Chapter

7 TECHNOLOGY TRANSFER, DISCLOSURE, EXPORT CONTROLS, AND INTERNATIONAL PROGRAMS SECURITY

INTRODUCTION

International trade is a global enterprise in which the United States participates for all manner of goods, information, software, and services. This trade may take place both within and outside of the borders of the territory of the United States. This chapter discusses the ways in which the international transfer of these items takes place and focuses on the methods by which the United States safeguards military and enabling technologies (to include intellectual property).

The U.S. government (USG) transfers both military and dual-use articles, information, software, and services to other governments through traditional Security Assistance (SA) programs and Security Cooperation (SC) programs. In order to safeguard the technologies provided, the U.S. government applies technology transfer laws, regulations, policies, and practices which encompass program security for international programs. This chapter will cover technology transfer and disclosure policies responsibilities, and basic processes under both Government-to-Government programs as well as Direct Commercial Sales. It provides an overview of discusses the application of technology security these laws, regulations, and policies applied to international technology transfers as implemented under Security Assistance (SA) and Security Cooperation (SC) programs.

U.S. government policy supports U.S. trade in the global market, to include international arms sales. Economic security is an important part of American foreign policy and the U.S. National Defense Strategy, it is an important consideration for the export of dual-use technology. There are numerous economic and defense benefits associated with supporting U.S. defense and commercial industries trading internationally. As outlined in earlier chapters, Security Assistance (SA) and Security Cooperation (SC) programs remain essential instruments to U.S. foreign relations, supports coalition interoperability, affordability of U.S. defense programs, etc.

However, the desire to support free trade must be balanced with the need to protect critical U.S. military and enabling technologies. As markets for military equipment continue to evolve, competition based on leading-edge technology has caused a significant increase in economic espionage aimed at U.S. technology. It is the responsibility of those who control access to defense technologies to understand the laws, regulations, and directives that govern their international transfer. DoD officials must understand how to protect the U.S. military capability, which is represented by the related technology and other controlled information and, at the same time, support international security cooperation/assistance programs.

International technology transfers reviews are initiated by a basic assessment of the benefits of providing access to the ability of the recipient to protect the technology. U.S. law and policy requires that two fundamental considerations be addressed prior to sharing U.S. defense articles with a foreign government or international organization:

- U.S.'s Best Interest to Provide Access: Determining whether granting access to U.S. defense articles, technology, or services is in the best interest of the U.S.
- Adequate Protection: Determining whether the prospective recipient can and will satisfactorily protect the technology, article, or information.

In order to best understand these two fundamental security considerations, it may be useful to think of them as part of a formula. That formula is as follows:

Best Interest of U.S. to Provide Access + Adequate Protection = Potential Access

Once the potential for access has been validated, additional national security and foreign policy considerations may be applied to evaluate the proposed transfer for export authorization. This may include the appropriateness of the transfer.

This chapter is organized into three main topics: (1) Technology Transfer, Disclosure, and Export Controls and (2) Programs Security Requirements; and (3) International Visits and Assignments with the following sub-topics:

1. Technology Transfer, Disclosure, and Export Controls

- Technology Transfer and Technology Security
- Legal and Policy Basis
- Transfer / Export Legal Authorities
- Technology Security and Foreign Disclosure
- Disclosure
- Sanctions, Embargoes, and Country Specific Policies (OFAC, 126.1, country policies – under ITAR and EAR)

2. Programs Security Requirements

- Information security programs–Technology Control Plan (TCP)
- Role of Defense Counterintelligence Security Agency (DCSA) in international programs / National industrial security program
- Industry & Academia's roles (national industrial security overview – need to cover academia due to nefarious characters of late)
- Entity List
- International transportation of classified military material
- Foreign government and the North Atlantic Treaty Organization (NATO) information

3. International Visits and Assignments

- International visits and assignments
- Concept of technology transfer and export controls
- Executive Branch key players for exports
- Controlled Unclassified Information (CUI)
- Foreign Disclosure and the National Disclosure Policy (NDP)

- Export approval and license process
- International visits and assignments
- International transportation of classified military material
- Role of Defense Counterintelligence Security Agency (DCSA) in international programs
- Foreign government and the North Atlantic Treaty Organization (NATO) information
- Influence (FOCI) Technology Transfer, Disclosure, and Export Controls

Technology Transfer, Disclosure, and Export Controls

Technology Transfer and Technology Security

Technology transfer in the simplest form is the transfer of technology from one source to another; it is agnostic of the method or manner in which the transfer takes place. Technology security seeks to securely transfer this technology from the source or origin to another authorized. Protecting military technology, enabling technologies, and industry intellectual property are key to maintaining U.S. economic security and protecting the defense industrial base. Foreign adversaries are using increasingly more sophisticated, multi-pronged, and targeted campaigns to gain access to controlled U.S. information and goods. The United States utilizes various laws, regulations, and policies to protect technology, with stakeholders from the government, industry, and academia each playing important roles. DoDI-2040.02 establishes DoD's policy on international transfers, assigns responsibilities within the Department, and prescribes the procedures for transfers.

The Department of Defense is responsible for conducting national security reviews in order to provide policy and regulatory guidance on U.S. transfers or exports. These national security reviews include the complete spectrum from broad strategic reviews down to individual transactional reviews. It is important to remember that the DoD does not have the authority to authorize transfers, that authority lies solely with the Departments of State and Commerce. All transfers under SA and SC Programs undergo national security and foreign policy reviews as a matter of law and policy. The Security Assistance Management Manual (SAMM), Chapter 3, "Technology Transfer and Disclosure," is a key reference when working technology transfer and disclosure aspects of SA and SC programs or activities.

Department of Defense Policy on International Transfers

The primary DoD policy governing the process of technology transfer is contained in DoDI 2040.02, *International Transfers of Technology, Articles, and Services*. This instruction establishes DoD policy, assigns responsibilities, and prescribes procedures for the international transfer of dual-use and defense-related technology, articles, and services. It applies to all transfer mechanisms and will be implemented through such processes as export licensing; security cooperation (including Foreign Military Sales (FMS)); transfers of DoD personal property to parties outside of DoD control; and any DoD Research, Development, and Acquisition (RDA) activities, including international agreements. It outlines working relationships among the Joint Staff, the Military Departments, and the various Defense Agencies. As discussed in Chapter 2, U.S. arms sales serve specific legislative and U.S. foreign policy purposes.

DoDI 2040.02 states the following:

- Dual-use and defense-related technology will be treated as a valuable national security resource, to be protected and transferred only in accordance with export control laws and regulations, and national security and foreign policy objectives.

- In applying export control and technology security policies, emphasis will be given to preserving the U.S. military's technological superiority, establishing and maintaining interoperability with allies and coalition partners, and managing direct and indirect impacts on the defense industrial base.
- In recognition of the importance of international trade and scientific and technological cooperation, DoD must apply export control and other technology security policies and procedures in a way that takes into account support of the defense industrial base while maintaining U.S. nonproliferation imperatives.
- In determining DoD interests in technology and the means by which those interests are protected, DoD will consider such factors as the impact on the U.S. defense industrial base to support defense technologies, scientific and technological acceleration of change, as well as significant means in which scientific research and technological development are implemented in production.
- DoD will use available resources to achieve DoD and USG goals and objectives in transfers of technology, articles, and services, while recognizing that constant and rapid changes in technology pose difficult challenges in assessments, formulation of policy options, and implementation of policies.

Legal and Policy Basis for International Programs Security

Arms Export Control Act (AECA)

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) and is available online at https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987. The AECA forms the legal basis for the security requirements in 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 proposed recipient foreign countries or international organizations have agreed to certain security conditions regarding the protection of the articles or information. The three security-related conditions, which must be satisfied prior to the export of controlled defense articles and information to a foreign country or international organization, are as follows:

- Transfer: 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.
- Use: 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.
- Protection: The recipient country or organization agrees to maintain security of the articles or related technical information, and provide substantially the same degree of security to it as does the USG.

These security-related conditions are incorporated into the Foreign Military Sales (FMS) process via the standard terms and conditions of each Letter of offer and acceptance (LOA). Within any LOA, the standard terms and conditions will be listed at Section 2 "General Purchaser Agreements." Transfer, use, and protection are specifically addressed in subsections 2.4-2.6 of any LOA. By stating these conditions of sale in the LOA, the purchaser agrees to these conditions when they sign to accept the

LOA. The specific language of these conditions may be found in Chapter 8 of this textbook.

Executive Order 13526

E.O. 13526, dated December 29, 2009 establishes the executive branch's classified National Security Information Program. Section 4.1 of this order states that access to classified information 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. Additionally, it stipulates a requirement for the protection of any foreign government information (FGI) in the possession of the U.S. The executive order is implemented by Classified National Security Information, title 32 of the Code of Federal Regulations (CFR), part 2001 and 2003, effective 25 June 2010. The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), publishes "Classified National Security Information Directive 1" as the final rule pursuant to E.O. 13526 relating to classified national security information. It is also covered by DoD Manual 5200.01, DoD Information Security Program.

National Security Decision Memorandum (NSDM 119)

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 E.O. 13526. NSDM 119 defines CMI as information under the control or jurisdiction of the DoD; may be embodied written, oral, or other form; and requires protection. In addition, emphasizes that CMI is a national asset, and that the USG will not share it with a foreign government or international organization (i.e., permit access) unless such a 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. The NSDM 119 designates responsibility of controlling and releasing CMI to the Sectaries of State and Defense.

Controlled Transfers vs. Transfers that are Not Subject to Control

Classified Transfers

All classified technology, articles, and services are controlled. Classified transfers will be in compliance with DoDD 5230.11 *Disclosure of Classified Information to Foreign Governments and International Organizations*. Classified transfers will Avoid False Impressions and comply with National Disclosure Policy.

Unclassified Transfers of Articles

All international transfers, of both military and commercial (aka dual-use) articles, from the United States are controlled by U.S. export control law. These include the full spectrum of goods from pencils to advanced military weapons systems. Transfers may take place permanently or temporarily. Transfers may take place in U.S. territory (e.g., title transfer) or abroad.

Controlled Technology, Software, and/or Technical Data

Controlled unclassified information (CUI), export controlled technology, software, or technical data. Any release or disclosure of export controlled technology or technical data to any foreign person, whether it occurs in the United States or abroad, is deemed to be an export, requiring either an export license or an authorization for disclosure.

See the definition for technical data in the International Traffic in Arms Regulations 12x.[x]; technology and software definitions in the Export Administration Regulations 7xx.

In general export controlled technology, software, or technical data includes information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of an article. CUI may also include information on U.S. or foreign partner readiness and information on internal U.S. government assessments to determine the appropriateness of providing certain defense articles to partners (releasability).

Controlled technology or technical data is considered to be released or disclosed when information is transferred to foreign persons by means of any of the following:

- A visual inspection.
- An oral exchange.
- An application of the technology or data.
- The use of any other medium of communication (e.g., written), including but not limited to, electronic, magnetic, or laser technology.

Controlled transfers may apply to an U.S. person working for a foreign company. And conversely foreign persons working for U.S. companies.

Controlled Unclassified Information

Controlled unclassified information (CUI) is a term used to collectively describe all unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations and Volume 4 of DoDM 5200.01. A commonly seen marking for CUI in the U.S. is "For Official Use Only" (FOUO). FOUO information is unclassified official government information that has been determined by designated officials to be exempt from public disclosure under the Freedom of Information Act (FOIA). FOIA 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. Government agencies apply their own unique markings to identify the information. Consequently, the DoD has several policy directives addressing the release of CUI. These documents are listed as references to this chapter:

DoDD 5230.09 contains policies and procedures for the release of information for publication or public release.

DoDI 5200.21 and DoDD 5230.24 govern the release of DoD technical information.

DoDM 5400.07 contains the DoD policies and procedures governing FOIA requests.

DoDD 5230.25 provides procedures for the dissemination and withholding of unclassified technical data.

Controlled Services

Controlled services by U.S. persons include, but are not limited to, defense services such as operational and maintenance training on military defense articles. Controlled transfers can take place on U.S. soil or abroad. For example, inviting foreign partners to witness a demonstration of an U.S. weapon system in CONUS may be a controlled export activity. Certifying a defense article or system for readiness, to include providing an aircraft airworthiness certification is a controlled defense service.

See the definition for defense services in the International Traffic in Arms Regulations 12x.[x]; technology definition in the Export Administration Regulations 7xx.

Technology Transfers that are Not Subject to Export Control

- Publically available information (see DoD process for public release)
- Information provided under the Freedom of Information Act (FOIA)
- Most non-technical information, software, and certain academic basic research that are not controlled

See the definition for technical data in the International Traffic in Arms Regulations 12x.[x]; technology and software definitions in the Export Administration Regulations 7xx.

Freedom of Information Act

Congress has stated the U.S. public generally has the right to know what its government is doing. The FOIA requires government information to be made available to the public unless the information falls within one of the nine exemption categories described, and the appropriate USG official determines the information should be withheld from disclosure. Only information falling into one of these categories may be marked FOUO:

- Exemption 1 is classified information. The FOIA permits the withholding of any information properly and lawfully classified under the provisions of E.O. 13526. The other eight exemption categories deal with unclassified but generally sensitive information.
- Exemption 2 permits the withholding of information that 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 that 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.

It is DoD policy to place distribution statements on documents containing unclassified scientific and technical information produced either within the DoD or on its behalf by others. This policy was only marginally directed toward restricting the disclosure of such information to the public and, thus, to foreign persons. 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. This potential loophole was resolved by Public Law 98-94, enacted 24 September 1983, which provided the Secretary of Defense with the authority to withhold from the public critical technologies under Exemption 3 of the FOIA. For more specific information on FOIA as it relates to LOAs and FMS procurement contracts, refer to SAMM, Section C3.5, "Release of Information."

Technology Transfer Export Authorizations

Foreign Military Sales (FMS) & Building Partnership Capacity (BPC)

Government-to-government international transfers under FMS are authorized for export under the Letter of offer and acceptance (LOA) per the Arms Export Control Act (AECA) from the Department of State. This export authorization is limited to the United States Government's activities that fall within the scope of the LOA.

Title 10 or BPC programs are authorized for export under pseudo-LOAs per the Foreign Assistance Act (FAA) from the Department of State.

U.S. industry requires separate export authorization. This authorization may be in the form of export licenses/agreements or exceptions/exemptions from the Department of State or the Department of Commerce, as appropriate.

Direct Commercial Sales (DCS)

U.S. industry, organizations, academia, and persons may conduct international transfers under DCS, including directly with foreign parties (i.e., governments, companies, organization, or persons). Certain DCS transfers are controlled; certain controlled transfers require export authorizations.

For example, consider the following:

- Providing non-export controlled marketing brochures at a tradeshow is not controlled and does not require export authorization.
- Pencils are export controlled, however for most international transfers authorizations are not required to carry a pencil outside of the United States.
- Providing commercial grade night vision devices to foreign persons outside of the United States is export controlled and requires authorization for most destinations.

The Department of State and/or Department of Commerce provide export authorizations with export license/agreements for DCS exports under the International Traffic in Arms Regulations and Export Administration Regulations. Alternatively, U.S. exporters may utilize exceptions/exemptions under the respective regulations.

Hybrid FMS/DCS programs require a combination of authorities, see Chapter 15 for more discussion on these types of transfers.

International Armaments Agreements

See Chapter 13 for export authorizations for international armament agreements which pertain to cooperative research and development, testing, and/or production activities with a foreign government.

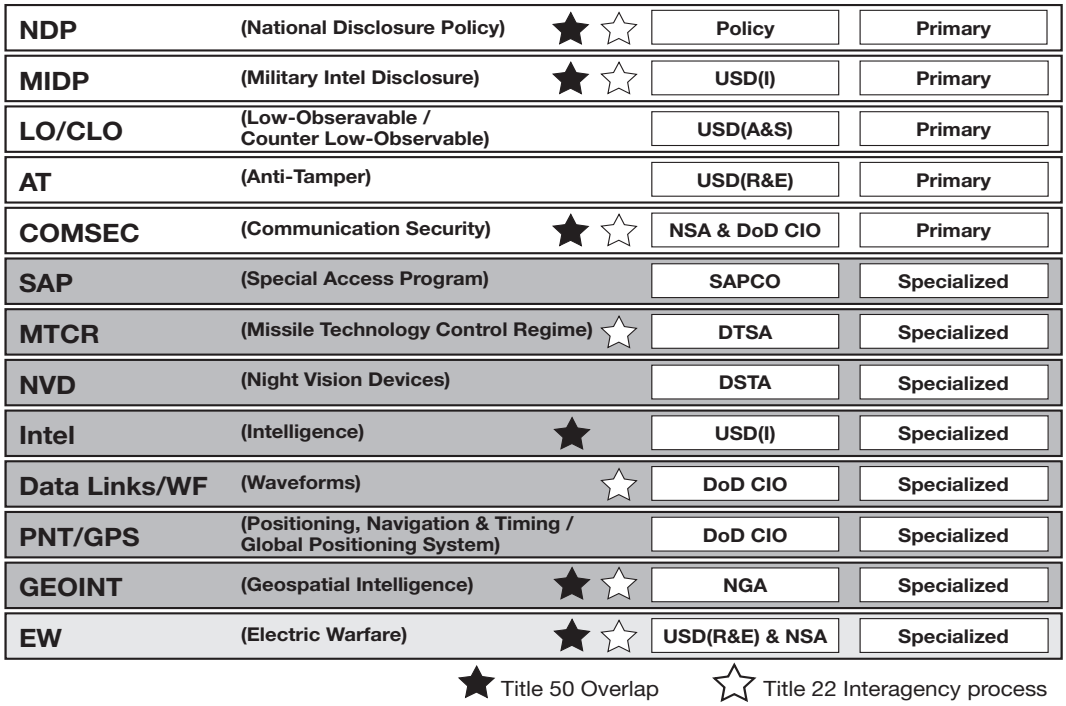
Technology Security and Foreign Disclosure (TS&FD) "Pipes"

At the core of TS&FD reform is the establishment of policy and responsibilities intended to minimize complexities while ensuring timeliness and efficient processing of disclosure requests. Within the DoD, one of the first export reform adjustments was a codification of those processes and procedures, which bear on the approval to export military technology. Previously, it was difficult to discern whether all necessary reviews and decisions were accomplished due to lack of clarity regarding the multitude of processes and approvals potentially necessary for a given export. While different communities within the DoD may have been cognizant of the review/approval processes necessary in certain specific areas, there had been no comprehensive documentation of all of potentially applicable procedures. With this in mind, the existing export/foreign disclosure decision-making process was more clearly mapped-out in what has come to be known as the "Thirteen Pipes of Technology Security and Foreign Disclosure," as seen in Figure 7-3. While it is likely that no decision will need to undergo review/approval procedures in all these thirteen pipes, it is now much more likely that individual export/foreign disclosure cases will be more comprehensively planned out in advance, and more easily monitored, so that unexpected delays may be resolved and faster comprehensive export decisions rendered.

Technology Security and Foreign Disclosure (TS&FD) Review Processes

Thirteen separate but related TS&FD processes, or "pipes" (see Figure 7-1), support DoD TS&FD release decisions. Additionally, each MILDEP, and many DoD agencies have internal review processes for approving the transfer of capabilities and technologies within their purview.

Figure 7-1
Thirteen Pipes of Technology Security and Foreign Disclosure



The Deputy Secretary of Defense has empowered the Arms Transfer and Technology Release Senior Steering Group (ATTR SSG) as the primary forum for review and adjudication of High Level Decision (HLD) TS&FD release requests. Also established was the Technology Security and Foreign Disclosure Office (TSFDO), which is designed to serve as the ATTR SSG's Executive Secretariat. The ATTR SSG has been charged with streamlining and harmonizing DoD TS&FD release processes. The

ATTR SSG develops, guides, and directs (consistent with U.S. policy and national security objectives) DoD-wide reform, implementation, and subsequent management of the DoD TS&FD system, and ensures critical U.S. technologies are protected, and release considerations are balanced with building allied and partner nation capability objectives. Ultimately, all of the aforementioned reforms are intended to foster the continued growth of a healthy defense industrial base, reduce stresses on U.S. forces, and facilitate efforts in training and equipping forces in countries where doing so advances U.S. national security interests.

Classified Information 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 materiel:

- Decision: In keeping with the AECA, E.O. 13526, and NSDM 119, the decision concerns whether the USG will release classified information to another government or international organization.
- Transfer: If the decision above is in the affirmative, the actual transfer must be made either through official government-to-government channels (e.g., government courier) or through other channels approved by the responsible governments.

Transfer via government channels is necessary so that government accountability and control can be maintained from the point-of-origin to the ultimate destination. Transfers normally occur between Designated Government Representatives (DGRs) when custody is officially transferred to a recipient government or international organization. The recipient then assumes responsibility for the protection of the article or information. A security assurance must be obtained prior to transferring classified material to a representative of a foreign government or international organization. A receipt must be obtained for classified information transfers to document the transfer of security responsibility.

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 classified information for its operation or maintenance, or for the foreign recipient training. Therefore, any 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 transferred. If the proposed foreign recipient is not authorized to receive the highest level of classified information required, no information, not even CUI, 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.

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

Foreign Disclosure and the National Disclosure Policy (NDP)

The NDP was established as a framework for the approval or denial of the transfer of classified military information (CMI) to foreign governments and international organizations. Basic authority and policy for transferring CMI 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.

The NDP-1 is the interagency document that implements the core U.S. policy for the disclosure of CMI. It promulgates U.S. policy in the form of specific disclosure criteria and limitations, procedures for handling exceptions to policy, and other guidance governing disclosure decisions of CMI. The NDP-1 also defines CMI into specific categories, designates countries eligibility to receive CMI, and establishes the National Disclosure Policy Committee (NDPC), which is discussed later in this chapter. DoD Directive 5230.11 Disclosure of Classified Military Information to Foreign Governments and International Organizations implements the National Disclosure Policy within the Department of Defense.

An official who has been specifically delegated disclosure authority, commonly referred to as a Foreign Disclosure Officer (FDO), may authorize disclosures of classified military information to foreign governments in support of a lawful and authorized U.S. government purpose in accordance with authorized disclosure authority. The Secretary of Defense has delegated disclosure authority to the Secretaries of the Military Departments (MILDEPs) and other DoD officials whose decisions must be compliant with NDP-1. They are required to appoint a Principal Disclosure Authority (PDA) at the component headquarters level to oversee the disclosure process and a Designated Disclosure Authority (DDA) at subordinate command and agency levels to oversee disclosure decisions at their level when disclosure authority is delegated. Most importantly, each disclosure decision is made on a case-by-case basis. Any commitment to disclosure or release of controlled defense-related information or technology must be authorized by the PDA or DDA unless authority is otherwise delegated in a Delegation of Disclosure Authority Letter (DDL).

National Disclosure Policy Committee/Exceptions to National Disclosure Policy

The NDP-1, and DoDD 5230.11 requires the establishment of an interagency National Disclosure Policy Committee (NDPC), to formulate, administer, and monitor NDP. General members of the NDPC include the following:

- Secretary of State
- Secretary of Defense (appoints Chairman)
- Secretary of the Army
- Secretary of the Navy
- Secretary of the Air Force
- Chairman, Joint Chiefs of Staff

On a day-to-day basis, these officials are represented in NDPC decisions by designated senior officials on their staff. NDPC general members have a broad interest in all committee activities and vote on all issues that come before the committee. Other members (such as the Director of National Intelligence, the Secretary of Energy, and many others) may vote on issues in which they have a direct interest (see Attachment 7-1 for a list of all the members of the NDPC). When an exception to NDP (ENDP) is required, because disclosure criteria cannot be met within the existing authorized classification level, such exceptions may be granted only by the NDPC, the Secretary of Defense, or the Deputy Secretary of Defense. A request for an ENDP must be sponsored by an NDPC member, normally the cognizant MILDEP for the classified information proposed for transfer. For military weapon systems, this is normally the MILDEP that has developed and produced the system.

On 14 February 2017, the Secretary of Defense codified in NDP-1, the Military Intelligence Disclosure Policy Committee (MIDPC), The MIDPC is the central authority for the formulation,

promulgation, administration, and monitoring of NDP-1 as it relates specifically to Category 8 (Military Intelligence). The MIDPC operates similar to the NDPC with a similar structure (see Attachment 7-2 for a list of all the members of the MIDPC). In situations where an ENDP includes multiple categories, to include Category 8, the NDPC has purview.

The NDP-1 Annex (classified) identifies the maximum classification level of information that can be released by country and by category of classified military information. NDP-1, by itself, does not authorize any disclosures. The Secretaries of the MILDEPs have generally been delegated authority by the NDP-1 to decide if CMI under their control may be released. The policy and guidance for implementing NDP-1 is contained in the DoDD 5230.11. 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:

1. Disclosure is consistent with U.S. foreign policy and national security objectives.
2. Disclosures, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology or operational capabilities.
3. 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 general security agreements.
4. Disclosure will result in benefits to the U.S. at least equivalent to the value of the information disclosed.
5. The disclosure is limited to information necessary to accomplish the purpose for which disclosure was authorized.

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 ENDP must be approved by the NDPC or MIDPC. 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 CMI 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 that 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. The Secretary or Deputy Secretary of State, with the consent of the originating or responsible NDPC or MIDPC member department or agency, may also authorize such disclosures. SAMM, Section C3.2, "Disclosure of Classified Military Information," provides additional information on the national disclosure process as it relates to SC.

Security Surveys

In addition to making determinations on the release of CMI, the NDPC also conducts security surveys (also called security visits) of foreign governments or international organizations. NDPC teams conduct periodic visits to foreign governments and their national industrial bases to assess capability and intent to protect U.S.-origin CMI. 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, industrial security and physical security. The views of the local U.S. embassy are also sought. If the result of a survey is satisfactory, it may result in an international security agreement (see below) with the other government. A survey may also result in changes to the classified annex in NDP-1 concerning a country's classification and eligibility for CMI without engaging the ENDP process.

International Security Agreements

E.O. 13526 requires persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch. In situations where classified information is being made available to foreign governments, these assurances may be obtained in several ways. First, they are included in the standard terms and conditions of FMS LOA, Section 2, "Conditions–General Purchaser Agreements." See Chapter 8 for further information. They may also be the subject of diplomatic notes, memoranda of understanding (MOUs) and similar correspondence. Separate international agreements known as General Security of Information Agreements (GSOIAs) or General Security of Military Information Agreements (GSOMIAs) have been concluded with approximately 72 countries. Since these are reciprocal agreements, the other governments may also send teams to the U.S. to ensure compliance with the agreements. GSOIA/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. Chapter 13 of this textbook contains additional information.

Similarly, DSCA Policy 16-26 observes that foreign partners' procurement laws sometimes forbid the submission of a Letter of Request (LOR) for U.S. defense systems prior to a competition among several vendors. The lack of an LOR may impede timely initiation of U.S. government technology release and foreign disclosure processes. In order to accelerate (when possible) the release reviews of U.S. technologies and to initiate foreign disclosure processes in the absence of an LOR, SCOs should be alert for potential sales of sensitive or classified defense articles, which would require the release of CMI.

In those instances that would require inter-agency technology security and foreign disclosure (TSFD) release (i.e., when the SCO becomes aware of credible demand signals indicating the probable submission of an LOR for Price and Availability [P&A] or LOA, or a commercial Request for Information or Request for Proposal for such items) the SCO should develop a Pre-LOR Assessment Request (PAR), as directed in SAMM C3.1.2, which will serve in place of a Country Team Assessment (CTA) to inform the inter-agency community and prepare the cognizant Implementing Agency (IA) to initiate TSFD processes for the timely release of information.

When no formal LOR is available, a PAR serves in place of an LOR and CTA as grounds for the IA to initiate applicable foreign disclosure and technology security release processes. However, it should be noted that a PAR does not serve in place of an LOR, or for any purpose other than initiation of the foreign disclosure and technology security release process.

In the preparation of the PAR, the SCO should compile the information described in SAMM Table C3.T2 and consult with the relevant IAs and CCMD for releasability and technical information. When complete, the SCO forwards the PAR to the CCMD. Because the PAR is an extraordinary process, a CCMD endorsement is required in each case to support initiation of the TSFD release processes. The CCMD provides comments on each of the elements addressed in the PAR in the endorsement, and forwards the PAR and endorsement to the Joint Staff, the applicable IA, and DSCA. This process forms the basis for a collaborative effort to analyze the recipient nation's military requirements, in order to identify a capability that fulfills those requirements and initiates the DoD's TSFD processes to meet the partner's acquisition needs.

In addition to national security reviews, various government stakeholders may provide foreign policy, human rights, per DoDI 2042.02 *International Transfers of Technology, Articles, and Services*.

It is Department of Defense (DoD) policy to treat defense-related technology as a valuable and limited national security resource to be protected and transferred only in pursuit of national security and foreign policy objectives. Determining which technologies should be controlled and to what extent necessitates an understanding of two seemingly conflicting elements of U.S. policy on international trade:

Technology transfer governs certain exports which require national security reviews, these may be for military items or for items that are used for both commercial and military purposes. U.S. law requires the provision of military items by foreign governments to be protected.

Programs Security Requirements

Information Program Security

Defense Counterintelligence and Security Agency Role in Programs Security

A role of the Defense Counterintelligence and Security Agency (DCSA) 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. In fulfilling this obligation, DCSA administers the National Industrial Security Program (NISP) operating on behalf of USD(&SI). DSS does not develop industrial security policy. DCSA implements industrial security policy established by USD (I&S) for SA and SC programs executed by USD (P).

Facility Security Clearance

Prior to a defense contractor being granted access to classified information, the contractor must be sponsored for a facility security clearance (FSC). This sponsorship is based upon a bona fide procurement need, and is submitted to DCSA by a U.S. or foreign government contracting activity or by another contractor already cleared under the NISP. DCSA 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. The security agreement is a legal contract to abide by the DoD 5220.22-M, National Industrial Security Program 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 DCSA 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. DCSA 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 FOCI situations. DCSA ensures appropriate transportation plans are in place for commercial overseas shipments of classified material and approves contractor international hand carriage arrangements. Additionally, DCSA 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 DCSA provides support to cleared contractors operating overseas, and monitors their compliance with the NISPOM. Finally, DCSA provides counterintelligence (CI) support to cleared contractors, including CI awareness briefings. More information about DCSA can be found at https://www.dcsa.mil.

Technology Control Plan

The technology control plan (TCP) provides guidance for controlling 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 126.13c, 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, Contract Security Classification Specification). The DCSA 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.

DoD Central Adjudicative Facility (CAF)

The National Industrial Security Program (NISP) establishes procedures for safeguarding classified defense information that is entrusted to contractors. Included in these procedures is a system for determining the eligibility of industrial personnel for access to classified defense information. The Central Adjudication Facility (CAF) is responsible, on behalf of the Department of Defense (DoD) and twenty-three other departments and agencies, for the following:

- Determining the personnel clearance eligibility of employees for access to classified information, foreign or domestic
- Maintenance of personnel clearance records, and furnishing information to authorized activities
- Processing security assurances, clearances, and visits involving the United States and foreign countries
- Monitoring the contractor's continued eligibility in the NISP

International Transportation of Classified Military Material

To ensure government accountability and control are maintained for classified material, all international transfers take place through official government-to-government channels or other channels mutually agreed upon in writing by the sending and receiving governments (i.e., collectively, a government-to-government transfer), consistent with the government-to-government principle. Transfers must take place between Designated Government Representatives (DGRs) who are appointed by their governments or international organizations. The U.S. DGR for Direct Commercial

Sales (DCS) is a Defense Counterintelligence Security Agency (DCSA) representative. Another USG employee at a facility may be given this responsibility. The U.S. DGR is responsible for performing the "foreign disclosure" verification (i.e., verifying the classified material to be transferred is covered by an export authorization); ensuring appropriate written security arrangements are in place; and decrementing and endorsing the license back to DDTC. In cases when a DCSA, or other USG official is not immediately available, DCSA may delegate certain DGR functions to a company's Empowered Official or Facility Security Officer. However, DCSA must ensure that the proper documentation is in place before delegating such authority, must maintain oversight responsibility, and must follow-up to ensure that proper procedures were followed. For FMS shipments, the U.S. DGR is appointed by the FMS case implementing agency.

The DGR of the recipient government or international organization receives or verifies receipt of the information or material (depending on the location of the transfer and the arrangements specified in the LOA and/or contract and the transfer plan) on behalf of the recipient government or organization.

The official transfer of security responsibility is not complete until the foreign government's DGR notifies the U.S. DGR that the recipient government or organization has taken final custody of the classified material and assumed full control for its safeguarding under bilateral security or program-specific security agreements between the USG and the foreign government. A freight forwarder or commercial carrier is a transfer agent and cannot be a DGR. All transfers must be consistent with the NISPOM for commercial sales and DoDM 5200.01 and the SAMM Chapter 7 for FMS sales.

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 CUI that is provided in confidence.

As a result of numerous international security and program agreements, the NATO security agreements obligate 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 controlled and managed under E.O. 13526 in order to receive protection equivalent to that provided by the originating government or organization, as stipulated in E.O. 13526 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 Authorized." 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.13526, the Presidential directive on safeguarding classified national security information, and DoD-M 5200.01.

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. CUI, 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 Affairs (USSAN) for safeguarding NATO information involved in international programs. DoDD 5100.55 USSAN Affairs 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 and implemented by DoDD 5100.55, and the NISPOM. These documents must be consulted for specific details.

Classification Levels

"NATO information" is information that is circulated within NATO. 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 "NATO Information." Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom atomic information 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 provider or originator. Once NATO no longer needs the information, the NATO markings are removed and the information is returned to the originator.

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).

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 NATO 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 comingled 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 NATO 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 Washington, D.C., 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.

Multinational Industrial Security Working Group Documents

The multinational industrial security working group (MISWG) is composed of the NATO countries (minus Iceland) as well as Austria, Sweden, Switzerland, and Finland. This ad hoc group was 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 DCSA may approve the use of the documents in individual commercial programs. However, the Designated Security Authority, part of DTSA, will approve the use of the documents when they are required by an international agreement such as in a PSI.

Another important aspect of program security includes processes and procedures governing international visits.

International Visits and Assignments

International Visits and Assignments

DoDD 5230.20, Visits and Assignments of Foreign Nationals, sets forth standard procedures concerning requests for visits, assignments, and exchanges of foreign nationals to the DoD and to DoD contractor facilities over which the DoD components have security responsibility. SAMM, Section C3.4, "Visits, Assignments, and Exchanges of Foreign Nationals," provides further discussion relating to SC.

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.

International Visits Program

The International Visits Program (IVP) establishes 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:

1. Facilitate planning, scheduling, and administration of a visit
2. Provide a vehicle for consideration of proposed export/disclosure decisions related to the visit and record the decision(s)
3. Obtain the required assurances regarding the security clearance, need-to-know, and sponsorship from the visitor's government if classified military information is involved

Types of Visits

Under the IVP, there are three types of visits that may be authorized:

1. One-time: a single visit, normally less than thirty days
2. Recurring: recurring visits over a period of time; normally not exceeding one year
3. Extended: a single visit for an extended period of time (beyond 30 days) to support a combined program, or for liaison officer, exchange officer, or cooperative program

Whether the DoD funds any portion of the visit is an entirely separate issue from the approval of the visit under the IVP. Before issuing an invitation, DoD officials must ensure that any classified information proposed for disclosure is approved by the delegated disclosure authority. 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 cannot change.

Visit Procedures

Visit requests to DoD organizations or facilities are submitted by the foreign embassy in Washington, D.C., usually by a military attaché of the partner nation. The requests normally are submitted electronically through the automated Foreign Visit System (FVS), which has been provided by DIA to foreign embassies. The FVS is a component of the Security Policy Automation Network (SPAN). 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.

The FVS automatically routes each request for visit to the Defense Visit Office (DVO) in one of four designated organizations. These include the Department of the Army, Department of the Navy, and Department of the Air Force for all organizations, facilities, and other entities under their control. The fourth organization is DIA itself, which administers visit requests for the Office of the Secretary of Defense, the Joint Staff, defense agencies, and their contractors. The DVOs forward, as necessary, the visit requests to the appropriate foreign disclosure offices of the organizations to be visited, and seek their comment. Based on this input, the DVO renders a decision on the visit, which is returned over the same electronic path used for submission to the embassy of the country submitting the visit request. There are three possible responses to a visit request through IVP channels:

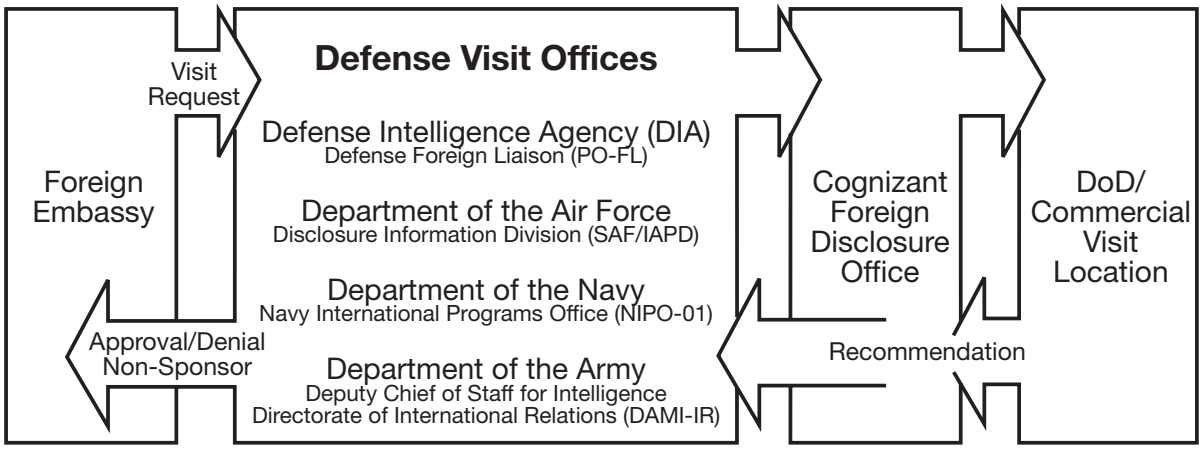
1. Approved: The visit can occur, and the specified information can be disclosed
2. Denied: The visit can occur, but the specified information cannot be disclosed
3. Not sponsored: There is no apparent government program. The visit can occur and information can be disclosed if there is a license or other authorization

Notification of approval of a foreign request for a visit or certification to a DoD component shall be forwarded to the contact 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. Correspondence with DoD contractors relative to approved foreign visits shall be forwarded to the cognizant DCSA regional office for transmittal to the contractor.

Disclosures of classified information to foreign visitors and certified foreign representatives shall be limited to that authorized per disclosure authority and in-accordance to guidance from the Foreign Disclosure Officer. Disclosures of classified information are further 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 7-2 provides an overview of the IVP within the DoD. At any time, participating activities have immediate access to all visit request status information.

Figure 7-2
International Visit Program



A request of visit authorization is not required at a contractor facility when the information to be disclosed is unclassified and (1) it is not subject to export controls, or (2) it is subject to export controls, but a contractor has an export license. A visit authorization is typically not required at a DoD facility when the facility is open to the public and the information is open for public release according to service regulations.

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.

Role of Security Cooperation Offices in International Visits

SCO personnel should be cognizant of the official travel of both host nation personnel to DoD organizations, as well as the travel of DoD personnel into country. SCOs frequently coordinate visits by host nation personnel to destinations such as a combatant command headquarters or a MILDEP installation for a program management review. However, the SCO cannot submit the visit request, which must originate in the host nation embassy in Washington, D.C., through the FVS. SCOs remind their host nation counterparts of this requirement and note that their own assistance in scheduling a visit is dependent on formal approval through the FVS. A SCO cannot approve a visit to any DoD organization or facility, other than its own office.

For DoD visitors traveling into the host nation, the SCO should control these through the granting or denying of country clearance. In doing this, the SCO follows the procedures in DoD 4500.54, DoD Foreign Clearance Guide. The SCO may also support DoD visitors by passing assurances and other documentation to and from the host nation, and by using its office as necessary to appropriately store CMI or CUI.

Defense Personnel Exchange Program

The Defense Personnel Exchange Program (DPEP) authorizes the exchange of personnel between the U.S. military services and their counterparts of friendly governments for assignment to established positions within the military services. 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 authority letter (DDL). Written procedures must be developed to prevent inadvertent disclosure of classified or CUI as described in DoDD 5230.20. DPEP assignees may not act as a representative of their government.

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 Chapter 13 for a 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.

Visits Overseas by Department of Defense Personnel

The policy for overseas travel of DoD personnel is covered under DoDD 4500.54E, DoD Foreign Clearance Program (FCP), the DoD Foreign Clearance Manual (FCM), and Foreign Clearance Guide (FCG). The FCM and FCG implement clearances and DoD personnel travel clearances through U.S. embassies for overseas travel. 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 organization or contractor facility.

Whether the DoD funds any portion of the visit is an entirely separate issue from the approval of the visit under the IVP. Before issuing an invitation, DoD officials must ensure that any classified information proposed for disclosure is approved by the delegated disclosure authority. 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 cannot change.

Visit Procedures

Visit requests to DoD organizations or facilities are submitted by the foreign embassy in Washington, D.C., usually by a military attaché of the partner nation. The requests normally are submitted electronically through the automated Foreign Visit System (FVS), which has been provided by DIA to foreign embassies. The FVS is a component of the Security Policy Automation Network (SPAN). 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.

The FVS automatically routes each request for visit to the Defense Visit Office (DVO) in one of four designated organizations. These include the Department of the Army, Department of the Navy, and Department of the Air Force for all organizations, facilities, and other entities under their control. The fourth organization is DIA itself, which administers visit requests for the Office of the Secretary of Defense, the Joint Staff, defense agencies, and their contractors. The DVOs forward, as necessary, the visit requests to the appropriate foreign disclosure offices of the organizations to be visited, and seek their comment. Based on this input, the DVO renders a decision on the visit, which is returned over the same electronic path used for submission to the embassy of the country submitting the visit request. There are three possible responses to a visit request through IVP channels:

1. Approved: The visit can occur, and the specified information can be disclosed
2. Denied: The visit can occur, but the specified information cannot be disclosed
3. Not sponsored: There is no apparent government program. The visit can occur and information can be disclosed if there is a license or other authorization

Notification of approval of a foreign request for a visit or certification to a DoD component shall be forwarded to the contact 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. Correspondence with DoD contractors relative to approved foreign visits shall be forwarded to the cognizant DCSA regional office for transmittal to the contractor.

Disclosures of classified information to foreign visitors and certified foreign representatives shall be limited to that authorized per disclosure authority and in-accordance to guidance from the Foreign Disclosure Officer. Disclosures of classified information are further 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 7-5 provides an overview of the IVP within the DoD. At any time, participating activities have immediate access to all visit request status information.

Summary

The DoD has identified the areas where U.S.-origin technology and other sensitive information should be rigidly protected. These include the critical military technology products, transfer mechanisms and information that the DoD has determined should be subject to export and disclosure controls. The NDP provides guidance on the disclosure and release of U.S. classified military information. The criteria for disclosure decisions in the NDP-1 and 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. Balance must be struck to ensure that the extent of control considers the realities associated with worldwide competition and the impacts upon U.S. industry and the preservation of U.S. economic security as a prerequisite condition to maintaining national security. DoD Officials must be ever vigilant to do their part to protect U.S. military capability and the U.S. tactical edge in an increasingly aggressive information stealing environment by America's adversaries. U.S. international arms and critical technology transfers are authorized solely at the benefit of the United States, the national security and foreign policy reviews conducted under technology transfer and disclosure reviews are key decision points that maintain the U.S. military advantage. Technology transfer play an important role in all manners of transfer including 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.13526, NSDM 119, NDP-1, and DODD 5230.11 to each case, and the analysis of a potential recipient's need, the intended use and protection measures for such information. The directives are explicit as to procedures and channels to be followed to preclude unwarranted release and disclosure of information.

References

Laws

Arms Export Control Act

Atomic Energy Act of 1954

Defense Authorization Act of 1986 (Nunn Amendment/NATO Cooperative R&D)

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

Energy Reorganization Act of 1974

Export Administration Act of 1979

Foreign Assistance Act

Freedom of Information Act

Public Law (PL-110-49), 26 July 2007, Foreign Investment and National Security Act of 2007.

Stephenson-Wydler Technology Innovation Act of 1980

Department of State Documents

DDTC Website: https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id24d528fddbfc930044f9ff621f961987

International Traffic and Arms Regulations (ITAR) (22 CFR 120-130).

Department of Commerce Documents

Export Administration Regulations (EAR) (15 CFR 730-774)

Department of Defense Documents

DoDI 2040.02, International Transfer of Technology, Articles, and Services.

DoDI 2030.08

DoD 4500.54E, DoD Foreign Clearance Program

DSCA Manual 5105.38-M, Security Assistance Management Manual (SAMM), Chapter 3. http://www.samm.dsca.mil/.

DoD-M 5200.01 *DoD Information Security Program and Protection of Sensitive Compartmentalized Information* (SCI)

DoDD 5100.55, United States Security Authority for North Atlantic Treaty Organization Affairs

DoDI 5220.02 *National Industrial Security Program*

DoD 5220.22-M, *National Industrial Security Programs Operating Manual* (NISPOM)

DoDD 5230.09, *Clearance of DoD Information for Public Release*

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*

DoDD 5230.24, *Distribution Statements on Technical Documents*

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*

DoDI 5230.29, *Security and Policy Review of DoD Information for Public Release*

DoDD 5400.07, *Freedom of Information Program* (FOIA)

DoDI 5530.03, *International Agreements*

U.S. Security Authority for the North Atlantic Treaty Organization, Instruction I-07

Other U.S. government Documents

Defense Technical Information Centers (DTIC). www.dtic.mil

Executive Order 13526.

National Security Decision Memorandum 119

Office of Foreign…(OFAC) (13 CFR 500-598)