CHAPTER 3

NATIONAL DISCLOSURE POLICY

A. INTRODUCTION

1. The National Disclosure Policy (NDP), the policy that governs the disclosure of United States classified military information (CMI) to foreign governments and international organizations, stems from National Security Decision Memorandum (NSDM) 119 *(reference t)*. The Secretaries of State and Defense, consulting as appropriate with other Department and Agency heads, are jointly assigned the responsibility for implementing NSDM 119. NDP-1 *(reference s)* is the interagency document, which implements this policy. It is issued by the Secretary of Defense with the concurrence of the Secretaries of State and Energy and the Director of Central Intelligence (DCI). This assignment of responsibility includes:

a. The establishment and management of an interagency mechanism (the National Military Information Disclosure Policy Committee (NDPC) and implementing procedures;

b. The promulgation of specific disclosure criteria and limitations, definitions of terms, and other guidance governing decisions on the disclosure of CMI;

c. The continuing review of intelligence and the conduct of on-site surveys to determine the capability of foreign recipients to provide CMI the requisite degree of security protection;

d. The submission of an annual report to the National Security Council (NSC) covering the highlights of the program, including exceptions to policy that were approved during the reported year;

e. The negotiation of General Security Agreements (GSAs) or other bilateral security arrangements with foreign governments, outlining the responsibilities of both parties pertaining to the safeguarding of classified information provided by the other party. These agreements are described under Section H, below; and,

f. The development and issuance of instructional guidance to be uniformly applied by all personnel involved in any manner with international programs through which CMI may be disclosed.

2. DoD Directive 5230.11 *(reference ee)* implements the NDP within the Department of Defense (DoD).

B. CLASSIFIED MILITARY INFORMATION (CMI)

1. CMI is information which is originated by or for the DoD or its Components or is under their jurisdiction or control and which requires protection in the interests of national security. It is designated TOP SECRET, SECRET and CONFIDENTIAL as described in Executive Order (E.O.) 12958 *(reference i)*. CMI may be disclosed in oral, visual or documentary form and is divided into eight categories:

a. **Category 1 - Organization, Training and Employment of Military Forces**. Military information of a general nature necessary to the organization of military, paramilitary or irregular forces. It includes those tactics, techniques and tactical doctrine (including military intelligence and counterintelligence doctrine and techniques) necessary to train and employ those forces. This category does not include specific technical data and training needed to operate and maintain individual items of military materiel and munitions;

b. **Category 2 - Military Materiel and Munitions**. All military materiel, arms and munitions procured and controlled by the U.S. government for the equipage, operation, maintenance and support of its military forces or the military, paramilitary or irregular forces of its allies. This category includes items developed by U.S. private interests as a result of U.S. government contracts or derived from technology paid for by the U.S. government. Items proposed for sale by U.S. private interests that are covered under the United States Munitions List (USML); i.e., Part 121 of the International Traffic in Arms Regulations (ITAR) *(reference c)*, or items specifically covered by other U.S. government export control regulations fall within this definition. (Items under development fall under Category 3.) This category also comprises information to include technical data and training necessary to operate, maintain or support specific military materiel, arms or munitions. It does not include information and techniques used to produce, co-produce or manufacture the item;

c. **Category 3 - Applied Research and Development Information**. CMI resulting from the extension of fundamental theories, designs and data from purely theoretical or experimental investigation into possible military applications. This includes research, the construction and testing of prototypes and design changes affecting qualitative performance during the service life of an item. This also includes engineering data, general operational requirements, concepts and military characteristics required to adopt the item for production. Development ceases when materiel has completed operational suitability testing or has for all practical purposes been adopted for military use or production. It includes tactics, techniques and tactical doctrine pertaining to specific equipment not yet in production or not yet approved for adoption by U.S. forces. It includes military information, materiel or munitions under development by U.S. private interests as a result of U.S. government contracts, or derived from technology paid for by the U.S. government;

d. **Category 4 - Production Information**. Designs, drawings, chemical and mathematical equations, specifications, models, manufacturing techniques, software source code and related information (excluding Categories 2 and 3 information) necessary to manufacture or

substantially upgrade military materiel and munitions. The following information is furnished to further clarify the definition of Production Information:

(1) **Manufacturing information** (more sensitive than Build-to-Print or Assembly information): This includes the know-how, techniques and processes required to produce or substantially upgrade military materiel and munitions. A manufacturing process or technique is a set of instructions for transforming natural substances into useful materials (metals, plastics, combustibles, explosives, etc.) or for fabricating materials into aerodynamic, mechanical, electronic, hydraulic or pneumatic systems, subsystems and components. Software source code including related documentation that describes software or development know-how for a particular U.S. warfare system which has completed Acquisition Milestone B (Technology Development) or documentation used for production thereof are considered to be design and manufacturing data and equivalent to Category 4, Production Information. A manufacturing data package describes how to manufacture, test and accept the item being produced and what tools and processes are required. Types of manufacturing information include drawings, process sheets, wiring diagrams, instructions, test procedures and other supporting documentation. Software source code and software documentation that contain or allow access/insight to classified algorithms or design rationale are considered to be manufacturing information requiring NDPC review and approval. Unclassified software source code and software documentation that is required for minor software maintenance, interface/integration, or to make administrative changes to tables, symbology, markers, displays will be handled through normal technology transfer channels and does not require NDPC review. Such information will normally be considered for release to foreign customers who possess an indigenous weapon system or verifiable country unique operation or maintenance requirement the United States is willing to support. Manufacturing information classified solely because of related Category 2 information should be handled as Category 2 information.

(2) **Build-to-Print Information** (more sensitive than Assembly information). Assumes the country receiving the information has the capability to replicate an item, subsystem or component from technical drawings and specifications alone without technical assistance. Release of supporting documentation (e.g. acceptance criteria, object code software for numerical controlled machines) is permissible. Release of any information which discloses design methodology, engineering analysis, detailed process information or manufacturing know-how associated with the end item, its subsystems or components is excluded. Build-to-Print information is not considered Category 4 information. Disclosure of Build-to-Print information is approved through normal technology transfer channels unless other NDP categories are involved which require NDPC review and approval.

(3) **Assembly Information**. Normally associated with hardware (parts or kits to be assembled, special tooling or test equipment to accomplish specific tasks) and information which allows assembly and testing of the finished product. Only top level drawings will be released. Detailed assistance is not to be provided if such assistance would provide production or manufacturing techniques. The level and depth of assembly

or co-assembly allowed is subject to negotiation and defined in the co-assembly or coproduction agreement. Assembly information is not considered Category 4 information. Disclosure of Assembly information must be approved through normal technology transfer channels unless other NDP categories are involved which require NDPC review and approval.

e. **Category 5 - Combined Military Operations, Planning and Readiness**. That information necessary to plan, assure readiness for and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. Includes installations and facilities located within territory under the jurisdiction of, or of direct concern to, the recipient foreign government or international organization. This category is limited to that information on installations and facilities as well as readiness, planning and operational information which is necessary to further specific multilateral or bilateral plans and agreements for common defense purposes between the United States and the recipient. It does not include strategic planning and guidance or North American Defense information;

f. **Category 6 - U.S. Order of Battle**. Information pertaining to U.S. forces located within territory that is under the jurisdiction of a recipient government or is otherwise of direct concern to a foreign government or international organization. In general, authorization is limited to U.S. Order of Battle in the recipient countries or in adjacent geographical areas;

g. **Category 7 - North American Defense**. North American Defense Information is that which concerns plans, programs, projects, operations and certain specific technical data pertaining to equipment directly related to North American Defense, especially when it is originated by or under the mission and control of the North American Aerospace Defense Command (NORAD) North American Defense Information includes, but is not limited to:

(1) Plans and related documents prepared by combined United States/Canada defense agencies.

(2) Information concerning U.S. operational and logistical plans for employment of reserve forces.

(3) Information revealing the vulnerability of a North American Defense area, or a vulnerability or official appraisal of the combat readiness of any unit or facility, or the effectiveness of North American Defense systems.

h. **Category 8 - Military Intelligence**. Information of a military character pertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the DCI.

C. DISCLOSURES NOT COVERED BY THE NDP

1. The NDP does not govern the disclosure of the following types of information:

   a. Classified information the disclosure of which is prohibited by Federal law or international agreement.

   b. Naval nuclear propulsion information, except under an agreement negotiated under the Atomic Energy Act of 1954, as amended *(reference f)*.

   c. Proprietary information owned by private firms or citizens. If release is authorized by legislation, that legislation will govern the release. (Note: While the private firm may retain property rights, foreign disclosure of any classified information is governed by the NDP-1.)

   d. National or interdepartmental intelligence produced within the National Foreign Intelligence Board structure. Foreign disclosure is governed by DCI Directives 6/6 and 6/7 (*references p and q*).

   e. Information Systems Security (INFOSEC), Communications Security (COMSEC), and Signals Intelligence (SIGINT) information and products that are under the jurisdiction of the Committee on National Security Systems (CNSS) (formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) and the DCI SIGINT Committee. CNSS disclosure procedures are set forth in a NSTISSC policy document, NSTISSP #8. CNSS controls the release of INFOSEC. The DCI SIGINT Committee controls the release of SIGINT information. Information that has been sanitized to delete the controlled INFOSEC and SIGINT information is governed by NDP-1.

   f. Operational counterintelligence information, the disclosure of which is the responsibility of the DCI. DCI Directives apply to the disclosure of counterintelligence information.

   g. Atomic information, disclosures of which are made in accordance with the Atomic Energy Act of 1954. The Joint Atomic Information Exchange Group (JAIEG) is responsible for reviewing these releases.

   h. Strategic planning and guidance. Only the Secretary of Defense or the Deputy Secretary of Defense may authorize the disclosure of this information.

2. Although these categories of information are not covered by the NDP-1, they can have a bearing on NDP decisions. If any of the information is included in a defense system or program, the decision of the responsible agency must be obtained before any commitment can be made on the defense system or program.

D. DISCLOSURE AUTHORITY

1. The Secretary of Defense and the Deputy Secretary of Defense hold original authority to disclose CMI and grant exceptions to disclosure policy.

2. Through DoD Directive 5230.11, the Secretary of Defense has delegated authority to the following DoD officials to disclose CMI originated by or under the control of their organizations:

a. The Secretaries of the Military Departments.

b. The Chairman of the Joint Chiefs of Staff.

c. The Under Secretary of Defense for Policy.

d. The Under Secretary of Defense for Intelligence.

e. The Under Secretary of Defense for Acquisition, Technology and Logistics.

f. The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer.

g. The Director, Defense Intelligence Agency.

h. The Director, National Security Agency/Central Security Service.

i. The Director, Missile Defense Agency.

3. Each of these officials must appoint a senior official in writing to be the Principal Disclosure Authority (PDA) within that Component. They may also delegate disclosure authority to the heads of commands, agencies and major staff elements under their authority. These heads of commands, agencies and major staff elements must then in turn appoint a Designated Disclosure Authority (DDA) to control disclosures of CMI by his or her organization.

4. The PDAs for the above organizations are listed at Appendix A. They are responsible for:

a. Controlling disclosures within their respective Component.

b. Ensuring the competency of subordinate officials appointed as DDAs.

c. Ensuring coordination of their proposed disclosure actions with other DoD Components having a joint or shared interest in the information.

d. Appointing a member and alternate to represent their Component on the NDPC.

e. Ensuring that their Component complies with CMI disclosure reporting requirements of DoD Directive 5230.11 by entering disclosure decisions into the CMI Database of the Foreign Disclosure System (FDS) on the Security Policy Automation Network (SPAN) as described in Section E. 8 below. (Note that the FDS replaces the Foreign Disclosure and Technical Information System (FORDTIS).)

f. Coordinating requests for disclosures of CMI involved in litigation with the DoD or Component General Counsel, as appropriate.

g. Ensuring that persons traveling overseas receive disclosure guidance and are knowledgeable of and comply with the special access program overseas travel policy in DoD Regulation 5200.1-R, (*reference j*) and DoD Directive 4500.54 (*reference pp*).

5. The delegation of disclosure authority must be in writing and clearly state the limits of the authority. The means of delegating disclosure authority normally is by a Delegation of Disclosure Authority Letter (DDL) or a Component regulation. Broad disclosure authority normally is promulgated in Component regulations. The DDL normally is used for individual programs and is discussed in detail in Chapter 8. DDAs are responsible for reporting in the FDS all disclosures of CMI made under their delegation.

E. DISCLOSURE DECISIONS

1. **General**. The NDP establishes the framework in which foreign disclosure decisions are made by PDAs or DDAs. It is derived from the requirements of the Arms Export Control Act (AECA) (*reference b*), E.O. 12958, and NSDM 119. In making a disclosure decision these officials must assure that:

a. The proposed disclosure is in support of a lawful and authorized U.S. government purpose;

b. Their Component is the originator of the information. If another DoD Component or U.S. government department is the originator, the request or proposal must be forwarded to them for a decision;

c. They personally have disclosure authority (i.e., a DDL or other written authority);

d. The disclosure meets all disclosure criteria and conditions in Subsections 2 and 3, below;

e. The classification level of the CMI does not exceed the classification level that has been delegated for the subject matter category and specific nation or organization as described in Annex A, NDP-1 or Component implementing regulations or DDL;

f. The disclosure is consistent with applicable Disclosure Policy Statements in Annexes B and C, NDP-1;

g. The decision would be consistent with the "false impressions" policy (see paragraph 6. below) and disclosure limitations (see paragraph 4. below);

h. Other DoD Components having joint or shared interest in the information

2. Disclosure Criteria.

a. A decision to disclose CMI must satisfy each of the following five criteria. Failure to satisfy any one of the criteria is cause for denial unless the proponent of the disclosure believes disclosure would result in a clearly defined benefit to the United States and an exception to the NDP is obtained as described in Section G, below. The criteria are:

(1) Disclosure of the information is consistent with U.S. foreign policy objectives toward the recipient nation or organization or geographical region. Regional considerations may affect a proposed disclosure to a particular country. For example, explain how:

(a) The disclosure supports a mutual security or similar agreement.

(b) The prospective recipient government cooperates with the United States in pursuance of military or political objectives that are compatible with those of the United States and the proposed disclosure contributes to the furtherance of those objectives.

(2) Disclosure of the information is consistent with, and will not jeopardize, U.S. military and security objectives. The objective of this criteria is to place a value on the knowledge or capability to be disclosed (it is a "national asset") and estimate the damage in the event of compromise. To ensure that this criterion is met, the decision-maker must determine:

(a) The level of technology or sensitivity of information involved, its foreign availability and its criticality to U.S. systems or plans;

(b) The damage to U.S. military capabilities or plans if a compromise occurs;

(c) The susceptibility of the information or technology to compromise or reverse engineering and the capability of the recipient to exploit the knowledge that is gained;

(Note: The decision-maker must use the above determinations in an analysis of the risks versus gains and the need to develop alternatives to minimize or prevent damage, such as time-phasing of disclosures, withholding of certain information or developing an export version of the hardware, as described below.)

(3) The prospective recipient will afford the information substantially the same degree of protection as that provided by the United States. The objective is to estimate the risks

involved with respect to the intended recipient government or international organization. This criterion is based on the AECA and E.O. 12958, as discussed in Chapter 2. It requires an evaluation of the proposed recipient government's or international organization's capability and intent to protect the information.

(a) The existence of a GSA is normally sufficient to infer the intent of the recipient. Annex A of NDP-1, lists the countries covered by such agreements. (The list is controlled and is releasable to government agencies only. Contractors can verify the existence of these agreements with the Defense Security Service (DSS).

(b) Validation of the capability of the recipient to provide the necessary degree of protection is generally based on three sources of information. First, the NDPC periodically obtains copies of other countries security laws and regulations and visits the countries with which the U.S. government shares CMI to review implementation of the laws and regulations. The NDPC reports on these visits contain a description of each country's security program. Copies of the reports are provided to each Department or Agency represented on the NDPC. Second, the NDPC tasks the intelligence community to provide an assessment of foreign government security programs and their compliance therewith. These reports are also provided to NDPC member Departments and Agencies. Third, the intelligence community can be tasked to provide special reports related to specific technologies and capabilities.

(4) Disclosure will result in benefits to the United States that are at least equivalent to the value of the information disclosed. The benefits must outweigh the risks that may be involved in comparison to the likely damage that may result, as determined by criteria numbers 2 and 3.

(a) The benefits may be a contribution to U.S. political, military, or economic objectives in relation to the recipient(s) or region. Primary issues to be considered are standardization and interoperability of equipment; increased defensive capability for an important ally; or support of an important political objective.

(b) Economic benefit alone is not an acceptable basis for sharing CMI. However, programs that satisfy other requirements and have a positive impact on the U.S. industrial and technology bases generally will receive a favorable review.

(c) Establishment of, or continued good relations with the recipient is normally not an acceptable benefit in a single disclosure or export. Such relations rarely hinge on a single decision. However, foreign government support or participation in a specified military objective may result in an important advantage to the United States.

(5) The information to be disclosed must be limited to that which is necessary to fulfill the purpose of the disclosure. For example, if the purpose of the disclosure is to support the sale of an item of equipment, the recipient government is entitled to receive information necessary for operating and maintaining it and for training. Other information, such as research and development and production information would be withheld. If risks are

significant and the likely damage would be harmful to U.S. military interests, the information to be provided may have to be tailored or sanitized, or a lesser capability may be provided.

3. Disclosure Conditions.

a. Once the decision has been made that CMI can be disclosed to a foreign government or international organization, actual release is dependent upon the recipient agreeing to certain minimum conditions. These conditions, some of which are similar to those required by the AECA, are:

(1) The recipient will not reveal the information to a third-country government, national, organization or other entity of a third country without the written permission of the originator;

(2) The recipient will afford the information substantially the same degree of security protection as the United States affords to it;

(3) The recipient will use the information only for the purpose for which it was provided;

(4) The recipient will report promptly and fully to U.S. authorities any known or suspected loss or compromise of U.S. CMI released to it;

(5) Individuals who are to be given access will have a need-to-know and security clearance granted by their government at a level at least equal to that of the CMI to be disclosed. Contractor facilities must have at least an equal level of facility clearance and storage capability, if applicable, granted by their government (see Chapter 6);

(6) Transfer of the information will be through government-to-government channels (See Chapter 6);

(7) Visits will be permitted by security experts to review and discuss each other's security policies and practices for protecting CMI; and,

(8) The recipient must agree to abide by or meet U.S.-specified special terms and conditions for the release of U.S. information or material.

b. If there is a GSA with the intended recipient government, the above conditions normally will be satisfied by the terms of that agreement (see Section H., below). Therefore, for bilateral government programs (e.g., Foreign Military Sales (FMS), coproduction, cooperative research and development) the security requirement normally can be satisfied by referencing the applicable GSA in the sales contract or program agreement. However, in those cases where there is no GSA with the intended recipient government or extraordinary security requirements must be met, and in the case of commercial sales, other solutions are necessary, as described below. When there is no GSA or equivalent agreement with the intended recipient government, the specific security conditions may be included in the program agreement for government programs, or in an exchange of diplomatic notes or a

separate program security agreement for commercial programs. The agreement must specify that the security conditions will apply as long as the recipient has the U.S. information or system in its custody. An example of a program specific security agreement can be found in the Security Assistance Management Manual (SAMM) (reference d).

c. Requests for commercial export authorizations that will involve the transfer of Significant Military Equipment (SME) (see Appendix GG) or classified information must be accompanied by a Department of State form DSP-83, Nontransfer and Use Certificate, with all items properly completed and signed. If classified information is involved, the form must be signed by an official of a foreign government agency that has the authority to commit the government to compliance with the certification contained therein (see Sections 124.10 and 125.3(a) of the ITAR). The foreign end-user should be consulted to identify the responsible government agency. The signature of an appropriate foreign government official is accepted as recognition that the transfer is for government purposes and, therefore, that the classified material will be protected in compliance with a GSA, or other legally binding government-to-government security agreement with the recipient government. However, if there is no GSA or other government-to-government agreement containing required security principles, such agreement will be necessary prior to the transfer of the material (see Subsection c., above). The DSS or other U.S. government representative will provide information to contractors on the existence of specific agreements, as required. If a foreign government refuses to sign the Form DSP-83, citing an existing agreement as the basis for its refusal, that government should be requested to contact the Department of State, Directorate of Defense Trade Controls (DDTC), in writing, through its embassy in Washington, D.C. to address the requirement. The correspondence must cite the pertinent agreement and certify that the material to be transferred is for government purposes and will be protected in compliance with the cited agreement.

4. **Limitations on Disclosure Authority**. The disclosure authority delegated to PDAs and DDAs is limited as follows:

a. Classified information officially obtained from a foreign government may not be disclosed unless the originating government specifically agrees in writing to further disclosure;

b. Combined military information (Category 5 information) (see B.1.e., above) may not be disclosed unless all parties agree in writing;

c. Joint information (see Appendix FF) may not be disclosed without prior written agreement of all DoD Components or Federal Departments and Agencies having control or jurisdiction of the information;

d. Information originated by or for another Department or Agency may not be disclosed unless it consents in writing to the disclosure;

e. Disclosures of intelligence information shall be governed by the requirements of NDP-1. (NOTE: These requirements are classified and therefore cannot be described in this Handbook.)

f. Disclosure under Subsection a. through c., above, must be recorded in the FDS by the organization that makes the disclosure. Disclosures under Subsections d. and e. must be reported by the organization that authorizes the disclosure. The FDS is discussed further in Subsection E. 8, below.

5. **Security Assurances**. Designated disclosure authorities shall not authorize the disclosure of CMI to a foreign national prior to the receipt of a security assurance from the sponsoring foreign government or international organization concerning the facilities and individuals that ultimately are to receive the information (see Chapters 6 and 7).

6. **False Impressions**. There are two policies that prohibit disclosures or releases that might create a false impression that the DoD is willing to provide defense articles or information to foreign entities. The first concerns the disclosure of classified information, material or technology. The second deals with the furnishing of funds, goods and services to foreign governments and international organizations in a foreign assistance program.

a. NDP-1 prohibits creating false impressions of the U.S. government's readiness to make available CMI, including classified equipment and technology. Accordingly, proposals to or discussions with representatives of foreign governments and international organizations which result from either U.S. or combined initial planning and which will lead to the eventual disclosure of classified military equipment, technology, or information, including intelligence threat data or countermeasures information, must be authorized in advance by designated disclosure officials in the Departments and Agencies originating the information. However, if the disclosure of any CMI ultimately to be involved will require an exception to NDP-1, the decision is to be made by the Secretary of Defense, Deputy Secretary of Defense or the NDPC, in accordance with DoD Directive 5230.11.

b. U.S. policy prohibits "... an individual representing the U.S. [from making] commitments, expressed or implied, to furnish funds, including long term credit arrangements, goods or services to foreign governments (the terms foreign government and foreign official shall include officials of any international organization or supra-national authority as well as of any foreign national government) without:

(1) Appropriate governmental clearances;

(2) Satisfactory assurance that such commitments (a) can and will be met, and (b) do take into account the best interests of the U.S. in the use of its resources; and,

(3) A clear understanding with the recipient about the nature, scope and time-span of the commitment."

7. **Disclosures Related to Actual or Potential Hostilities**. Under conditions of actual or imminent hostilities, any Unified Commander may disclose CMI through TOP SECRET to an actively participating allied force when support of combined combat operations requires it. The U.S. Commander must notify the Chairman of the Joint Chiefs of Staff (JCS) immediately of such disclosures. The Chairman of the JCS, in turn, must notify the Office of the Under Secretary of Defense for Policy, ATTN: Chair, NDPC. The Chair will determine whether any limitations are necessary on continuing disclosure of the information. The U.S. Commander will receive appropriate instructions through the Chairman, JCS. The JCS will be responsible for reporting the authorized disclosures in the FDS.

8. **Reporting of Disclosure Decisions**. *All disclosures and denials* of CMI must be reported in the CMI Database of the FDS on SPAN..

a. The FDS is a Windows-based automation system consisting of both an online and an offline application. The online application supports the international security foreign disclosure processes, to include disclosure reporting by disclosure authorities that have high-speed links to SPAN, normally via the Secret Internet Protocol Network (SIPRNET). The FDS offline capability facilitates required disclosure reporting by DDAs who currently do not have high-speed links (i.e., Secret Internet Protocol Router Network (SIPRNET)) to SPAN. This capability provides the transfer of data from the offline activity to an online activity for electronic uploading to the FDS database.

b. The FDS is designed to provide support to the international security community in fulfilling DoD responsibilities assigned by the NDP-1, the AECA and the EAA (*reference e*). It supports the implementation of departmental policies contained in DoD Instruction 2040.02, (*reference rr*), DoD Directive 5230.11, DoD Directive C-5230.23 *(reference r)*, and DoD Directive 5230.20, *(reference gg)*.

c. Decisions on the release of CMI; liaison officer certifications; personnel exchanges; munitions, Commerce Control List (CCL), and international export control regime license applications when they are required; and NDP exception cases (NDPE) are recorded in FDS and/or other SPAN databases. Foreign government visit requests are processed and recorded in the Foreign Visit System (FVS) on the SPAN.

F. THE NDPC

1. **Functions**. The NDPC is responsible for formulating, issuing, administering and monitoring the implementation of the NDP. It may grant exceptions to the NDP under the authority granted by the Secretary of Defense. Only committee members may sponsor requests for exceptions to policy. A DoD Component not represented on the Committee must obtain disclosure authority from the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (DUSD (TSP & NDP)). The NDPC also conducts security survey visits to perform evaluations of the security programs of foreign governments and international organizations.

2. **Committee Membership**. By agreement between the Secretaries of State and Defense, a representative of the Secretary of Defense chairs and provides administrative support for the NDPC. The Under Secretary of Defense (Policy) designates the Chairperson. The Director, International Security Programs, Office of the DUSD (TSP & NDP) provides the Executive Director, Executive Secretary and administrative support of the Committee. There are two categories of Committee members.

a. General members have a broad interest in all aspects of Committee deliberations and therefore, vote on all issues that come before the committee. They are representatives of:

(1) The Secretary of State.

(2) The Secretary of Defense.

(3) The Secretaries of the Army, Navy, and Air Force.

(4) The Chairman of the Joint Chiefs of Staff (Also represents the Commander of the Unified Commands).

b. Special members have a significant interest in some, but not all, aspects of committee deliberations. They normally vote only on those issues in which they have a direct interest. They are:

(1) The Secretary of Energy.

(2) The Director of National Intelligence

(3) The Director of Central Intelligence.

(4) The Under Secretary of Defense for Policy.

(5) The Under Secretary of Defense for Acquisition, Technology and Logistics.

(6) The Under Secretary of Defense for Intelligence.

(7) The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.

(8) The Assistant to the Secretary of Defense (Nuclear, Chemical and Biological Defense Programs).

(9) The Director, Defense Intelligence Agency.

(10) The Director, Missile Defense Agency.

(11) The Director, National Geospatial-Intelligence Agency.

(12) The Director, National Security Agency.

G. REQUESTS FOR AN EXCEPTION TO NATIONAL DISCLOSURE POLICY

1. A proposed disclosure would have to be denied or, if the proponent of the disclosure desires to pursue a disclosure, an exception to the disclosure policy would be required for one or more of the following reasons:

a. A proposed disclosure may not satisfy NDP disclosure criteria described in Subsection E.2., above;

b. The proposed disclosure may be inconsistent with one or more of the policy statements in Annexes B and C in NDP-1 (*reference s*);

c. The classification assigned to the highest level of classified information to be disclosed may exceed the delegated disclosure authority level in NDP-1; or,

d. The information to be disclosed may be under the jurisdiction of, or shared by another Department or Agency that does not support the disclosure.

2. If one or more of the above situations apply, but it is believed that a disclosure will result in a clearly defined benefit to the United States, an exception to policy may be requested. Requests for exceptions to policy must be forwarded through channels to the official who represents the requester's organization on the NDPC. A request for an exception to the NDP must include the information required in Appendix B. The request must represent a fully coordinated position of the requesting organization. The NDPC Executive Secretary ensures that all members having an interest in the request for exception to policy can receive a copy via the FDS. The members must respond with a fully coordinated position of their Department or Agency within 10 working days. If there is not unanimous agreement on the proposed disclosure, the Committee Chairman must formulate a proposed "Chairman's decision" and inform the members of the decision, again within 10 working days. The decision of the Chair will become final unless successfully appealed to the Secretary of Defense or Deputy Secretary of Defense by the cognizant Department or Agency head or PDA within 10 working days.

H. SECURITY AGREEMENTS

1. After a favorable disclosure decision is made, actual transfer of CMI cannot occur until the intended recipient government agrees to the conditions described in Subsection E.3., above. The

existence of a GSA or equivalent, and, if applicable, an Industrial Security Agreement (ISA) normally will satisfy this requirement. (Note: The GSA also is known as a General Security of Information Agreement (GSOIA) or a General Security of Military Information Agreement (GSOMIA).) In general, agreements negotiated prior to 1970 cover all classified information and those negotiated since 1970 cover only CMI. This Handbook contains the pertinent requirements for such agreements. Information on specific agreements may be obtained from the responsible DDA or from DSS.

a. The GSA, negotiated through diplomatic channels, requires each party to the agreement to afford to the classified information provided by the other substantially the same degree of security protection afforded it by the releasing government. (Note: It is for this reason that foreign government information must be protected differently than U.S. classified information.) It contains provisions concerning limits on the use of each government's information, including restrictions on third party transfers and proprietary rights. It provides for the reporting of losses or compromises or possible losses or compromises of classified information. It does not commit governments to share classified information, and the existence of such an agreement with a particular country does not constitute authority to release classified material to that government. It does commit each government to protect the other's classified information if a decision is made to provide the information. It also satisfies, in part, the eligibility requirements of the AECA concerning the agreement of the recipient government to protect U.S. classified defense articles and technical data.

b. The Industrial Security Agreement is negotiated by the DoD as an annex to the GSA with those foreign governments with which DoD has entered into arrangements involving industry participation, such as the reciprocal procurement agreements. Other Federal Departments and Agencies also may be a party to this agreement. It includes provisions for information handling, security classification guidance, visits, and the exchange of security assurances, and it designates a responsible government agency to administer the agreement. Authority to negotiate the agreements and to negotiate amendments or approve exceptions to the provisions of these agreements rests with the Office of the Under Secretary of Defense (Policy). The Director, DSS, has been delegated authority to administer implementation of the provisions of this agreement.

I. SECURITY SURVEYS

1. The purpose of security surveys is to enable the NDPC to establish by on-site review whether a foreign government or international organization has the capability to protect CMI in a manner substantially the same as that protection provided to it by the United States as required by the AECA, E.O. 12958, as amended, and NSDM 119. They also permit the parties to exchange information on each other's programs to ensure proper implementation of the security agreements as well as cooperative agreements and sales contracts. The survey consists of a review of the government's security laws and regulations and discussions with responsible foreign officials, including foreign security personnel, concerning their procedures for protecting classified information. The views of U.S. Embassy personnel are also obtained. The level of

delegated disclosure authority for foreign governments is based, in part, on the results of these surveys.

2. The surveys concentrate on developing information on the foreign government security program (including the organizational, legal, and regulatory basis for the program) and procedures as well as any changes since the previous visit. The team evaluates the methods and procedures used by the government and industry in:

a. Personnel security, including clearance and investigations;

b. Information security, including all aspects of document and information control, the use of U.S. information, the flow of information from national level to user, and methods to protect the information and restrict access to properly cleared persons; and,

c. Physical security.

3. The security officials of the foreign country also conduct similar reviews of the U.S. security program.