approval of a foreign request for a visit or certification to a DoD component shall be forwarded to the contract officer of the DoD component concerned, or where the representative will visit. This notification shall contain adequate guidance regarding the parameters of the subject visit and the maximum permissible level of classified information that has been authorized for disclosure.

Disclosures of classified information to foreign visitors and certified foreign representatives shall be limited to releasable oral and visual information, unless the release of documentary information is specifically authorized in an approved visit request or letter of acceptance for certified officials, or when the U.S. contractor has secured an export license specific to the documentation intended for release. When documentary release is authorized, the visitor must have courier orders.

**Figure 7-3  
International Visit Program**



However, if classified information is to be disclosed, a visit request must be submitted even though the contractor has a valid export authorization or license. In this case, the visit request is used to pass the security assurance on the visitors. Requests for classified documentary information resulting from a foreign visit shall otherwise be processed through normal foreign disclosure channels. In either case classified documentary information shall be transferred through government-to-government channels, unless the visitor is also acting as a courier and has courier orders.

DoD officials who wish to invite foreign representatives to visit a DoD component, or who wish to have a foreign national certified to the component, shall coordinate their actions with DIA or the MILDEP concerned before extending an invitation.

A request of visit authorization is not required at a contractor facility when the information to be disclosed is unclassified and not subject to export controls, the information is unclassified but is subject to export controls, but a contractor has an export license for its export. It is not required at a DoD facility when the facility is open to the public, the information is open for public release according to service regulations, or for non-U.S. citizen DoD employees policies and procedures already exist to authorize access by such personnel.

**Other Visit Processes**

A “hosted visit” occurs when a senior foreign national is extended an invitation by a DoD counterpart.

“Emergency visits” may be approved only for legitimate program, project or contract purposes. The visit request can not be amended.

“Amendments” to visits may be used only to change dates (no earlier dates) and list of visitors. The information to be discussed during the visit can not change.

**Defense Personnel Exchange Program**

The defense personnel exchange program (DPEP) includes the exchange of personnel between the U.S. military services and their counterparts of friendly governments for assignment to established positions within their force structure. This exchange is implemented under an agreement conforming to DoDD 5530.3, *International Agreements*. Assignments can be negotiated as a reciprocal exchange of military personnel. Also, civilian position assignments such as intelligence analysts, scientists and

engineers, medical personnel, and administrative specialists may be negotiated. Exchange personnel perform the functions of the specific position within the organization to which they are assigned. Since they are not designated officials of their government, classified information may not be released into their permanent custody. They may only be given oral or visual access to specific classified information authorized in the applicable delegation of disclosure letter (DDL). Written procedures must be developed to prevent inadvertent disclosure of classified or controlled unclassified information as described in DoDD 5230.20, *Visits and Assignments of Foreign Representatives*. Such personnel may not be given access to information classified under the Atomic Energy Act of 1954, as amended. DPEP assignees may not act as a representative of their government or the USG.

### **Foreign Attendance at Classified Meetings Leading to Contract Opportunities**

The USG has entered into cooperative agreements with allies and other friendly nations that allow the exchange of information in specific areas of mutual interest required for their participation in contractual opportunities. See later Chapter 13, “International Armaments Cooperation Programs,” for discussion of reciprocal procurement memoranda of understanding. Planning for meetings that may lead to contracts for foreign nationals shall be based on the assumption that there will be foreign attendance. DoDD 5200.12, *Conduct of Classified Meetings*, contains policies and procedures for sponsoring and conducting meetings involving classified information attended by foreign nationals.

### **Visits Overseas by DoD Personnel**

The policy for overseas travel of DoD personnel is covered under DoDD 4500.54, *Official Temporary Duty Travel Abroad*, and DoD 4500.54-G, *Foreign Clearance Guide* (FCG). DoD components must appoint a responsible official and follow the FCG. Normally thirty days advance notice is needed before travel. Procedures also must be established to ensure disclosure authorization has been obtained if classified or export controlled unclassified information is to be divulged. A “theater clearance” is required for visits to a U.S. military facility overseas as specified in the FCG. A “country clearance” is required for visits to a host government facility or contractor facility for classified discussions.

## **INTERNATIONAL TRANSFERS**

### **United States Classified Contracts with Foreign Firms**

A USG agency awards or permits one of its contractors to award a classified contract to a foreign contractor, only if the classified information involved has been approved for release or is determined to be releasable to the government of that country under the national disclosure policy. In addition, the foreign government concerned must have entered into a security agreement with the U.S. under which it agrees to protect U.S. classified information released to it. User agency responsibilities are contained in DoD 5220.22-R, *Industrial Security*.

### **Transmission of Classified Materiel to Foreign Governments**

Transmission of classified materiel to foreign governments, either to addresses in the U.S. or outside the U.S., must be on a government-to-government basis, e.g., U.S. Postal Service registered mail through an Army or Air Force APO or Navy FPO postal service; and such transmissions should be in accordance with DoD 5200.1-R, *Information Security Program*, Chapter VIII. Disclosures or denials are recorded in the SPAN. To assure compliance, each contract agreement, LOA, or other arrangement that involves the release of classified materiel to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials and applicable foreign governments prior to release of the

materiel. Government arrangements cannot be used as a means to bypass the ITAR. More information about the transfer of classified items may be found in Chapter 11, “Foreign Military Sales Transportation Policy” of this text book under classified shipments.

## **DEFENSE SECURITY SERVICE ROLE IN INTERNATIONAL PROGRAMS**

The role of the DSS is to provide government contracting agencies with an assurance that U.S. defense contractors are both eligible to access and properly safeguard any classified information for which it is entrusted. In fulfilling this obligation, DSS administers the national industrial security program (NISP) operating on behalf of the under secretary of defense for intelligence [USD (I)]. DSS does not develop industrial security policy. DSS implements industrial security policy established by [USD (I)], and for international programs established by the under secretary of defense for policy [USD (P)]. Prior to access by a defense contractor to classified information, the contractor must be sponsored for a facility clearance. This sponsorship is based upon a bona fide procurement need, and is submitted to DSS by an U.S. or foreign government contracting activity or by another contractor already cleared under the NISP. DSS will conduct a facility clearance survey to determine the contractor’s eligibility for access to classified information, and will review the contractor’s organizational structure and key management personnel, and adjudicate any existing foreign ownership, control, or influence (FOCI). Once a favorable determination is made and a facility clearance is granted, the contractor will execute a security agreement with the USG, a legal contract to abide by the DoD 5220.22-M, *National Industrial Security Operating Manual* (NISPOM). The NISPOM is a contractually binding document and mandates industrial security practices for contractors. The NISPOM derives its authority from the ITAR and implements applicable statutes, executive orders, national directives, and international treaties toward the protection of classified information.

The DSS verifies the export of classified articles and technical data against the license or the U.S. company’s empowered official’s certification, assures that secure means of transfer have been arranged, and endorses the license back to the DoS. DSS oversees plant visits by foreign nationals and ensures that companies have adequate technology control plans in place for long-term foreign national visitors, foreign national employees, and for FOCI situations. DSS ensures appropriate transportation plans are in place for commercial overseas shipments of classified material and approves contractor international hand carriage arrangements. Additionally, DSS provides security assurances to other governments for U.S. contractor facilities and personnel and obtains assurances on foreign facilities and personnel. It advises cleared contractors concerning program protection plans, ensures compliance, and trains DoD and contractor personnel on program protection planning. The DSS provides support to cleared contractors operating overseas, and monitors their compliance with the NISPOM. Finally, DSS provides counterintelligence (CI) support to cleared contractors, including CI awareness briefings. More information about DSS can be found at its web site <http://www.dss.mil>.

### **Technology Control Plan**

The technology control plan (TCP) provides guidance on the control of access to classified and unclassified export controlled information by foreign employees and long-term foreign national visitors of a cleared U.S. contractor’s facility. The TCP explains how the requirements of the ITAR, the EAR, and the NISPOM will be carried out. The TCP is developed by the U.S. contractor, based on the requirements of the ITAR, Section 126.13(c), and the NISPOM. The content regarding information access and restrictions may be derived from other documents provided by the USG (for example, the license provisos and the program security instructions or the form DD 254). The DSS will assist the contractor in developing the TCP and will approve it. A specific TCP may not be required if the company’s internal security operating procedures, e.g., standard practice procedures (SPP) contain the

necessary details. If security requirements are partially contained in a document such as an SPP and additional export control procedures are in a TCP, the latter must refer to the applicable portions of the other document.

### **Defense Industrial Security Clearance Office**

The defense industrial security program (DISP) establishes procedures for safeguarding classified defense information which is entrusted to contractors. Included in these procedures is a system for determining the eligibility of industrial personnel for access to classified defense information. This function is performed centrally by the Defense Industrial Security Clearance Office.

## **FOREIGN GOVERNMENT AND NORTH ATLANTIC TREATY ORGANIZATION INFORMATION**

### **Foreign Government Information**

Foreign government information (FGI) is information that has been provided by a foreign government or international organization, or jointly produced, with the expectation that the information will be treated “in confidence.” The information may be classified or unclassified. In addition to TOP SECRET, SECRET, and CONFIDENTIAL, many foreign governments have a fourth level of security classification, RESTRICTED as well as controlled unclassified information (CUI) that is provided in confidence.

As a result of numerous international security and program agreements, the NATO security agreement obligates member nations to adopt common standards of protection. U.S. national policy affords FGI a degree of protection equivalent to that provided to it by the originating government or international organization. Since foreign government accountability and control measures often exceed those of the U.S., the U.S. applies separate security procedures to protect FGI. Because most exchanges are with NATO and its members, the NATO standards are used as the baseline for U. S. procedures for protecting FGI.

FGI, including RESTRICTED and foreign government CUI, must be classified under E.O. 12958 in order to receive protection equivalent to that provided by the originating government or organization, as stipulated in E.O. 12958 and international agreements. FGI that is classified by the originating government or organization will be marked with the equivalent U.S. classification, if it is not already marked in English, and the identity of the originating government or organization. Foreign government RESTRICTED and CUI are to be marked, “Handle as CONFIDENTIAL - Modified Handling Authorize.” FGI cannot be provided to third country entities or used for a purpose other than that for which it was provided without the consent of the originating government or organization. It must receive protection commensurate with that provided by the originating government or organization. The procedures for handling FGI are contained in two national policy documents, E.O. 12958, the presidential directive on safeguarding classified national security information, and DoD 5200.1-R.

Basic handling procedures for FGI are as follows:

**Storage.** The same as U. S. information of the same classification, but FGI is to be stored separately. FGI that is marked “Handle as CONFIDENTIAL – Modified Handling Authorized” is stored in the same manner as U. S. FOUO information, e.g., in a locked desk or file cabinet.

**Access.** Using the need-to-know principle, no access by third country persons without the prior consent of the originating country or organization.

**Transmission.** The same as U.S. classified information of the same classification level; however, express commercial carriers cannot be used. Receipts are required for international transfers

wherever they occur, although exceptions are made for RESTRICTED information. There are no receipts for CUI.

**Records.** TOP SECRET - Receipt, dispatch, internal distribution, annual inventory, and destruction (two persons); SECRET - receipt, dispatch, internal distribution, and destruction; CONFIDENTIAL - receipt and dispatch, and as required by originator.

### **North Atlantic Treaty Organization Disclosure Security Procedures**

Basic security requirements are necessary to comply with the procedures established by the U.S. Security Authority for the North Atlantic Treaty Organization (USSAN) for safeguarding NATO information involved in international programs. DoDD 5100.55 contains the terms of reference designating the secretary of defense as the USSAN for the USG. These requirements are consistent with USSAN Instruction 1-70, 5 April 2007, which were implemented by DoDD 5100.55, DoD C-5220.29, and the NISPOM. The foregoing documents must be consulted for specific details.

#### ***Classification Levels***

NATO security regulations prescribe four levels of security classification, COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). The terms COSMIC and NATO indicate that the material is the property of NATO. Another marking, ATOMAL, is applied to U.S. restricted data or formerly restricted data and United Kingdom atomic information that have been released to NATO. Once disclosed to NATO, the classified information loses its country of origin identity and is marked as NATO information. Thereafter, access, dissemination, and safeguarding of the information is accomplished in accordance with NATO procedures. The information remains the property of the entity that originated or furnished it.

#### ***Access Requirements***

DoD and contractor employees may have access to NATO classified information only when access is required in support of a U.S. or NATO program that requires such access, i.e., need-to-know.

Access to NATO classified information requires a final DoD personnel clearance (except for RESTRICTED) at the equivalent level and a NATO-specific security briefing discussed later in this chapter. A personnel security clearance is not required for access to NATO RESTRICTED information.

Foreign nationals from nations not members of NATO may have access to NATO classified information only with the consent of the originating NATO member nation or civil or military body. Requests with complete justification, as described in the NISPOM, will be submitted through the cognizant security office (CSO).

#### ***North Atlantic Treaty Organization Disclosure Briefings***

Prior to having access to NATO classified information, contractor and government personnel must be provided a NATO security briefing. The contractor's facilities security officer (FSO) will initially be briefed by the CSO. Annual refresher briefings will be conducted. When access to NATO classified information is no longer required, personnel will be debriefed, as applicable, and acknowledge their responsibility for safeguarding the NATO information.

## ***Marking and Handling North Atlantic Treaty Organization Disclosure Documents***

Normally, NATO documents do not carry portion markings as are required for U.S. classified documents. Nevertheless, all classified documents created by U.S. contractors and DoD components will be portion-marked.

NATO classified documents, and NATO information in other documents, may not be declassified or downgraded without the prior written consent of the originating NATO member nation civil or military body. Recommendations concerning the declassification or downgrading of NATO classified information are to be forwarded to the central U.S. registry (CUSR) via the CSO by contractors and via command or organizational channels by government personnel.

NATO classified documents, except for NATO RESTRICTED, are to be stored as prescribed in DoDD 5100.55 and the NISPOM for U.S. documents of an equivalent classification level. However, NATO documents must not be co-mingled with U.S. or other documents. NATO restricted documents may be stored in locking filing cabinets, book cases, desks, other similar locked containers that will deter unauthorized access, or in a locked room to which access is controlled.

## ***International Transmission of Classified North Atlantic Treaty Organization Disclosure Documents***

NATO policy requires the establishment of a central registry for the control of the receipt and distribution of NATO documents within each NATO member country. The CUSR, located in the Pentagon, establishes sub-registries at USG organizations for further distribution and control of NATO documents. Sub-registries may establish control points and sub-control points as needed within their activities for distribution and control of NATO documents. COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be transferred through the registry system.

## ***Marking the Documents***

When a document containing U.S. classified information is being specifically prepared for NATO, the appropriate NATO classification markings will be applied to the document only after the U.S. information contained in the document is authorized for release to NATO. If the information is to be provided pursuant to a NATO contract, the requirements of the NATO security aspects letter and security requirements checklist will be followed. However, if U.S. classification guidance for the U.S. information is not consistent with NATO classification guidance, the matter must be forwarded to the CSO for resolution.

## **Transmission**

The CSO will provide transmission instructions to the contractor:

The material must be addressed to a U.S. organization at NATO, e.g., U.S. mission to NATO, U.S. national military representative to Supreme Headquarters Allied Powers Europe (SHAPE), or the U.S. representative to the NATO Maintenance and Supply Agency which will place the material into NATO security channels. The material must be accompanied by a letter to the U.S. organization that provides the necessary transfer instructions and provides assurances that the material has been authorized for release to NATO. The material will be properly double-wrapped as described in the NISPOM and DoDD 5100.55. However, the inner wrapper will be addressed to the intended NATO recipient, and the outer wrapper shall be addressed to the U.S. organization at NATO.

Classified material is sent to NATO via registered mail and will be routed only through the U.S. postal service and U.S. military postal channels to the U.S. organization that will affect the transfer. The use of express mail is not authorized.

## **Multinational Industrial Security Working Group Documents**

The multinational industrial security working group (MISWG) is composed of the NATO countries, less Iceland, plus Austria, Sweden, and Switzerland. It is an ad hoc group organized to rationalize different security practices and develop standard procedures for multinational programs. Although initially developed to standardize procedures among NATO member nations working jointly on a non-NATO project, the MISWG documents contain procedures that may be used in any bilateral or multilateral program or project, including NATO projects. NATO, NATO countries, and other countries have adopted the MISWG procedures. Therefore, they should be used as the baseline in preparing individual arrangements or when consolidated in a program security instruction (PSI), MISWG document 5, for international programs.

Most of the MISWG documents provide procedural guidance for implementing security requirements for international programs. Other MISWG documents are used in preparing the content of international agreements and contracts involving access to classified information. The DSS may approve the use of the documents in individual commercial programs. However, the Designated Security Authority, DUSD (TSP&NDP), will approve the use of the documents when they are required by an international agreement such as in a PSI.

### **COMMITTEE ON FOREIGN INVESTMENT IN THE U.S. AND FOREIGN OWNERSHIP, CONTROL OR INFLUENCE**

The Exon-Florio Amendment to the Omnibus Trade and Competitiveness Act of 1988, as amended by the Defense Authorization Act for Fiscal Year 1993, empowers the president to suspend, prohibit or dissolve (“block”) foreign acquisitions, mergers and takeovers of U.S. companies. The president has broad authority to block a transaction under the statute if he determines the foreign interest acquiring control might take action that threatens to impair the national security. The 2007 Foreign Investment and National Security Act requires mandatory investigation where critical infrastructure is vulnerable to foreign control.

To exercise his authority, the president must find that:

- There is credible evidence that leads him to believe that a foreign interest might take action to threaten or impair national security
- Provisions of law, other than Exon-Florio and the Emergency Economics Powers Act, are not adequate to protect the national security

There is no mandatory requirement for a company to report under the law. Nevertheless, the president or his designee may investigate a merger, acquisition, or takeover at any time, including after a transaction has been concluded. The president can reopen a case on the basis of material omissions or material misstatements in the original notice.

The president delegated responsibility for carrying out the requirements of Exon-Florio to the interagency committee on foreign investment in the U.S. (CFIUS). The CFIUS is comprised of representatives of the Departments of Treasury (chair), DoD, DoS, Justice, Homeland Security, and Commerce, the Attorney General of the U.S., the Secretary of Labor (non-voting), and the Director of National Intelligence (non-voting). The President may determine on a case-by-case basis to include heads of any other executive department, agency, or office as members of a CFIUS team.

Once CFIUS considers a possible transaction as the result of a notification by the investors, on its own initiative, or at the request of a third party, it has thirty days to decide whether to initiate an investigation. The investigation must be completed not later than forty-five days after its commencement, at which time the committee must present a recommendation to the president. The president is required

to render a decision within fifteen days after completion of the investigation. If the president decides to take action as the result of a CFIUS investigation, he must submit a written report to Congress on the actions that he intends to take, including detailed rationale for his findings. The committee or a lead agency of the committee may, on behalf of the committee, negotiate, enter into or impose and enforce any agreement or condition with any party to the specified transaction in order to mitigate any threat to the national security of the U.S. that may arise as a result of the transaction.

### **Foreign Ownership, Control or Influence**

It is not in the interest of the U.S. to permit foreign investment in the defense industrial base where it is inconsistent with U.S. national security interests. USG contracts requiring access to classified information may be awarded to companies under FOCI when adequate safeguards exist to protect national security interests. Within the context of the DoD, national security interests are represented by information and technical data inherent in the development and production of military systems, such as system capabilities and vulnerabilities. If this knowledge is lost or compromised, potential adversaries of the U.S. would have the capability to duplicate or neutralize those systems. As a result, the U.S. must take steps to ensure that foreign interests do not have the power to direct or decide matters a company operating under a facility security clearance if such power may result in the unauthorized disclosure of classified and controlled unclassified information, or may adversely affect the award or performance of classified contracts. FOCI encompasses the possible avenues from which unauthorized foreign power may be exerted. When competent authority determines foreign interests have the power to exert such power, measures must be established to negate the FOCI or mitigate the associated risk.

When a company performing classified work is to be acquired by or merged with a foreign interest, an industrial security review is undertaken. The purpose of the review is to determine whether existing industrial security measures require enhancement. The matter of FOCI is considered in the aggregate, and the fact that FOCI elements are present will not necessarily bar a company from receiving a facility security clearance.

There are many components of foreign involvement requiring examination to determine whether a company is under FOCI and the extent of FOCI, such as those identified on Standard Form (SF) 328. Documents other than the SF 328 are analyzed, to include filings with the Security and Exchange Commission for publicly traded companies, articles of incorporation, by-laws, loan and shareholder agreements, and other documents pertinent to potential foreign control or influence.

The FOCI is then examined within the context of risk factors such as the foreign intelligence threat, potential for unauthorized technology transfer, record of compliance with laws, regulations, and contracts, and the nature of applicable international agreements between the U.S. and foreign governments. If a company is determined to be under FOCI, and risks associated with FOCI are considered unacceptable, the company would be ineligible for a facility clearance or an existing clearance would be suspended or revoked, unless steps are taken to negate FOCI or mitigate associated risks to the satisfaction of the USG. The principal objective of each arrangement is to ensure there is no unauthorized access to classified and controlled unclassified information by foreign owners, their agents or representatives, or by other non-ownership derived sources of foreign control or influence. For a detailed discussion of these arrangements and agreements, refer to the *International Programs Security Handbook* found at: [www.avanco.com](http://www.avanco.com), and the NISPOM.

## SUMMARY

The DoD has identified the areas of technology where U.S. know-how should be rigidly protected. These include the critical military technology products, transfer mechanisms and information which DoD has determined should be subject to the most stringent controls. The NDP provides guidance on the disclosure and release of U.S. classified military information. The criteria for disclosure decision-making in the NDP-1 and the NSDM 119 do not categorically dictate whether classified military information will be released to a specific country. These decisions are made on a case-by-case basis, in accordance with satisfying all of the five policy objectives of NSDM 119, which are restated in DoDD 5230.11.

Controlling the transfer of selected technologies is but one way to maintain the integrity of the U.S. defense-related industrial base. However, the extent of control is at issue. Many feel that controls should be tempered by the realities associated with worldwide competition and the impacts upon U.S. industry and the preservation of U.S. economic security as the prerequisite condition to maintaining national security. Others, however, as noted in the chapter introduction, believe that transfer of advanced technology for military or dual-use applications can lead to the proliferation of dual-use technology as well as of nuclear and conventional arms. Technology transfer issues continue to play an important role in government-to-government sales programs, commercial sales programs, international armaments cooperation programs, and industrial base considerations.

Policies and supporting directives governing technology transfer emphasize the application of the U.S. policy and legal requirements in the AECA, E.O. 12958, NSDM 119, NDP-1, and DoDD 5230.11 to each case, and the analysis of a potential recipient's need and the implied use of such information. The directives are explicit as to procedure and channels to be followed to preclude unwarranted release and disclosure of data.

## REFERENCES

U.S. Department of Defense, DoD 5105.38-M, *Security Assistance Management Manual (SAMM)*, Chapter 3.

U.S. Department of Defense, DoDD 2040.2, *International Transfers of Technology, Goods, Services and Munitions*.

U.S. Department of Defense, DoD 5220.22M, *National Industrial Security Programs Operating Manual (NISPOM)*.

U.S. Department of Defense, DoD 5220.22-R, *Industrial Security Regulation*.

U.S. Department of Defense, DoDD 5230.11, *National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

U.S. Department of Defense, DoDD 5230.20, *Visits and Assignments of Foreign Representatives*.

U.S. Department of Defense, DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*.

U.S. Department of Defense, ODUSD (Technology Security Policy and National Disclosure Policy), *International Programs Security (IPS) Handbook*, February 1995, (Revised January 2006). URL: <http://www.avanco.com>.

U.S. Government. Title 22, CFR, Parts 120-130, *International Traffic in Arms Regulations (ITAR)*.  
URL - <http://www.pmdtc.gov>.

U.S. Department of Defense, DoD 5400.7, *Freedom of Information Program*.

Executive Order 12958, as Amended

National Security Decision Memorandum 119.

*National Industrial Security Program Operating Manual (NISPOM)*, located at: <http://www.dtic.mil/whs/directives/corres/html/522022m.htm>.

U.S. Department of Defense, DoD 5200.1R, *Information Security Program*.

U.S. Department of Defense, DoD 4500.54-G, *DoD Foreign Clearance Guide*.

U.S. Department of Defense, DoDD 5200.12, *Conduct of Classified Material*.

U.S. Security Authority for the North Atlantic Treaty Organization, Instruction I-07 Public Law (PL-110-49), 26. July 2007.

## ATTACHMENT 7-1



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-1010  
22 OCTOBER 1999

**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN, JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DIRECTORS OF DEFENSE AGENCIES**

**Subject:** Training in International Security and Foreign Disclosure Support to International Programs

Strong allies, and well-equipped coalition partners, make America stronger. It is, therefore, in America's national security interest to promote cooperation with other nations, seek-international participation in our weapons acquisition process and support appropriate foreign military sales.

At the same time, we must ensure that sensitive and classified U.S. technology and military capabilities are protected. Classified information should be shared with other nations only when there is a clearly defined advantage to the United States. Disclosures must be carefully designed to achieve their purpose, and recipients must protect the information. To make certain that we accomplish these goals, certain security arrangements must be in place prior to any foreign participation in DoD programs. It is therefore vital that every DoD employee involved in international programs understand these security arrangements, as well as the laws, policies, and procedures that govern foreign involvement in our programs.

To insure that all relevant employees are fully trained in this area, the Office of the Deputy to the Under Secretary of Defense (Policy) for Policy Support (DUSD(PS)) has developed a course of instruction that covers the practical application of relevant law, executive orders, and DoD policies on this subject. All DoD personnel responsible for negotiating, overseeing, managing, executing or otherwise participating in international activities shall successfully complete either the International Security Requirements Course offered by DUSD(PS), the International Programs Security and Technology Transfer Course taught by the Defense Systems Management College, or an executive version of the course for mid-level and senior managers now being developed. This requirement applies to anyone who works in an office dealing exclusively with international matters, in international cooperation offices within broader functional offices, and those working on international issues within a DoD program. Examples of applicable activities include: security assistance, cooperative research, foreign disclosure, specific country relationships, and other international policy activities.

The law also requires that we consider systems of allied nations, or the co-development of systems with allied nations, before a U.S.-only program may be initiated. Therefore the basic, intermediate, and advanced program manager courses at DSMC shall include at least four hours of training in international security requirements related to acquisition programs. Anyone working in program offices where any international activities occur, including exports, must also complete the full five day course. DoD personnel who are newly assigned to international programs shall participate in one of the courses within six months of the assignment.

To ensure consistency, DoD components that offer specialized training in foreign disclosure and security requirements for international programs shall coordinate the contents of their courses with the DUSD(PS).

//Signed//  
John J. Hamre

## **ATTACHMENT 7-2**

### **SELECTED U.S. TECHNOLOGY LAWS AND PUBLICATIONS**

#### **Laws:**

Atomic Energy Act of 1954  
Energy Reorganization Act of 1974  
Arms Export Control Act  
Export Administration Act of 1979  
Stephenson-Wydler Technology Innovation Act of 1980  
Defense Authorization Act of 1986, Nunn Amendment/NATO Cooperative R&D  
Defense Authorization Act of 1993, Defense Technology and Industrial Base, Reinvestment and Concession

#### **Department of Defense Documents:**

DoD 5120.49, *International Technology Transfer Coordinating Committee*  
DoD 5200.1, *DoD Information Security Program*  
DoD 5230.9, *Clearance of DoD Information for Public Release*  
DoD 5230.24, *Distribution Statements on Technical Document*  
DoD 5400.7, *DoD Freedom of Information Act Program*  
DoD 5530.3, *International Agreements*  
*International Programs Security Handbook*, DUSD (TSP&NDP) available at [http://www.avanco.com/n/ips\\_handbook.html](http://www.avanco.com/n/ips_handbook.html)  
*International Armaments Cooperation Handbook*, USD(AT&L), Director of International Cooperation available at <http://www.acq.osd.mil/ic/handbook.pdf>.  
Militarily Critical Technologies List (MCTL) (Available from Institute for Defense Analysis)

#### **Department of State Documents:**

International Traffic and Arms Regulations (ITAR) (22 CFR 120-130) (Available from OCR Services or DDTC at <http://www.pmdtc.gov>. Attachment 7-2  
Selected U.S. Technology Laws and Publications

#### **Laws:**

Atomic Energy Act of 1954  
Energy Reorganization Act of 1974  
Arms Export Control Act  
Export Administration Act of 1979  
Stephenson-Wydler Technology Innovation Act of 1980  
Defense Authorization Act of 1986, Nunn Amendment/NATO Cooperative R&D

Defense Authorization Act of 1993, Defense Technology and Industrial Base, Reinvestment and Concession

**Department of Defense Documents:**

DoD 5120.49, *International Technology Transfer Coordinating Committee*

DoD 5200.1, *DoD Information Security Program*

DoD 5230.9, *Clearance of DoD Information for Public Release*

DoD 5230.24, *Distribution Statements on Technical Document*

DoD 5400.7, *DoD Freedom of Information Act Program*

DoD 5530.3, *International Agreements*

*International Programs Security Handbook*, DUSD (TSP&NDP) available at [http://www.avanco.com/n/ips\\_handbook.html](http://www.avanco.com/n/ips_handbook.html)

*International Armaments Cooperation Handbook*, USD(AT&L), Director of International Cooperation available at <http://www.acq.osd.mil/ic/handbook.pdf>.

Militarily Critical Technologies List (MCTL) (Available from Institute for Defense Analysis)

**Department of State Documents:**

International Traffic and Arms Regulations (ITAR) (22 CFR 120-130) (Available from OCR Services or DDTC at <http://www.pmdtc.gov>).