CHAPTER 1

INTRODUCTION

A. INTRODUCTION

1. International programs with allied and other friendly countries have been an increasingly important part of U.S. national security and defense acquisition strategy in the post-Cold War era. These programs flow from U.S. efforts during the late 1940s and early 1950s to support Western Europe and create a strong defensive alliance. In the early years this support was largely in the form of grants of surplus military equipment. As the stockpile of surplus equipment decreased, the emphasis shifted to sales of military equipment and the furnishing of technical assistance. A principal purpose of these programs was to ensure a high degree of equipment standardization within the North Atlantic Treaty Organization (NATO) and to build a European defense industrial base.

2. Building on a base of sophisticated U.S. military technology, the Western European countries were designing and producing their own weapons systems by the late 1960s. In the early 1970s, the United States again began to emphasize standardization of the growing number of weapons systems. In a change to the philosophy of the 1950s, armaments cooperation evolved into a "two-way street" in defense trade in which the United States and its allies would encourage standardization by purchasing each other's equipment. Subsequent legislation encouraged the establishment of cooperative research and development programs to achieve standardization.

3. The mid-1980s saw a substantial increase in Department of Defense (DoD) international cooperative program activity. This was a result, in part, of the growing assertiveness and improved technological capabilities of the U.S. allies and other friendly countries. There also was a growing awareness of the wasteful and duplicative research and development (R&D) programs within NATO. In November 1985 the U.S. Congress established the NATO Cooperative Research and Development Program and the NATO Comparative Test Program.[1] Both of these programs emphasized collaborative research, development, test and evaluation (RDT&E) for weapon systems meeting common military requirements through deployment and support of common, or at least interoperable, equipment. The U.S. Congress later expanded the NATO Cooperative R&D Program to include major non-NATO allies (Australia, Egypt, Israel, Japan, Argentina, Jordan, and the Republic of Korea).

[1] The NATO Comparative Testing Program is now consolidated with the Foreign Weapons Evaluation Program into the Foreign Comparative Testing Program (FCT) , which is authorized under Title 10 United States Code (U.S.C.) 2350a (*reference a*).

4. Since the early 1990's, coalitions have become the preferred way for U.S. forces to confront major regional and global security issues – sharing the burden of resources and political legitimacy. However, inherent in coalition warfare is the critical requirement to significantly improve interoperability. An effective method to accomplish this is to develop and field new and improved weapons systems in concert with likely coalition partners.

5. As the defense industrial environment continues to change, DoD is forecasting fewer new major systems and longer intervals between systems. Major firms are becoming more concentrated and vertically integrated as companies complete acquisitions and adjust their strategic posture. Sub-tier consolidation is accelerating while acquisition reform reduces DoD control and visibility into subsystem source selections and sub-tier firms. These trends challenge DoD's ability to maintain industrial competition to facilitate cost and quality improvements and innovation. To address this challenge, DoD's industrial strategy has four broad thrusts:

a. Increase the opportunities available to DoD suppliers by expanding their access to global markets and encouraging diversification into commercial markets.

b. Increase the number of suppliers serving DoD by facilitating DoD's access to global suppliers and by breaking down barriers between the commercial and defense industries to realize the benefits of civil-military integration.

c. Invest in future industrial capabilities.

d. Address industrial issues in the acquisition process to assure required capabilities remain available or can be reconstituted when needed.

6. Concurrent with DoD's efforts to maintain competition, the Department is pursuing the critical goal of improving systems interoperability with allies and potential coalition partners. There are differences in international partners' national political and economic priorities that support coalition interoperability. Thus, the Department's objective is to capitalize on cooperative initiatives in joint and combined interoperability that incorporate solutions of materiel, doctrine, tactics, techniques, and procedures. The Department is focused not just on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems, but also on the goal of building a system of systems capability in support of joint and coalition operations.

7. International armaments cooperation, in its many forms, enhances interoperability, stretches declining defense budgets, and preserves defense industrial capabilities. It is a key element of DoD's acquisition and technology efforts to field the most capable force possible. Prior experience shows successful efforts require DoD to engage with potential partners in discussions at the earliest practicable stage to identify common mission problems and to arrive jointly at acceptable mission performance requirements to balance cost, meet coalition military capability needs, and assure interoperability. Many weapons programs will remain national. On the other hand, cooperation with allies must be the choice for those systems that require interoperability in coalition operations – for example, in areas such as air defense, communications, intelligence, chemical/biological defense, and information security. Where opportunities for cooperation do

exist, these programs must be implemented efficiently and effectively. Interoperability includes political and cultural aspects in relationships, as well as military activity.

8. As programs develop, cooperation continues and security cooperation in the form of Foreign Military Sales (FMS) and Direct Commercial Sales (DCS) are added. These days it is best to assume that nearly every new military article may end up for sale to other governments and international organizations. With this in mind, we must consider that there will be technology transfer of not only the major end item, but components, technical data and training for the subparts and proper protection must be engineered into new systems very early on in their development.

9. International programs are therefore a fact of life. They will require sharing defense articles, technical data, classified military information (CMI), and controlled unclassified information (CUI) with allies and other friendly countries. The risk of their being exploited and falling into the wrong hands must be taken into consideration. DoD officials must therefore understand how to protect the military capability of our Armed Forces, which is represented by the related technology and other controlled information and, at the same time, support international programs.

B. STRIKING A BALANCE

1. This section provides an overview of the major laws, Executive Orders, directives and departmental regulations that establish the foundation for the U.S. policy that governs the export or foreign disclosure of defense articles and technical data, CMI and CUI, and form the basis for related security requirements for international programs. The laws and Executive Orders contain basic principles and conditions intended to protect U.S. national interests. These basic principles and conditions must be understood and applied to international programs in a correct and efficient manner to avoid their being perceived as impediments to the programs.

2. **Federal Laws**

a. **Arms Export Control Act (AECA), Public Law 94-329 (1976), (22 U.S.C. 2751**)

(1) The AECA *(reference b)* governs the export of defense articles and services and related technical data and is the legal basis for most international programs covered by this handbook. The Secretary of State, acting for the President, in consultation with the Secretary of Defense, designates which articles and services are defense articles and services. The articles and services may be classified or unclassified. The articles comprise the U.S. Munitions List (USML) which is contained in the International Traffic in Arms Regulations or ITAR *(reference c)*. The AECA covers commercial and government sales programs, as well as certain DoD cooperative research and development programs. The ITAR implements Section 38 of the AECA for commercial sales. The Security Assistance Management Manual (SAMM) *(reference d)* implements the portions of the AECA covering the

government sales program. The cooperative research and development programs are covered by several DoD issuances in the 5000 series of DoD issuances.

(2) The AECA requires that arms exports support U.S. foreign policy and national security interests. It also requires the President to assure that a proposed foreign recipient of defense articles and services has agreed to certain conditions before an export of defense articles or services may be approved. First, the recipient country or international organization must agree not to transfer title or possession of the articles or services (which include technical data) to anyone who is not an officer, employee or agent of the country or international organization without the prior consent of the U.S. Government. Second, the recipient country or international organization must agree not to use the articles or services or permit their use for other than the purpose for which they were furnished without the prior consent of the U.S. Government. Third, the recipient country or international organization must agree to maintain the security of the defense articles and services and provide substantially the same degree of security as the U.S. Government. These conditions form the legal basis for the security assurances and requirements associated with international programs. The AECA is discussed further in Chapter 2.

b. **Export Administration Act of 1979, (EAA), Public Law 96-72 (1979), (50 U.S.C. Appendix 2401-2420), as Amended**

(1) The EAA *(reference e)* governs the export of commercial, unclassified items, software, and technical data of concern to DoD that are not covered by the AECA. Most items, software and technical data controlled by the EAA, approximately 80%, are of no concern to DoD. The items of concern to the DoD are those that have both a commercial and a military or strategic use – commonly referred to as "dual-use" items. The EAA is not permanent legislation and, when it has lapsed, its provisions have been extended by other legislation or by Executive Orders pursuant to the President's authority under the International Emergency Economic Powers Act. The provisions of the EAA are currently extended by Executive Order (E.O.) 13222 of August 17, 2001.

(2) The EAA is administered by the Department of Commerce; the responsible office is the Bureau of Industry and Security (BIS). The implementing regulation is the Export Administration Regulations (EAR). The EAR contains the Commerce Control List (CCL), which lists, by classification designation, the items, software, and technical data that are controlled. The EAA requires the Department of Commerce to work with DoD, the Department of State, and the Department of Energy to develop the list of controlled items and technical data. The EAR also contains a Country Chart that must be consulted to determine if a validated license is required for exports of items, software, or technical data on the CCL to a particular country. General prohibitions and lists of embargoed countries also must be reviewed to arrive at a decision on any license request.

c. **The Atomic Energy Act (AEA) of 1954, Public Law 83-703 (1954), (42 U.S.C. 2121, 2153, and 2164), as Amended**

The AEA *(reference f)* allows the U.S. Government to make available to cooperating nations and regional defense organizations certain nuclear material and information. An agreement for cooperation, which requires legislative review, is required for sharing material and information controlled by the AEA with another nation or regional defense organization. DoD and the Department of Energy have established the Joint Atomic Information Exchange Group (JAIEG), whose function is to review proposed foreign disclosures of AEA controlled information.

d. **The Freedom of Information Act (FOIA), Public Law 89-554 (1966), (5 U.S.C. 552)**

The FOIA *(reference g)* requires the United States Government to provide the public access to U.S. Government information, upon request, except when the information falls within any of nine categories of information that qualify for exemption to the requirement. Only certain designated DoD officials have the authority to authorize a specific exemption. DoD Regulation 5400.7-R *(reference h)* implements the FOIA within DoD. The first exemption category is national security information that is classified pursuant to E.O. 13526 *(reference i*), or predecessor or successor orders, as CONFIDENTIAL, SECRET, or TOP SECRET. The other eight exemption categories describe types of unclassified information that may be withheld from public disclosure. It is information in these eight categories that may be marked FOR OFFICIAL USE ONLY (FOUO). Safeguarding measures for information marked FOUO are contained in DoD Regulation 5200.1-R (*reference j*). The FOIA is discussed further in Chapter 4.

e. **10 U.S.C. 130**

10 U.S.C. 130 (*reference k*), also known as Public Law 98-94, permits the Secretary of Defense to withhold from public disclosure certain export controlled technical data with military or space application that is in the possession of, or under the control of the DoD. This information is identified by specified distribution and export control warning statements. DoD Directive 5230.25 *(reference l)* implements this law. DoD Directive 5230.24 *(reference m)* describes the distribution statements. This subject is covered in greater detail in Chapter 4.

3. **Executive Orders and National Security Council and Other Directives**

a. **E.O. 13526, Classified National Security Information.**

(1) E.O. 13256 provides the basis for classifying certain information as CONFIDENTIAL, SECRET, or TOP SECRET. The level of classification is based on the degree of damage to U.S. national defense or foreign relations that would occur from the loss or compromise of the information. The order also identifies the types of information that

qualify for classification and establishes the basic policy for declassification, downgrading, and for protecting classified information.

(2) It also establishes conditions that apply to all decisions on access to classified information, including foreign disclosure decisions, which are discussed in Chapter 3. First, it prohibits the release of classified information outside the Executive Branch without an assurance that it will receive equivalent protection. Second, it requires a determination that prospective recipients are trustworthy and have a need-to-know to perform or assist in a lawful and authorized government purpose. Third, it requires the originator's consent for further dissemination (third party rule). Fourth, it provides for safeguarding information received in confidence from or jointly produced with foreign governments and international organizations. It also provides for holding in confidence, by mutual agreement, information produced jointly with them. Fifth, it specifies that access may be permitted when necessary to perform or assist in a ***lawful and authorized*** governmental function. With respect to the latter, *lawful and authorized*, the international initiative that will result in the disclosure of classified information must be provided for in law, and the initiative must be authorized by an official having been given such authority. This principle applies, in fact, to all international programs, whether involving classified information or unclassified information that is controlled.

(3) This Executive Order is implemented by Classified National Security Information Directive 1, (32 Code of Federal Regulations (CFR) 2001 and 2004). The Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) is the agency that overseas the Executive Order. The Directive is sometimes referred to as ISOO Directive Number 1 (*reference* n).

b. **E.O. 12333, and Director Central Intelligence Directives (DCID) 6/6 and DCID 6/7**

E.O. 12333 *(reference o)* provides the basis for controlling disclosures of classified U.S. intelligence to officials of foreign governments and international organizations. DCIDs 6/7 and 6/6 *(references p and q)* provide the policy and procedures for the foreign disclosure of classified intelligence information. DoD Directive C-5230.23 *(reference r)* implements DCID 6/7 and establishes DoD policy and procedures and assigns responsibilities for the control of disclosures of classified U.S. intelligence to officials of foreign governments and international organizations. DCID 6/6, implemented by DoD Regulation 5200.1-R establishes a system for marking and controlling the dissemination and use of intelligence information produced by the intelligence community. The basic requirements for the disclosure of military intelligence are described in the National Disclosure Policy (NDP-1), *(reference s)*.

c. **National Security Decision Memorandum 119 (NSDM 119)**

(1) NSDM 119 *(reference t)* is the basic policy that governs the disclosure of U.S. CMI to foreign governments and international organizations and their representatives.

(2) NSDM 119 charges the Secretary of Defense and the Secretary of State with the responsibility for implementing the policy. It requires the Secretaries of Defense and State to form an interagency mechanism and establish procedures to carry out this directive. The procedures are in the National Disclosure Policy (NDP-1); the mechanism is the National Military Information Disclosure Policy Committee (NDPC). The implementation of NSDM 119 is discussed in detail in Chapter 3.

d. **International Traffic in Arms Regulations (ITAR), 22 CFR 120-130**

The ITAR (*reference c*) implements Section 38 of the AECA with regard to commercial exports of defense articles and services and related technical data. The Directorate of Defense Trade Controls (DDTC), Department of State, administers the ITAR. The ITAR contains the USML (Part 121) which identifies the defense articles that are subject to export control. The export of classified defense articles and technical data also are subject to the provisions of the NDP-1, which is discussed in detail in Chapter 3.

e. **Export Administration Regulations (EAR), 15 CFR 768-799**

These regulations *(reference u)* implement the EAA. The Secretary of Commerce issues the EAR in consultation with the Secretaries of Defense and State. The EAR governs the export of most goods that are not inherently of a military nature and thus do not qualify as defense articles. It takes special notice of those civilian goods that can also enhance the military capability of the recipient (i.e., dual-use items). The CCL, in Part 774 of the EAR, describes the items, technical data and software that are subject to control. The Bureau of Industry and Security (BIS), Department of Commerce, administers the EAR.

f. **National Policy Governing the Release of Information Systems Security (INFOSEC), Products and Associated INFOSEC Information to Foreign Governments (NSTISSP 8).**

NSTISSP 8, a limited distribution document issued by the Committee on National Security Systems (CNSS), provides the policy for the export or release of INFOSEC information (COMSEC and COMPUSEC) and material. DoD Instruction S-5225.1 *(reference v)* implements the NSTISSP. The sharing of COMSEC information also is subject to coordination with the Joint Staff in accordance with Chairman, Joint Chiefs of Staff Instruction 6510.06 (*reference w*).

C. The Basics

1. While all of the laws, executive orders, and policies described above have some bearing on participation in international programs, the principal ones that have a bearing on the security requirements for most international programs covered by this Handbook are the Arms Export Control Act, Executive Order 13526, and National Security Decision Memorandum 119. They

establish the basic principles and conditions for sharing classified information with foreign governments and international organizations.

a. Access and Protection. The conditions and criteria established by the basic laws and policies require that two fundamental considerations be addressed prior to involvement in a program involving the sharing of U.S. defense articles or information with another country or international organization. These are: whether their access is in the best interests of the United States and whether the articles or information will be protected—***ACCESS*** and ***PROTECTION***. The questions that must be answered to address these considerations, in order, are: (i) is all of the information or technology to be shared authorized for disclosure to the other government or international organization? (ii) does the potential recipient government or organization have the capability and intent to provide protection substantially equivalent to that provided by the United States? No discussions leading to the initiation of a program should take place until these considerations are satisfied.

(1) The **Arms Export Control Act**, which governs the export of defense articles and defense services (i.e., technical data) to foreign countries and international organizations, and covers both commercial and government programs, ***forms the legal basis for the security requirements of most DoD international programs***. The Act states that exports (i.e., **access**) must be consistent with U.S. foreign policy interests, strengthen the security of the United States, and contribute to world peace. The Act also requires the President to give 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 described in subparagraph B.2.a.(2), above.

(2) **Executive Order 13526** which establishes the Executive Branch's National Security Information Program 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.*** 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 ISOO is the responsible Executive Branch office for implementation of the Executive Order. To assist in implementing the E.O., ISOO issued 32 CFR Part 2001 and 2004, entitled "Classified National Security Information Directive No. 1" and sometimes referred to as ISOO Directive Number 1. Within DoD, E.O. 13526 and 32 CFR Part 2001 and 2004 are implemented by DoD 5200.1-R.

(3) **National Security Decision Memorandum 119** is the basic national policy governing decisions on the disclosure of CMI to foreign governments and international organizations. NSDM 119 reiterates the basic requirements of the AECA and Executive Order 13526 and emphasizes that classified military information is a national asset and the U.S. Government will not share it with a foreign government or international organization (i.e., ***permit access***)

unless its **disclosure *will result in a clearly defined benefit to the United* States** and the recipient government or organization will provide ***substantially the same degree of protection***.

2. **Government-to-Government Principle**. The "government-to-government principle," derived from the AECA and NSDM 119, means that classified information and technology is shared by governments with other governments and international organizations. It is the other government or international organization that has status in international law, and it will be held responsible for protecting the information or material. This principle governs two activities related to international programs. It applies to the ***export or disclosure decision*** and to ***transfers*** of classified information and material. First, in keeping with the AECA, E.O. 13526 and NSDM 119, the decision to be made is whether the U.S. Government will disclose classified information to another government or international organization (i.e., **access**). If the answer is yes, 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 in writing by the appropriate officials of the responsible governments in order to ensure proper ***protection***, i.e., collectively, a **government-to-government transfer**. This 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 and the recipient government assumes responsibility for the custody and protection of the articles or information. Receipts are required for international transfers to document the transfer of security responsibility (although many governments will waive this requirement for their RESTRICTED information). Transfers of classified material as freight occur between Designated Government Representatives (DGR). A DGR of the sending government will verify that the necessary authorization is in place, assure that the material is properly packaged and proper transfer arrangements have been agreed upon by the governments, and ensure that the material is placed in the proper transfer channels. A DGR of the receiving government will assure receipt of the material and assume custody and control on behalf of the recipient government. (Note: Freight forwarders are transfer agents, making transfer arrangements for either the sending or receiving government, and cannot perform the responsibility of a DGR.) A security assurance must be obtained prior to transferring classified material to a representative of a foreign government or international organization.

D. ISSUES NOT COVERED

This handbook does not cover the details of information security, personnel security, physical security, communications security or other specific security disciplines. It also does not cover intelligence programs. To the extent that this handbook addresses such matters, it does so in terms of their relationship to foreign disclosure or export decisions related to international arms programs and the related security requirements. However, pertinent references are provided, where applicable.