



Department of the Navy

Foreign Disclosure Manual

September 2007

**DISTRIBUTION STATEMENT A: Approved
for public release; distribution is unlimited.**



DEPARTMENT OF THE NAVY
NAVY INTERNATIONAL PROGRAMS OFFICE
2521 S. CLARK STREET SUITE 800
ARLINGTON VA 22202-3928

NAVY FOREIGN DISCLOSURE MANUAL CHANGE TRANSMITTAL 1

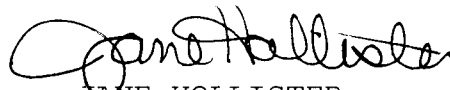
From: DIRECTOR, NAVY INTERNATIONAL PROGRAMS OFFICE

Subj: NAVY FOREIGN DISCLOSURE MANUAL

Encl: (1) Revised Page 55
(2) Revised Page 56
(3) Revised Page 57
(4) Revised Page 58
(5) Revised Page 59

1. Purpose. To transmit new pages 55-59 in response to request from NAVSEA 08 (Chief of Naval Operations, Director, Naval Nuclear Propulsion). Individual paragraphs with changes are marked with an asterisk.

2. Action. Remove pages 55, 56, 57, 58 and 59 of the basic manual and insert enclosures (1), (2), (3), (4) and (5) respectively.


JANE HOLLISTER
By Direction

NOTE: The references used in this manual are not necessarily listed in the order in which they are discussed. A complete list of all references cited can be found at the end of the manual.

PART I - CHAPTER 1
 BASIC DISCLOSURE POLICY, ORGANIZATION, AND RESPONSIBILITIES 5
 10101. Purpose..... 5
 10102. General..... 5
 10103. Applicable Laws, Executive Orders, and Policies 5
 10104. Government-to-Government Principle 10
 10105. Department of the Navy Foreign Disclosure Organization 10
 10106. Delegations of Disclosure Authority 10
 10107. Designated Disclosure Authority (DDA)..... 11
 10108. Foreign Disclosure Point of Contact (FDPOC) 11
 PART I – CHAPTER 2..... 12
 DISCLOSURE CRITERIA AND LIMITATIONS 12
 10201. General Disclosure Criteria..... 12
 10202. General Disclosure Limitations 13
 PART I – CHAPTER 3..... 15
 NDP-1 ANNEXES AND CATEGORIES OF INFORMATION 15
 10301. General..... 15
 10302. Categories of Information Defined 17
 PART I – CHAPTER 4..... 17
 DISCLOSURES TO INTERNATIONAL ORGANIZATIONS 17
 10401. General..... 17
 10402. International Organizations..... 17
 PART II - CHAPTER 1 19
 GENERAL PROCEDURES FOR THE DISCLOSURE OF CLASSIFIED MILITARY
 INFORMATION AND CONTROLLED UNCLASSIFIED INFORMATION..... 19
 20101. General..... 19
 20102. Policy 19
 20103. Procedures for Foreign Disclosure Decisions..... 20
 20104. Foreign Disclosure Decision Tools..... 25
 20105. Limitations on Disclosure Authority 25
 20106. Other Disclosure Considerations 29
 PART II CHAPTER 2 31
 TECHNOLOGY TRANSFER AND SECURITY ASSISTANCE REVIEW BOARD..... 31
 20201. General..... 31
 20202. Policy 31
 20203. Procedures..... 31
 PART II CHAPTER 3 33
 EXPORT LICENSES 33
 20301. General..... 33
 20302. Policy 33
 20303. Procedures..... 34
 20304. DoN ITAR Exemption Request Procedures 34
 PART II - CHAPTER 4 36
 INTERNATIONAL AGREEMENTS 36
 20401. General..... 36

NAVY FOREIGN DISCLOSURE MANUAL

20402. Policy 37

20403. Procedures..... 37

PART II – CHAPTER 5 39

FOREIGN MILITARY SALES (FMS) AND LEASES 39

20501. General..... 39

20502. Policy 39

20503. Procedures for FMS or Leases..... 39

PART II – CHAPTER 6 43

THE FOREIGN COMPARATIVE TESTING (FCT) PROGRAM 43

20601. General..... 43

20602. Policy 43

20603. Procedures..... 43

PART II – CHAPTER 7 45

TRANSFER OF U.S. NAVAL VESSELS TO FOREIGN GOVERNMENTS AND
INTERNATIONAL ORGANIZATIONS 45

20701. General..... 45

20702. Policy 45

20703. Procedures..... 45

PART II - CHAPTER 8 47

ONE-TIME AND RECURRING VISITS BY FOREIGN NATIONALS AND
REPRESENTATIVES OF FOREIGN GOVERNMENTS AND INTERNATIONAL
ORGANIZATIONS 47

20801. General..... 47

20802. Policy 47

20803. The Foreign Visit System (FVS) 48

20804. FVS Exemptions 49

20805. Disclosures by U.S. Government Personnel During Travel 51

20806. The FVS Request Process..... 51

20807. Special Visit Conditions 53

20808. Procedures for the Hosting Command..... 57

PART II - CHAPTER 9 60

EXTENDED VISITS AND ASSIGNMENTS OF FOREIGN NATIONALS AND
REPRESENTATIVES OF FOREIGN GOVERNMENTS AND INTERNATIONAL
ORGANIZATIONS 60

20901. General..... 60

20902. Policy 60

20903. Procedures..... 61

20904. Procedures For Foreign Liaison Officer (FLO)..... 62

20905. Procedures For Defense Personnel Exchange Program (DPEP) 63

20906. Cooperative Program Personnel 65

20907. Other Extended Visits 67

20908. Visits to Navy and Commercial Shipyards..... 67

20909. Visits to U.S. Government Facilities other than DoN 67

PART II – CHAPTER 10 68

DISCLOSURE TO FOREIGN NATIONALS IN NAVAL TRAINING..... 68

21001. General..... 68

21002. Policy	68
21003. Procedures for Classified Training Disclosure Reviews	69
21004. Other Training Disclosure Procedures.....	71
PART II - CHAPTER 11	73
DISCLOSURE OF DOCUMENTARY INFORMATION.....	73
21101. General.....	73
21102. Policy	73
21103. Procedures for Reviewing Documents.....	73
21104. Procedures for Staffing Documents.....	80
21105. Procedures for Sanitization of Documents	80
21106. Procedures for Document Transmittal.....	81
21107. Alternate Procedures for Disclosure of Documents to Foreign Governments ..	82
PART II - CHAPTER 12	85
DISCLOSURE OF FOREIGN GOVERNMENT INFORMATION	85
21201. General.....	85
21202. Policy	85
21203. Procedures.....	85
PART II - CHAPTER 13	87
DISCLOSURE OF RESTRICTED DATA AND FORMERLY RESTRICTED DATA (ATOMIC INFORMATION).....	87
21301. General.....	87
21302. Policy	87
21303. Procedures.....	87
21304. US/UK Polaris Sales Agreement and Polaris Trident H Technical Arrangement	89
21305. Unauthorized Disclosure.....	89
PART II - CHAPTER 14	89
PARTICIPATION BY FOREIGN CONTRACTORS IN DEPARTMENT OF THE NAVY PROCUREMENTS.....	90
21401. General.....	90
21402. Policy	90
21403. Procedures.....	91
PART II - CHAPTER 15	93
DISCLOSURE OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION TO U.S. COMPANIES UNDER FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI).....	93
21501. General.....	93
21502. Background.....	93
21503. Policy	94
PART II - CHAPTER 16	96
SECURITY POLICY AUTOMATION NETWORK (SPAN).....	96
21601. Purpose.....	96
21602. Policy	96
21603. Primary SPAN Components	96
21604. Reporting Procedures.....	97
21605. Output Records	98

NAVY FOREIGN DISCLOSURE MANUAL

GLOSSARY 99
MASTER REFERENCE LIST 107
INDEX 110

PART I - CHAPTER 1

BASIC DISCLOSURE POLICY, ORGANIZATION, AND RESPONSIBILITIES

- Ref:
- (a) SECNAVINST 5510.34A
 - (b) “National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations” (hereafter, “National Disclosure Policy” or “NDP-1”) (NOTAL)
 - (c) DoD Directive 5230.11
 - (d) DoD Directive 5230.20
 - (e) DoD Directive 4500.54
 - (f) Arms Export Control Act (22 U.S.C. 2751) (NOTAL)
 - (g) Export Administration Act (50 App. U.S.C. 2401 et seq.)
 - (h) DoD 5400.7-R
 - (i) SECNAVINST 5510.36
 - (j) SECNAVINST 5720.42F
 - (k) Public Law 98-94 (10 U.S.C. 130)
 - (l) DoD Directive 5230.24
 - (m) OPNAVINST 5510.161
 - (n) DoD 5105.38-M “Security Assistance Management Manual (SAMM)”
 - (o) DoD 5220.22-M National Industrial Security Operating Manual (NISPOM)
 - (p) SECNAVINST 4900.46B
 - (q) DOD Manual S-5230.28

10101. Purpose

This manual implements references (a), (b), (c), and (d). It provides Department of the Navy (DoN) foreign disclosure policy and procedures, delegates disclosure authority, and assigns responsibilities. It applies to DoN commands, agencies, staff elements, and other DoN organizations that are involved in activities that will result in contacts with, or the disclosure of, Classified Military Information (CMI) to foreign governments and international organizations, their representatives, and other foreign persons and entities pursuant to references (a), (b), (c), (d), and (e). In addition, this manual provides policy and assigns responsibilities for the foreign disclosure of Controlled Unclassified Information (CUI) that is determined, in accordance with reference (f), to require export controls as well as other unclassified information with a military or space application that is determined to be exempt from public disclosure pursuant to reference (g).

10102. General

Part I of this manual summarizes the basic laws, executive orders, and national and DoD policies that govern the disclosure of CMI and CUI to foreign governments or international organizations, or to persons who are sponsored by them, whether in the U.S. or abroad. Part I also describes the DoN foreign disclosure organizational structure, the process by which

disclosure authority is delegated within the DoN, and the responsibilities assigned to each disclosure authority. The specific DoN implementing procedures are in Part II of this manual.

10103. Applicable Laws, Executive Orders, and Policies

a. Arms Export Control Act (AECA) and Export Administration Act (EAA). The AECA, reference (f), governs the export of classified and unclassified defense articles and services and related technical data to foreign countries and international organizations. It is the principal statute that governs international commercial and government sales, co-production arrangements, loans, leases and grants of defense articles, as well as DoD participation in cooperative arms programs. The AECA is the legal basis for the security arrangements for most DoD international programs. It stipulates that recipient countries and international organizations that receive U.S. defense articles and services must agree to specified conditions on the retransfer, end-use, and protection of the articles and related technical data. The EAA, reference (g), governs the export of unclassified items and technical data that have civil application as well as those items and technical data that have both a civil and military application (“dual-use” items).

b. Executive Order (EO) 12958. EO 12958, which is implemented in the DoN by reference (h), establishes the U.S. National Security Information Program and governs the classification, declassification, downgrading, and safeguarding of classified national security information. The EO states that access to classified information must be in support of a lawful and authorized governmental purpose, and that the ability of a potential recipient to provide protection must be verified prior to a release of the information. The EO further specifies that classified information cannot be shared with a third party without the consent of the originator. In addition, U.S. Government departments and agencies are required to protect Foreign Government Information (FGI), classified or unclassified, that is provided in confidence (see Part II, Chapter 12).

c. National Disclosure Policy (NDP-1). NDP-1 (reference (b)) implements National Security Decision Memorandum 119 (NSDM-119). NSDM-119 establishes the basic U.S. policy for the disclosure of CMI to foreign governments and international organizations and assigns responsibility jointly to the Secretaries of State and Defense. The Secretaries of State and Defense are required, in coordination with the Secretary of Energy, the Director of Central Intelligence, and the heads of other departments and agencies, as appropriate, to establish procedures and an interagency mechanism to implement the national policy. The National Military Information Disclosure Policy Committee (hereafter, “National Disclosure Policy Committee” or “NDPC”) formulates foreign disclosure policy and procedures, and considers requests for exceptions to the policy. The NDPC is guided by the policy and procedures contained in NDP-1, which has been approved by the Secretaries of State and Energy, the Director of Central Intelligence, and issued by the Secretary of Defense. NDP-1 is a controlled document that will be issued only to Principal Designated Disclosure Authorities (PDAs) or Designated Disclosure Authorities (DDAs) and those DoN officials appointed as Foreign Disclosure Points of Contact (FDPOCs). Other DoN officials will receive disclosure guidance as described in section 10106, below. Only the Secretary of Defense (SECDEF), Deputy Secretary

of Defense (DEPSECDEF), and the chairperson of the NDPC are authorized to approve Exceptions to NDP-1 (ENDP). NDP-1 provides the following:

(1) Disclosure Criteria and Limitations. NDP-1 requires that specified criteria and limitations be satisfied in order to disclose CMI to representatives of foreign governments or international organizations. The criteria and limitations are described at Part I, Chapter 2.

(2) General Disclosure Limitations and Prohibited Disclosures. NDP-1 does not permit the disclosure of certain categories of classified information, the disclosure of which is governed by separate statutes, executive orders, or national policies. These limitations and prohibitions must be considered prior to initiating or responding to proposals involving the disclosure of CMI and CUI. The categories of information that are subject to disclosure limitations and prohibitions also are listed in Part I, Chapter 3.

(3) Categories of CMI and Delegation of Disclosure Authority Charts. Annex A to NDP-1 contains charts that identify eight categories of information that constitute CMI. The charts also delegate authority to NDPC member departments and agencies to disclose CMI for which they are the original classification authority, up to a specified classification level, by category, to countries and international organizations identified in the charts, subject to compliance with the disclosure policy, criteria, conditions, and any pertinent NDPC Policy Statements. If these policy, criteria, and conditions are not met, the proposed disclosure must be denied, or an exception to NDP-1 policy may be sought. The content of the charts is classified and may not be shared with any foreign person, entity, government or international organization. Annex A to NDP-1 is discussed in more detail in Part I, Chapter 3 (individual countries) and Part I, Chapter 4 (international organizations).

(4) NDPC Policy Statements. NDP-1 also contains NDPC Policy Statements (PSs) that provide special procedures to govern disclosures to certain countries or provide special procedures related to certain weapon systems, technologies, and other information. The PSs are described in Part I, Chapter 3.

(5) False Impressions. In accordance with reference (b), DoN organizations and their personnel must scrupulously avoid any action that creates a false impression that the U.S. is willing to enter into any arrangement with a foreign government that will involve the eventual disclosure of CMI or CUI. Therefore, before a DoN organization enters into an initiative with a foreign government that will entail the eventual disclosure of any CMI or CUI, the organization shall obtain disclosure authority sufficient to provide all of the information of the type and at the classification level that is known or anticipated for the life of the program or initiative.

(6) Reporting of Compromises. The U.S. Government is obligated by international agreements that are concluded pursuant to NDP-1 to report to the originating government the loss or compromise of classified FGI.

NOTE: The NDP-1 establishes the national policy and procedures and provides the mechanism for making decisions on the disclosure of any CMI that may be involved in those transactions. It

NAVY FOREIGN DISCLOSURE MANUAL

does not provide the authority to execute a sale or other transfer of articles, services, or technical data to a foreign government or international organization.

d. DoD Directive 5230.11. This directive (reference (c)) implements NDP-1 within the DoD. It delegates disclosure authority to the heads of certain DoD Components, including the Secretary of the Navy. It requires that each DoD Component with delegated disclosure authority appoint a Principal Disclosure Authority (PDA) to oversee the Component's foreign disclosure program. The Directive permits the DoD Components to re-delegate disclosure authority to subordinate commands, agencies, and staff elements as necessary to ensure efficient operations, provided that a Designated Disclosure Authority (DDA) is appointed at each such command, agency, or staff element to oversee foreign disclosure activities. The Directive requires the DoD components to report their decisions on disclosures of CMI by logging the decisions into the Security Policy Automation Network (SPAN) (see Part II, Chapter 16).

e. DoD Directive 5230.20. This directive, reference (d), establishes DoD policies and procedures for visits or assignments of foreign nationals to DoD Components and DoD cleared contractor facilities. It establishes the DoD International Visits Program (IVP), the DoD Foreign Liaison Officer (FLO) Program, the DoD Personnel Exchange Program (DPEP), and the conditions for the assignment of Cooperative Program Personnel (CPP). It requires the DoD Components to establish information access and physical procedures for controlling access by foreign nationals to classified information and programs. The DoN procedures are set forth in Part II, Chapter 8.

f. DoD Directive 4500.54. This directive (reference (e)) establishes DoD policies and procedures for temporary travel by DoD personnel overseas. It requires, among other things, that the DoD Components establish procedures to ensure that requests for travel authorization include a statement certifying that the appropriate disclosure authorization has been approved. If the traveler is to carry classified information, compliance with the required security procedures also must be certified.

g. The Freedom of Information Act (FOIA). The FOIA is implemented within DoD by reference (h) and in the DoN by reference (j). Generally, the U.S. public is entitled to have access to federal agency records, except when the information in the records is protected from public disclosure by one of nine exemptions. Pursuant to reference (h), information that is determined to be exempt from disclosure by a DoD Component normally is to be marked "For Official Use Only" or "FOUO" if it is not classified. Some information that is determined to be exempt from public disclosure will bear other markings, such as "Unclassified Controlled Nuclear Information," which also is marked "UCNI," and medical and personnel files, which are marked with privacy statements. Because unclassified information that qualifies under FOIA for withholding from public disclosure is of such sensitivity that it is not available to the U.S. public, it must undergo a review to determine if it may be authorized for release to foreign governments and international organizations and their representatives.

10104. Government-to-Government Principle

CMI can be disclosed or released (whether in oral, visual, or material form) as a government-to-government transfer and only to a person representing or sponsored by a foreign government or international organization in compliance with the policy described in reference (a). Planning and coordination (to include the recipient foreign government or international organization) for international transfers shall be initiated as soon as a foreign disclosure and export authorization are obtained. References (i) and (o) must be consulted for the proper transfer arrangements for classified information and material.

a. Government-to-Government Transfer. Classified information or material must be transferred through official government channels (e.g., U.S. Postal Service and military postal service registered mail, diplomatic pouch, Defense Transportation Service (DTS), Defense Courier Service (DCS) or other government courier, or through similar official channels arranged by the receiving foreign government or international organization), or through other arrangements (e.g., hand carry by designated courier or commercial transportation and a transportation plan for freight). The latter arrangements must be agreed upon in writing on a case-by-case basis for specific programs, and must provide for the secure transfer from the point of origin to the ultimate destination. Top Secret information, however, must always be transferred via official government channels (e.g., U.S. Government courier or U.S. Government approved secure communications systems). Reference (i) must be consulted for the proper transfer arrangements for classified information.

(1) Transfer Pursuant to a Government Sale. The transfer of classified articles or other classified material that result from a government sale shall be in compliance with references (i) and (n). The necessary security arrangements are made during the negotiation of the FMS agreement with the purchasing government. The DoN security office that supports the DoN FMS case executing agency is responsible under an FMS sale to ensure that all security requirements necessary for a government-to-government transfer are in place and are in compliance with references (i) and (n) prior to the materiel being released to the purchasing government's representative, unless specific written arrangements are included in the contract that instruct the U.S. contractor to initiate the transfer. The DoN security office supporting the DoN FMS case administering office is responsible for approval of transportation plans in those cases where the transfer is made by the DoN.

(2) Transfer Pursuant to a Commercial Sale. Transfers under commercial sales are the responsibility of the U.S. contractor and must conform with the International Traffic in Arms Regulation (ITAR) and the NISPOM (reference (o)).

b. Security Assurances and Receipts. The person to whom the information is provided must be specifically "sponsored" by his or her government. Sponsorship is usually provided in the form of a Security Assurance. Receipts must be obtained for all classified information transferred in documentary or material form in order to document the transfer of security jurisdiction to the intended foreign government or international organization. The security assurance, which normally is contained in a visit request or courier orders, is the recipient government's certification to the organization that the person is representing the foreign

government, is properly cleared, and the government will be responsible for protecting the information that is transferred. CMI will not be released to a foreign national in the absence of a Security Assurance.

10105. Department of the Navy Foreign Disclosure Organization

a. Navy Principal Disclosure Authority. The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) is designated as the PDA for the DoN. The Deputy Assistant Secretary of the Navy for International Programs (DASN(IP))/Director, Navy International Programs Office (Navy IPO) is designated by ASN (RD&A) to act as the PDA for the DoN. The PDA oversees compliance with SECNAVINST 5510.34A and this manual within the DoN and is the only DoN official other than the Secretary or Under Secretary of the Navy who is authorized to deal directly with the Secretary or Deputy Secretary of Defense regarding DoN requests for exceptions to NDP-1 policy or other foreign disclosure matters.

b. Navy IPO (Technology Security & Cooperative Programs) Responsibilities. The Director, Navy International Programs Office (Director, Technology Security & Cooperative Programs), hereafter known as Navy IPO-01, has been designated by reference (c) as the central authority for overseeing the foreign disclosure of CMI and CUI within the DoN. Navy IPO-01 is specifically directed to develop DoN implementing procedures for references (c) and (d) and to ensure compliance with the provisions of any treaty, agreement, statute, executive order or directive affecting the disclosure of CMI and CUI to foreign persons, entities, governments or international organizations. No command, agency, or staff office within the DoN will disclose, make commitments or enter into arrangements that will result in a requirement to disclose, or direct the disclosure of CMI or CUI except as set forth in Part II of this manual or as specifically authorized by Navy IPO-01. Navy IPO-01 represents the Secretary of the Navy on the NDPC.

c. Technology Transfer and Security Assistance Review Board (TTSARB). The TTSARB, established by reference (p), develops disclosure policies for the DoN on all precedent-setting or significant issues concerning technology transfer, security assistance, arms cooperation, and other international programs. TTSARB positions may require final approval as an ENDP. In such cases, Navy IPO-01 coordinates the DoN position on the matter and submits it for approval to the NDPC. Requests that are to be sent to the Secretary or Deputy Secretary of Defense are coordinated through Navy IPO-01 to the Secretary or Under Secretary of the Navy or Navy IPO.

10106. Delegations of Disclosure Authority

In the interest of meeting operational commitments and management efficiency, the SECNAV delegates disclosure authority to DoN commands, agencies, and staff elements.

a. General Delegations of Disclosure Authority (DDA). General delegations of disclosure authority to DoN commands, agencies, and staff elements are provided via official correspondence. The organization that has been given a general delegation of disclosure authority shall nominate a military or civil service official of suitable grade as the organization's DDA. Navy IPO approves the DDA nominations. DDAs may approve or deny disclosures of

CMI and CUI for which they are the originating authority or for which they have been delegated disclosure authority, in compliance with this manual. The DDA will perform the functions and meet the qualifications described in more detail in section 10107.

b. Delegation of Disclosure Authority Letters (DDLs). Navy IPO-01 and DDAs, as appropriate, will issue specific Delegation of Disclosure Authority Letters (DDLs) for individual programs that will detail the classification levels, categories, scope, and information limitations. DoN personnel who propose to enter into arrangements with a foreign government or international organization that will entail the disclosure of CMI or CUI, but do not have a DDL that permits disclosure, must seek disclosure authorization in writing, in advance of disclosure, from their DDA or Navy IPO-01, as applicable.

c. Other Disclosure Authorizations. Not all programs will have a DDL. A Letter of Offer and Acceptance (LOA) and a Foreign Visit System (FVS) visit authorization are also forms of disclosure authority. If the LOA, visit authorization, or other document is not specific about the exact elements of CMI or CUI authorized for disclosure, a DDL shall be prepared to describe the information.

10107. Designated Disclosure Authority (DDA)

The DDA has the authority and responsibility to control disclosures of CMI and CUI to foreign governments and international organizations and their representatives or persons sponsored by them. Navy IPO, on behalf of the PDA, will issue general delegations or DDLs to delegate disclosure authority to DDAs and to other DoN offices or officials for disclosures of CMI for specific programs, projects, or contracts that are not covered by the general delegations of disclosure that will be issued separately from this document.

10108. Foreign Disclosure Point of Contact (FDPOC)

The Commandant of the Marine Corps, Naval Component Commanders, Commanders of Systems Commands, and the Chief of Naval Research will each maintain dedicated FDPOCs within their headquarters and at subordinate commands and activities to coordinate foreign disclosure reviews and to facilitate a complete and timely response to foreign requests which represent the organizations consolidated position. The following offices of the Chief of Naval Operations (CNO) will each maintain a FDPOC: N2, N3/N5, N6/N7. Each FDPOC should have a basic working knowledge of foreign disclosure procedures. The FDPOCs will be DoN military or civil service employees. When the organization has a DDA, the FDPOC will coordinate disclosure requests with the DDA. If the organization is not required to have a DDA (i.e., no general delegation of disclosure has been issued by Navy IPO) the FDPOC will coordinate responses through his or her normal chain of command.

PART I – CHAPTER 2

DISCLOSURE CRITERIA AND LIMITATIONS

- Ref: (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (hereafter “National Disclosure Policy” or “NDP-1”) (NOTAL)
- (c) DoD Directive 5230.11
- (f) Arms Export Control Act (22 U.S.C. 2751) (NOTAL)
- (r) Atomic Energy Act of 1954, 42 U.S.C. 2011-2297 (NOTAL)
- (s) DoD Manual C-5230.23
- (v) NSTISSP No. 8
- (w) International Traffic in Arms Regulations (ITAR)

10201. General Disclosure Criteria

The proponents of a disclosure initiative must address, as a minimum, the factors described below when submitting an issue for disclosure review. The results of the Designated Disclosure Authority’s (DDA) analysis, together with an analysis of the risks of compromise described in the subsequent criteria, will be used to determine the type and level of information or technology that may be authorized in order to satisfy the U.S. requirement for the initiative. Disclosures in categories 1 through 7 of the Charts located in Annex A to NDP-1, will be made only when all of the following criteria are satisfied per reference (c):

a. Disclosure is consistent with U.S. foreign policy and national security objectives concerning the recipient foreign government or international organization. For example:

(1) The recipient cooperates with the U.S. in pursuance of military and political objectives, which are compatible with those of the U.S.

(2) A specific national purpose, diplomatic or military, will be served.

(3) The information will be used in support of mutual defense and security objectives.

(4) The disclosure of CMI considers the regional implications of the initiative. For example, in certain regions, the U.S. must consider the possible political consequences of providing a system or capability to a particular country relative to the other countries in that region.

b. Disclosure is consistent with U.S. military and security objectives. For example:

(1) Disclosures of advanced technology, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology regardless of the intended recipient.

(2) The proposed disclosure reflects the need for striking a proper balance between pursuit of our mutual defense and foreign policy objectives on the one hand and the preservation of the security of our military secrets on the other.

c. Disclosures will result in a clearly defined benefit to the U.S., for example:

(1) The U.S. obtains information from the recipient nation on a quid pro quo basis.

(2) The exchange of military information or participation in a cooperative project will be advantageous to the U.S. from a technical or other military viewpoint.

(3) The development or maintenance of a high level of military strength and effectiveness on the part of the government receiving the information will be advantageous to the U.S.

d. The disclosure is limited to information necessary to the purpose for which disclosure is made.

e. The recipient government must have the capability and intent to protect classified information. Paragraph 10301, subparagraph b provides additional information on assessing this capability. If capability and intent have not been established, approval of the initiative normally cannot be given until they are established.

10202. General Disclosure Limitations. Disclosures of the following types of information will not be authorized by DoN DDAs, except as specified below:

a. Classified or unclassified information, the disclosure of which is governed by federal legislation or by an international agreement to which the U.S. is a party, will not be authorized, except in compliance with the pertinent legislation or agreement.

b. Low Observable/Counter Low Observable (LO/CLO) information or technology, except as approved through the LO/CLO EXCOM process, as specified in reference (p).

c. Naval Nuclear Propulsion Information (NNPI), except under an agreement negotiated pursuant to reference (r) as required by reference (c).

d. Classified or unclassified proprietary information, the intellectual property rights to which are owned or controlled by private firms or citizens (i.e., patents, copyrights, or trade secrets) will not be authorized, except with the owner's consent, unless such disclosure is authorized by relevant legislation, and then release will be subject to that legislation.

e. Classified Military Information (CMI) or Controlled Unclassified Information (CUI) officially obtained from a foreign source or other Foreign Government Information (FGI) will not be authorized, except when the information has been conveyed by the source with the expressed consent to its disclosure further.

NAVY FOREIGN DISCLOSURE MANUAL

f. Combined military information without prior agreement of all applicable countries will not be authorized.

g. Joint information without prior agreement of all departments or agencies having control or jurisdiction will not be authorized.

h. Information about strategic war plans, contingency plans, or related plans, and concepts will not be authorized without prior coordination with the Chairman, Joint Chiefs of Staff (CJCS) and approval by the SECDEF or DEPSECDEF.

i. Information originated by or for any other department or agency will not be authorized without its consent.

j. Atomic information (RD/FRD) will not be authorized except pursuant to reference (b) (See Part II, Chapter 13).

k. Category 8 (Military Intelligence) information, unless the DDA has been delegated disclosure authority covering the disclosure of intelligence information or has received approval in advance from the originating intelligence agency.

l. Communications Security (COMSEC) information will not be authorized unless authorized by the Committee on National Security Systems (CNSS) in accordance with reference (e).

m. Information that could give assistance to any foreign nation's ability to develop or acquire an independent ballistic missile delivery capability will not be authorized unless approved in compliance with the Missile Technical Control Regime (MTCR) in reference (f) via Navy IPO-01.

n. Information relating to the control of compromising emanations (TEMPEST) will not be authorized unless recommended by the Director, Naval Criminal Investigative Service (NCIS) and approved by Navy IPO-01.

o. Generally, bibliographies and reference lists containing listings of classified publications will not be authorized, unless it is determined that all listed publications are authorized for disclosure or the lists are sanitized to delete publications that cannot be authorized for disclosure.

PART I – CHAPTER 3**NDP-1 ANNEXES AND CATEGORIES OF INFORMATION**

- Ref: (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (Hereafter, “National Disclosure Policy” or “NDP-1”) (NOTAL)
(c) DOD Directive 5230.11

10301. General

There are three annexes to NDP-1 (see reference (b)). These annexes provide important policies and guidelines that must be factored into each foreign disclosure decision. Therefore, Department of the Navy disclosure authorities must understand the content and use of the annexes.

a. Annex A, Part A sets forth the maximum level of disclosure authority delegated by the NDPC to the military departments for each country and category of information. Annex A, Part A, is generally referred to as the “Country Charts.” The delegations of authority in the charts are made to the heads of the departments and agencies that are represented on the NDPC, who do not routinely delegate the same level of disclosure authority to subordinate commands and agencies. Within the DoN, delegations of authority are limited by the pertinent DDL.

b. Annex A, Part B provides data related to specific countries, such as the date the U.S. Government concluded a General Security of Military Information Agreement (GSOMIA) or General Security of Information Agreement (GSOIA); the date an Industrial Security Agreement (ISA) was concluded; the last date a NDPC Security Survey was completed; and the last date a CIA Risk Assessment was made. The existence of a GSOMIA, GSOIA, ISA, security assessments, and NDPC Security Survey normally satisfy the Arms Export Control Act and NDP-1 requirements with respect to establishing a potential recipient government’s capability and intent to protect CMI that is to be provided to that government. In some situations, additional security commitments on the part of the recipient government may be necessary, and may be incorporated in a special program agreement or Letter of Offer and Acceptance (LOA).

c. Annex B contains Policy Statements (PSs) specific to certain foreign governments. These statements provide special disclosure manuals and guidelines for specified foreign governments. These statements may supplement or clarify the delegations of disclosure authority in Annex A. Designated Disclosure Authorities (DDAs) must consult these statements before a decision is made on a proposed disclosure.

d. Annex C contains PSs for weapon systems, technologies, and other information. These statements provide special disclosure manuals and procedures similar to those for countries. The statements also may modify and supplement the delegations of authority in Annex A, and must be consulted prior to a disclosure decision being made.

10302. Categories of Information Defined

The NDPC has divided military information into eight categories. The following abbreviated definitions are found in reference (c).

a. Category 1 - Organization, Training, and Employment of Military Forces. Information of a general nature pertaining to tactics, techniques, tactical doctrine, and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for the operation, training, and maintenance on specific equipment covered under Categories 2 and 3, below.

b. Category 2 - Military Materiel and Munitions. Information on specific items of equipment already in production, or in service, and the information necessary for the operation, maintenance, and training. Items on the U.S. Munitions List fall within this category. This category does not pertain to equipment that is in research and development.

c. Category 3 - Applied Research and Development Information and Materiel. Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.

d. Category 4 - Production Information. Information related to designs, specifications, manufacturing techniques, and such related information necessary to manufacture materiel and munitions.

e. Category 5 - Combined Military Operations, Planning, and Readiness. Information necessary to plan, ensure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. It does not include strategic plans and guidance or North American defense information.

f. Category 6 - U.S. Order of Battle. Information pertaining to U.S. forces in a specific area. In general, disclosures of this information are limited to those countries in which U.S. forces are stationed or are in adjacent geographical areas.

g. Category 7 - North American Defense. Information related to plans, operations, programs, and projects, to include data and equipment, directly related to North American defense.

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 Director of Central Intelligence (DCI).

PART I – CHAPTER 4**DISCLOSURES TO INTERNATIONAL ORGANIZATIONS**

Ref: (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (Hereafter “National Disclosure Policy” or NDP-1”) (NOTAL)

10401. General

a. Per reference (b), when the information is disclosed to an organization, the organization, as a legal entity, is held accountable to the U.S. for the control and protection of the information. Similarly, if the information is approved for export or disclosure to an individual country that is a member of an organization, that individual country is held accountable for control and protection. The approval of the disclosure to a country in an international organization does not constitute approval to export or disclose the information to the other nations that are members of the organization, or to the organization.

b. While Classified Military Information (CMI) may be authorized for export or disclosure to an international organization at a particular classification level, an exception to policy would be required for the export or disclosure of the same information to each individual member country. This principle is reflected in the delegation of disclosure authority charts for the international organizations in Annex A to NDP-1.

c. Care must be exercised when considering disclosures to an international organization. Generally, once the information has been provided to an international organization, the organization will determine the need-to-know for further access within the organization. Therefore, particular attention must be given to the countries that comprise the organization’s membership before making a decision to disclose. However, there may be circumstances when the advantages from the disclosure may outweigh the risks associated with sharing the information with one or more of the member countries (e.g., participation in coalition operations). Consideration also should be given to establishing a “closed program” (which is provided for in NATO policy), specifically when it is intended that the information is to be shared with only certain specified member nations of the organization who are participating in the program.

d. The process for making disclosure decisions with respect to international organizations is otherwise the same as the process for making disclosure decisions for the individual countries listed in Annex A to NDP-1.

10402. International Organizations

The NDP-1 currently recognizes and authorizes classified disclosure to only one international organization: the North Atlantic Treaty Organization (NATO) including its subordinate commands (e.g., SHAPE, NAMSA). Authority for the disclosure of CMI to any international organization other than NATO must be processed as a request for exception to

NAVY FOREIGN DISCLOSURE MANUAL

NDP-1. NATO is comprised of the following countries: U.S., Belgium, Bulgaria, Canada, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, and the United Kingdom. Please note that the NATO country list may change periodically.

PART II - CHAPTER 1

GENERAL PROCEDURES FOR THE DISCLOSURE OF CLASSIFIED MILITARY INFORMATION AND CONTROLLED UNCLASSIFIED INFORMATION

- Ref:
- (a) SECNAVINST 5510.34A
 - (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (hereafter, “National Disclosure Policy” or “NDP-1”)
 - (c) DoD Directive 5230.11
 - (d) DoD Directive 5230.20
 - (f) Arms Export Control Act (AECA)
 - (g) Export Administration Act (EAA) (50 App. U.S.C. 2401 et seq.)
 - (i) SECNAVINST 5510.36
 - (j) SECNAVINST 5720.42F
 - (s) DoD Directive 5230.23
 - (m) OPNAVINST 5510.161
 - (o) DoD 5220.22-M
 - (q) DoD Directive S5230.28
 - (r) Atomic Energy Act
 - (t) Guide for Foreign Attaches Accredited to the Department of the Navy (NOTAL)
 - (u) SECNAVINST 5510.30A
 - (w) International Traffic in Arms Regulation (ITAR)
 - (x) Export Administration Regulations (EAR) (15 CFR 730-799) of 30 Jul 04

20101. General

This chapter and subsequent chapters of Part II provide mandatory procedures for the disclosure of Classified Military Information (CMI) and Controlled Unclassified Information (CUI) to foreign governments and international organizations (i.e., “foreign disclosure”) and implement references (a), (c), (d), (i), (j), and (m). The export of CMI or CUI related to defense articles or services and related technical data controlled by the Arms Export Control Act (AECA), and which are defined as such in its implementing regulation, the International Traffic in Arms Regulations (ITAR), as well as dual-use items that are controlled by the Export Administration Act (EAA) and the Export Administration Regulations (EAR), is subject to these policies and procedures. These policies and procedures apply to foreign disclosures by DoN personnel in the U.S. and abroad.

20102. Policy

a. Foreign Disclosure Decisions. CMI and CUI under DoN control may be disclosed to foreign representatives only when a DoN official who has been specifically delegated disclosure authority determines

(1) that the disclosure is in support of a lawful U.S. Government purpose (e.g., foreign military sales, direct commercial sales, cooperative program, personnel exchange program),

(2) disclosure is in compliance with NDP-1, and

(3) disclosure is in compliance with the procedures established in the Manual.

b. Government-to-Government Principle. As discussed in paragraph 10104, classified information and material will be transferred by government officials through official government channels and only to a person specifically designated in writing by the foreign government as its designated government representative for that purpose.

c. False Impressions Doctrine. As discussed in paragraph 10103(c) subparagraph (5), DoN organizations and their personnel will scrupulously avoid any action that creates a false impression that the United States is willing to enter into any arrangement with a foreign government that will involve the eventual disclosure of CMI or CUI.

20103. Procedures for Foreign Disclosure Decisions

There are certain requirements that must be met by DoN Designated Disclosure Authorities (DDAs) when making all foreign disclosure decisions. In order to meet the requirements, DDAs shall follow the steps described below in making foreign disclosure decisions.

a. Origin of the Request. Requests involving the possible foreign disclosure of CMI and CUI in the possession of the DoN may originate from official or unofficial sources. An official source may be a proponent from within the DoD, from another U.S. Government department or agency, or from a foreign government or international organization. A request from a foreign government may be made through its embassy in the U.S., or through a U.S. representative assigned for duty to a foreign country or organization. Foreign embassies are provided guidelines, in reference (t), on the proper procedures to follow for requesting information from the DoN, as well as on the clearance of foreign visitors and exchange under personnel exchange programs. Only requests that are received through official channels shall be processed for a foreign disclosure decision. Requests for CMI or CUI from foreign sources that are not received through official channels should be returned to the requestor with the explanation that the requested information is controlled information, and that it therefore cannot be provided outside official, government-to-government channels.

b. Originator or Controlling Authority. DoN disclosure authorities shall disclose only DoN CMI and CUI. The DoN does not have the authority to disclose information that has been originated by or is under the control of another DoD or U.S. Government department or agency, or a foreign government or international organization. The originator is the entity that has original classification authority for CMI; for CUI, it is the entity that controls the information. The controlling office is the office that has assumed responsibility for the information when the originator has been disestablished or which has otherwise been assigned responsibility for the information. The identity of the originator or controlling office usually appears on the document that contains the information. If a request or proposal would involve the disclosure of CMI or CUI that is originated or controlled by another department or agency or by a foreign government

or international organization, or information that is listed in Part I, Chapter 2, and the DoN recipient of the request or the DoN proponent for the proposal believes that a favorable disclosure decision is warranted, the request or proposal shall be forwarded to Navy IPO-01, together with the justification for the proposed disclosure decision (see subparagraph d., below). Further guidance on the disclosure of Foreign Government Information (FGI) is at Chapter 12 of this Part. Navy IPO-01 shall coordinate the request with the points of contact listed below, as applicable. Additionally, Part I, Chapter 2, paragraph 10202 of this Manual lists types of information for which special disclosure authorization must be obtained.

(1) CMI under the Jurisdiction of the Military Departments and other DoD Components shall be coordinated with the responsible office as follows:

Office of the Deputy Chief of Staff of the Army, Intelligence
 ATTN: DAMI-CDD
 1000 Army Pentagon
 Washington, DC 20310-1000

Air Force Disclosure Directorate (SAF/IAPD)
 1010 Air Force Pentagon
 Washington, DC 20330-1010

Defense Intelligence Agency (For other DoD Components)
 Attn: Pentagon, DXD-2
 Building 6000
 Washington, DC 20340-5100

(2) Intelligence Information. Proposed disclosures of intelligence information, including that described in Part I, Chapter 2, shall be coordinated with the following offices of the Office of Naval Intelligence or the Commandant of the Marine Corps, as applicable:

Office of Naval Intelligence
 Attn: ONI-333
 4251 Suitland Road
 Washington, DC 20395-5720

Commandant of the Marine Corps
 Attn: HQMC (I)
 2 Navy Annex
 Washington, DC 20380-177547

c. Classification Level of the Information. DDAs may disclose classified information up to and including the levels that have been delegated to the DoN in Annex A to NDP-1 (See Part I, Chapter 1, subparagraph 10103.c. (3) and Chapter 3), and subject to applicable Policy Statements in Annexes B and C of NDP-1, provided all other requirements described in this Chapter are satisfied. DoN disclosure authorities shall carefully examine a request or proposal involving the disclosure of CMI to determine the security classification of all of the information

NAVY FOREIGN DISCLOSURE MANUAL

that would have to be disclosed to satisfy the request or proposal. In considering the sale of a weapon system, for example, the decision will include the classification of the hardware and all information that will be needed for operation, training, and maintenance. If any of the information ultimately required to satisfy the request or proposal exceeds the levels delegated to the DoN in NDP-1, the request or proposal shall be denied, or an Exception to the National Disclosure Policy (ENDP) may be requested (see subparagraph h., below).

d. Justification. CMI and CUI will be provided to a foreign government or international organization or their representatives only when the disclosure can be justified as supporting a lawful and authorized U.S. Government purpose. Examples of such purposes are commercial or government sales pursuant to the AECA, a cooperative arms program, or an Information Exchange Agreement (IEA) Annex. The decision on whether a disclosure is justified shall conform to the requirements set forth in references (a) and (b) and this Manual.

(1) CMI. If CMI is to be disclosed, the DDA shall ensure that the disclosure decision will satisfy all of the disclosure criteria discussed in Part I, Chapter 2. If any one of the criteria cannot be satisfied, the request or proposal shall be denied, or an ENDP may be requested, see subparagraph h., below and refer to Navy IPO-01 with a recommendation.

(2) CUI. If the request or proposal will involve the disclosure of CUI, the DDA shall ensure that the disclosure of the information supports an authorized U.S. Government purpose. Moreover, it must be determined that disclosure would not be detrimental to DoD or U.S. Government interests that are protected by the access or control markings on the information. Because DoD organizations often fail to mark CUI at the time it is generated, all official information not cleared for public release must be reviewed to verify whether it is releasable to a foreign government or international organization. (Note: DoN personnel should be aware that specific statutes protect a significant amount of CUI (see Part I, Chapter 1, subparagraph 10103.g.), and violation may result in administrative or criminal sanctions.)

e. Disclosure Authority. Only DDAs may authorize or deny the foreign disclosure of CMI and CUI. The DDAs shall make the disclosure decision within the scope of their delegated disclosure authority (See paragraph 10106). In addition, Annexes B and C of NDP-1 (reference (b)) contain disclosure Policy Statements (PSs) on specified countries, systems and technologies that modify the scope of disclosure authority delegated to the DoN and other departments and agencies. If a response to the request or proposal is beyond the scope of authority delegated to the DoN recipient of the request or proposal, and such recipient believes that the request should be considered, the request will be forwarded to the next DDA who has the requisite delegated disclosure authority in the chain of command. If the decision is beyond the scope of authority of all DDAs in the chain of command, the request or proposal will be forwarded, with justification, to Navy IPO-01 for action.

f. Special Access Programs (SAP) and Sensitive Compartmented Information (SCI). In most cases, DDAs shall only authorize the disclosure of collateral U.S. CMI and/or CUI. They generally will not provide authorization for the disclosure of Special Access Programs (SAP) or sensitive compartmented information (SCI), equipment, or systems without obtaining written disclosure approval from the office or agency with disclosure cognizance over such items.

Foreign national special access security clearances passed through Special Security Office (SSO) channels do not, by themselves, constitute disclosure authorizations for SAP or SCI, equipment, or systems.

g. False Impressions. When a response is to be provided to a foreign government or international organization or its representative (including its contractors), the DoN official providing the response shall ensure that the response does not make false impressions.

h. Requests to be Submitted to Navy IPO-01. Requests that are submitted to Navy IPO-01 for a foreign disclosure decision, including requests for an ENDP that must be submitted to the National Disclosure Policy Committee (NDPC), requests that must be coordinated with another U.S. Government department or agency, and requests to be forwarded to a foreign government or international organization, shall be fully justified. The justification shall identify the program, project, or contract involved, identify the information to be provided, and describe how all of the disclosure criteria at Part I, Chapter 2, paragraph 10201 will be met.

i. Response Time for Foreign Disclosure Decisions. Proposals initiated by DoN organizations and requests received from foreign governments and/or international organizations which must be forwarded to another DDA or to Navy IPO-01 for a decision must allow sufficient time for processing and coordination prior to the desired disclosure date. Thirty calendar days lead-time is normally required to obtain a decision on a matter that is within the disclosure authority of the DoN. However, if the request or proposal requires a TTSARB decision, an exception to NDP-1, a decision by another U.S. Government department or agency, coordination with a foreign government or international organization, or a decision by another Military Department or the Joint Staff, one should allow 90-180 days or longer, depending upon the complexity of the issues involved.

j. Disclosures and Releases of CMI to Representatives of a Foreign Government or International Organization. The following requirements shall be met for all disclosures or releases of CMI in oral, visual, or material form. Failure to comply with these requirements may result in invalidation of the applicable security agreement and ultimate compromise of the information.

(1) Government-to-Government Transfer. CMI shall be disclosed or released as a government-to-government transfer and only to a person representing or sponsored by a foreign government or international organization in compliance with the policy described in reference (a) and paragraph 10104 of this Manual.

(2) Security Assurance and Receipts. After a decision is made to transfer CMI to a foreign government or international organization, reference (b) specifies that the proposed recipient government or organization must provide all of the following assurances before the disclosure or release can occur:

(a) The information will not be revealed to a third party without U.S. Government consent.

NAVY FOREIGN DISCLOSURE MANUAL

(b) The recipient government or organization will afford the information substantially the same degree of protection.

(c) The information will be used for only the purpose for which it was provided.

(d) Any known or suspected compromise of the information will be reported.

(e) All individuals and facilities that will have access to the classified military information will have security clearances granted by their government at a level equal to that of the classified information involved and an official need to know.

(f) Transfers will occur as a government-to-government transfer.

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

(h) The recipient government or organization will abide by or meet any U.S. specified conditions for the release of the information or material.

These assurances normally will be satisfied by a General Security Agreement (also referred to as General Security of Information Agreement or General Security of Military Information Agreement) between the U.S. and the other country or the organization. Annex A to NDP-1 lists the countries with which the U.S. has a General Security Agreement. All NATO countries have signed the NATO Security Agreement. In the absence of a security agreement, the required assurances shall be included and agreed to in a program specific agreement, in a Letter of Offer and Acceptance, exchange of diplomatic notes, visit clearance requests, courier orders, or transportation plans.

The DoN official who discloses or releases the information shall verify that the person who is to receive the information or material has been authorized by his or her government, or by the international organization, to receive the information or material and assume custody on behalf of the government or organization. Receipts shall be obtained for all CMI in order to document the transfer of security jurisdiction. (Note: A foreign government or international organization may waive this requirement for release of its own Restricted information.)

k. Disclosures to Foreign Nationals Employed by the DoN and DoN Contractors. Although non-U.S. citizens are not eligible for a U.S. security clearance, access to classified information may be justified for compelling reasons in furtherance of the DoD mission. A Limited Access Authorization (LAA) may be justified in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed and for which a cleared or clearable U.S. citizen is not available. CNO N09N2 will review and coordinate proposed LAAs with the applicable DDA (typically the cognizant SYSCOM or Navy IPO). References (o) and (u) provide guidance which include, but are not limited to, the following disclosure/access considerations:

(1) Access will be limited to classified information relating to a specific program or project.

(2) Appropriate foreign disclosure authority determines that access to classified information must be consistent with release policy to the individual's country of origin.

(3) Physical custody of classified material will not be authorized.

(4) Personnel granted LAA's will not be permitted uncontrolled access to areas where classified information is stored or discussed. Classified information will be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

(5) LAAs are not valid for access to NATO information (with certain exceptions), TOP SECRET, Restricted Data/Formerly Restricted Data (Atomic Energy Act RD/FRD), Communications Security (COMSEC) and intelligence information.

20104. Foreign Disclosure Decision Tools

This section covers the most common decision tools that can be used to facilitate foreign disclosure determinations and defines how they are used in the disclosure decision-making process. DDAs shall use these tools when they make foreign disclosure decisions. Access to the tools can be arranged through Navy IPO-01.

a. Technology Transfer and Security Assistance Review Board (TTSARB) Decisions. The purpose of the TTSARB, co-chaired by the Vice Chief of Naval Operations (VCNO)/Assistant Commandant of the Marine Corps (ACMC) and the Assistant Secretary of Navy (Research, Development and Acquisition) (ASN (RD&A)), is to promote centralized policy development, ensure that all precedent-setting or significant issues concerning technology transfer, disclosure, security assistance, and other international programs are reviewed by all concerned DoN officials, and ensure that decisions represent a coordinated DoN position. TTSARB Decisions establish a DoN policy position for the disclosure of information and the release of specific major defense articles developed by or under the cognizance of the DoN. Because they may represent DoN positions only, they often contain caveats warning that an ENDP or other coordination is necessary before a program is initiated or any disclosure is made. They also provide specific manuals to DoN personnel regarding information and systems that can and cannot be shared with foreign governments and international organizations. Each TTSARB Decision usually contains an extensive set of General Terms and Conditions, as an enclosure. DoN DDAs shall become familiar with TTSARB Decisions that pertain to their organizations and programs.

b. Delegation of Disclosure Authority Letters (DDLs). DDLs provide detailed disclosure guidance for programs or projects within its scope. Each DDL will describe the NDP-1 category(ies) of information, the classification level, and scope of information that may be authorized for release, as well as specific security procedures to be followed in transferring

the information. The DDLs may be prepared by Navy IPO-01, by other DoN organizations for approval by Navy IPO-01, or by DoN DDAs for programs and information over which they exercise foreign disclosure jurisdiction. DDLs issued to specified DoN officials must be signed by a DDA who already holds adequate disclosure authority for the DoN information. Normally this DDA is Navy IPO-01.

c. Foreign Disclosure Databases. Many foreign disclosure decisions can be related to precedents that are established by prior decisions. There are several SIPRNET sources that are available to research policies and precedents. Using these sources can often serve to expedite and assure the accuracy of foreign disclosure decisions. DDAs shall refer to these databases before making or recommending foreign disclosure decisions.

(1) DoD Security Policy Automation Network (SPAN) databases. These databases include, (i) the Technology Protection System (TPS) containing decisions on export license applications, (ii) decisions on foreign visitors, exchange personnel, and foreign liaison officers contained in the Foreign Visit System (FVS), (iii) the Foreign Disclosure System which records decisions by the DoD Components on the disclosure of classified documents and training material, and (iv) the National Disclosure Policy System (NDPS), which contains Records of Action (RAs) on requests for ENDP. See Part II, Chapter 16.

(2) DoN Disclosure Database (DND2). This database, which contains ENDP and TTSARB Decisions, is available through Navy IPO Disclosure Portal on the Navy IPO classified website at www.nipo.navy.smil.mil/disclosure.

(3) Navy Tactical Publications Disclosure Database (NTPDD). This database, which contains disclosure decision precedents on Naval Warfare Publications (see Part II, Chapter 11), is available through the Navy IPO Disclosure Portal on the Navy IPO classified website.

20105. Limitations on Disclosure Authority

Certain types of CMI and CUI are not subject to the exclusive disclosure authority of either DoN or DoD. Special approvals and exceptions must be obtained from or through Navy IPO-01 as indicated below. These include, but are not limited to Low Observable (LO) and Counter Low Observable (CLO) information or technology, National Intelligence, Sensitive Compartmented Information (SCI), acoustic intelligence (ACINT), information controlled by the Committee on National Security Systems (Communications Security and INFOSEC information), threat parametric data, Global Positioning System (GPS) information, information related to offensive counterintelligence operations, narcotics intelligence, Strategic War Plans, foreign government information, and any information originated by a department or agency other than the DoN. DoN organizations shall comply with the procedures contained in the Manual when obtaining disclosure authorization for these and other types of information. In addition, Annex C of reference (b) sets forth specific disclosure policy guidance related to selected U.S. weapon systems, equipment, and technologies which in some cases require coordination with certain non-DoN organizations.

a. Classified or unclassified information, the disclosure of which is governed by law or by an international agreement to which the U.S. is a party, will not be authorized, except in compliance with the pertinent legislation or agreement. The supporting DoN legal advisor should be consulted with respect to disclosures affected by this prohibition.

b. Any aspect of U.S. foreign disclosure policy regarding any country, including the recipient's foreign country or international organization.

c. Classified Category 4 (Production) information, as defined in Part I, Chapter 3, unless an ENDP has been granted to specifically permit such disclosure. Category 4 information includes computer source code. See definition of NDP-1 Categories of Information in Part I, Chapter 3. See guidance contained in Part I, Chapter 1 regarding ENDP requests.

d. Any information related to Low Observable/Counter Low Observable (LO/CLO) technology developed in whole or part by DoD with information or knowledge obtained from or developed for DoD/DoN. Foreign disclosure of LO/CLO technologies, information, and systems shall be restricted consistent with LO/CLO Executive Committee (EXCOM) guidance, applicable NDPC Policy Statements, and reference (q). Disclosures involving LO/CLO technologies, including marketing, shall be coordinated through Navy IPO-01, the Chief of Naval Operations Director of LO/CLO Technology (N091D), and the Office of the Under Secretary of Defense, Acquisition, Technology, and Logistics (OUSD(AT&L)), Director of Special Programs (DSP), and approved through the LO/CLO EXCOM process.

e. Naval Nuclear Propulsion Information (NNPI), classified or unclassified will not be authorized, except when pursuant to the Atomic Energy Act (reference (r)). Moreover, disclosures will not be made that might be construed to affect or modify official policies and procedures for restricting visits by foreign nationals to the propulsion spaces of U.S. nuclear-powered naval vessels. (The "Policy on U.S. Government or Private Assistance in Regard to Foreign Nuclear Propelled Vessels" of February 4, 1965 forbids disclosure of classified or unclassified NNPI to foreign nationals, except under a specific government-to-government agreement for cooperation in the field of naval nuclear propulsion, executed under Section 123(d) of reference (r)).

f. Information subject to intellectual property rights (e.g., patent, copyright, trade secret) that prohibit the U.S. Government from transferring the information to a foreign recipient will not be authorized without the consent of the holder of those rights.

g. Classified Military Information (CMI) or Controlled Unclassified Information (CUI) officially obtained from a foreign source will not be authorized, except when the information has been conveyed by the source with expressed consent to its further disclosure.

h. Combined military information will not be authorized without prior agreement of all applicable countries.

i. Information originated by or for any other department or agency will not be authorized without the consent of the appropriate DDA.

NAVY FOREIGN DISCLOSURE MANUAL

j. Joint information will not be authorized without prior agreement of the DDAs of all departments or agencies having control or jurisdiction.

k. Information that reveals operational capabilities, limitations, or vulnerabilities of U.S. armed forces, ships, aircraft, weapons, and sensors, upon which countermeasures or counter-countermeasures could be developed by a potential adversary.

l. Information about strategic war plans, contingency plans, or related plans and concepts will not be authorized without prior coordination with the Joint Chiefs of Staff and approval by the Secretary or Deputy Secretary of Defense.

m. Restricted Data or Formerly Restricted Data (RD/FRD), as defined by the Atomic Energy Act of 1954, or performance capabilities of U.S. nuclear submarines that could be used to extrapolate RD/FRD. See Part II, Chapter 13 for additional guidance.

n. Category 8 (Military Intelligence) information, unless the DDA has been delegated disclosure authority covering the disclosure of intelligence information or has received approval in advance from the originating intelligence agency. See definition of NDP-1 Categories of Information in Part I, Chapter 3. Intelligence information will not be authorized except as provided in Section II of reference (b) and reference (s). When it is not clear which department or agency has primary cognizance, requests should be addressed to Office of Naval Intelligence (Foreign Disclosure Office), hereafter known as ONI-333, for coordination with the appropriate organization.

o. National Intelligence; i.e., intelligence produced within the National Foreign Intelligence Board (NFIB) structure will not be authorized, unless approved by the NFIB. Requests will be addressed to ONI-333.

p. Communications Intelligence (COMINT) which is under the cognizance of NSA or communication systems which have unique capabilities and were specifically developed to collect COMINT, Electronics Intelligence (ELINT), or Signal Intelligence (SIGINT) information will not be authorized unless authorized by the Director, NSA via CNO (N2). Weapon systems requiring threat parametric data shall be authorized for release only if threat parametric data has been authorized for release by DIA, NSA, the Services and the SIGINT Committee. Navy IPO will liaison with aforementioned organizations to obtain approval.

q. Counterintelligence information, as defined in Appendix A, will not be authorized unless coordinated with the Director, Naval Criminal Investigative Service (NCIS).

r. Sensitive Compartmented Intelligence (SCI) will not be authorized unless authorized by ONI-333. ONI will coordinate requests for SCI with the appropriate department or agency having primary cognizance over the information.

s. Intelligence information concerning activities of certain foreign governments described in subparagraph 5.c. (2) of section I, and subparagraph 5.b. (7) of section II, of NDP-1 (reference (b)) will not be authorized.

t. Acoustic intelligence (ACINT) information and products may not be disclosed without authorization from the ACINT Committee via ONI-33.

u. Communications Security (COMSEC) information will not be authorized unless coordinated with the applicable Combatant Commander and approved by the Committee on National Security Systems (CNSS). Requests for release of COMSEC must be sent to the Combatant Commander (J-6) for coordination with the Joint Staff (J-6). The Joint Staff will forward the request to the Director, National Security Agency (NSA) for consideration and approval by the CNSS.

v. Information that could give assistance to any foreign nation's ability to develop or acquire an independent ballistic missile delivery capability will not be authorized unless approved in accordance with the Missile Technology Control Regime (MTCR). Navy IPO-01 shall coordinate Direct Commercial Sales (DCS) of MTCR-controlled items, and Navy IPO-02 shall coordinate Foreign Military Sales (FMS) of MTCR-controlled items.

w. Information relating to the Global Positioning System Precise Positioning Service (GPS/PPS) will not be disclosed, except in accordance with the DoD Global Positioning System Security Policy issued by reference (bc).

x. Information relating to the control of compromising emanations (TEMPEST) will not be authorized unless recommended by the Director, Naval Criminal Investigative Service and approved by Navy IPO-01.

y. Bibliographies and reference lists containing listings of classified publications will not be authorized, unless it is determined that all listed publications are authorized for disclosure or the lists are sanitized to delete publications that cannot be authorized for disclosure.

20106. Other Disclosure Considerations

In addition to the requirements and limitations described in the above paragraphs, DDAs shall consider the following points when making foreign disclosure decisions. Further guidance on specific types of programs is provided at Chapters 2 through 16.

a. Consideration must be given to the possible broader impact of the decision to provide a military weapon system or capability to a particular country or region. Considerations such as those described below should be addressed in the decision-making process:

(1) Precedence. A precedent could be set which might result in requests for releases to other countries. The U.S. response in such situations should consider projected requests from other countries, the risk of creating an arms race, and the impact to arms control arrangements.

NAVY FOREIGN DISCLOSURE MANUAL

(2) Foreign availability. If the equivalent system, technology or capability is available from a foreign source, providing the U.S. system might not have significant implications.

(3) Impact on U.S. industrial base. The sharing of information that can be used for design or production purposes might have positive or negative implications for the U.S. industrial base.

(4) Political-Military impact. Military and political situations change over time, and the situation in some countries make them more susceptible to change. It is appropriate to seek advice or concurrence from applicable Pol-Mil offices, i.e. CNO N5IS, OASD ISA, or the State Department. Consideration must always be given to the impact on U.S. military forces of disclosure by the proposed recipient to an unauthorized third party.

(5) Feasibility of implementing proposed disclosure decision. In some cases, in order to obtain or expedite a favorable disclosure decision, conditions, safeguards, and limitations may be proposed. When this is done, consideration must be given to the ability of the DoN to implement such conditions, safeguards, or limitations and the impact on all parties involved.

b. Special care shall be exercised to ensure that weapon system information and follow-on support (including training, documentation, and spare parts) to be provided are consistent with the the weapon system configuration approved by the DoN and DoD for export or with equipment which is already in or approved for the country's inventory. Particular care must be exercised when a country has been provided an export variant or commercial variant of a system; documentation may have to be sanitized.

c. If the request is related to an approved international program, a DDL will provide specific disclosure guidance and/or restrictions to the DDA for implementation (see Part II, Chapter 4, paragraph 20403).

PART II CHAPTER 2**TECHNOLOGY TRANSFER AND SECURITY ASSISTANCE REVIEW BOARD**

Ref: (p) SECNAVINST 4900.46B

20201. General

Reference (p) establishes the Technology Transfer and Security Assistance Review Board (TTSARB) as the Navy's vehicle for rendering precedent setting disclosure decisions.

20202. Policy

The TTSARB was established to ensure that cognizant DoN officials review all precedent-setting or otherwise significant foreign disclosure issues to establish a coordinated DoN decision. Therefore, the Deputy Assistant Secretary of the Navy for International Programs (DASN(IP)) or the Director, Navy IPO, as the Executive Secretary of the TTSARB, will coordinate such issues with the acquisition program manager, resource sponsor, operational components, and others with an interest in the issue.

There are three levels of TTSARB decisions: Full TTSARB, Below-Threshold TTSARB (BTT), and Case-by-Case (CBC) TTSARB decisions.

a. Full TTSARB decisions are precedent-setting foreign disclosure decisions that require the review and approval of the TTSARB Co-Chairmen: the Vice Chief of Naval Operations (VCNO) for USN-specific issues or Assistant Commandant of the Marine Corps (ACMC) for USMC-specific issues, and the Assistant Secretary of the Navy, Research, Development, and Acquisition (ASN(RD&A)) for all DoN issues.

b. A BTT decision is a decision for which there is some precedence that has been established by a Full TTSARB but some aspect, as assessed by Navy IPO, requires further decision-making. A BTT decision requires approval by the Deputy Chief of Naval Operations (DCNO), Plans, Policy, and Operations (N3/N5) and the Director, Navy IPO.

c. A CBC TTSARB decision is developed based on an assessment by Navy IPO and is usually an option defined in an existing TTSARB decision for future consideration of the disclosure of a weapon system or platform to additional countries or method of disclosure (e.g., direct commercial sale). The original TTSARB decision defines which TTSARB member signatures are necessary to enact the CBC decision. A CBC decision requires approval by the Director, Navy IPO (Director, Technology Security and Cooperative Programs (IPO-01)).

20203. Procedures

a. Navy IPO drafts TTSARB decisions with substantial input from the cognizant acquisition program manager. It then staffs all TTSARB decisions via the TTSARB Voting System (TVS) to obtain the votes of applicable TTSARB members. After Navy IPO collects the

NAVY FOREIGN DISCLOSURE MANUAL

votes, the TTSARB decision package is forwarded to the VCNO or ACMC and then to the Assistant Secretary of the Navy (Research, Development & Acquisition) (ASN (RD&A)) for signature.

b. TTSARB decisions constitute DoN policy and may be subject to National or other agency approvals. These other approval requirements are identified in the TTSARB decision.

c. The Department of the Navy Disclosure Database (DND2) contains the records of completed TTSARB decisions as well as other disclosure policies.

d. Program Managers shall disseminate the decision of the TTSARB with cognizant DoN personnel and the respective prime contractors to ensure they are aware of Navy policy on export of their weapon systems and technologies.

e. A TTSARB decision may be used by a DDA to approve or deny disclosure requests provided all additional TTSARB conditions have been satisfied.

(1) DDAs must ensure that when reviewing the TTSARB decision they are aware that this is a DoN decision and may be subject to other agency approvals as indicated by the TTSARB. These may include Exceptions to National Disclosure Policy (ENDP), Low Observable/Counter Low Observable Executive Committee (LO/CLO EXCOM) approval, and Committee on National Security Systems (CNSS) approval.

(2) DDAs must also ensure that they review the TTSARB “Terms and Conditions,” which denotes classification levels of information that can be released, when they can be released (before or after signing of LOA), and what information cannot be released.

f. A TTSARB decision does not provide disclosure authority. It is used by DDAs as policy guidance in implementing their authority.

g. When there is no existing policy or when an existing TTSARB decision requires modification, the proponent for a proposed disclosure will submit the request for appropriate action to Navy IPO (Director, Disclosure Policy Division (IPO-01D)) via the cognizant DDA.

PART II CHAPTER 3

EXPORT LICENSES

- Ref: (i) SECNAVINST 5510.36
 (o) DoD 5220.22-M
 (u) SECNAVINST 5510.30A
 (w) International Traffic in Arms Regulations
 (x) Export Administration Regulations (EAR) (15 CFR 730-799) of 30 Jul 04
 (y) DODDIR 5200.1-R
 (z) DODDIR 5200.2-R
 (aa) SECNAVINST 5430.103

20301. General

The International Traffic in Arms Regulations (ITAR) implement the Arms Export Control Act (AECA) as it pertains to the export of defense articles (including technical data) and defense services. The ITAR, reference (w), issued by the Department of State (DoS) states that all exports of defense articles and defense services, as defined by the U.S. Munitions List (USML)(Part 121 of the ITAR), require either an approved export license or the use of a valid ITAR exemption. The Export Administration Regulations (EAR), reference (x), issued by the Department of Commerce (DoC) states that all exports of controlled commodities as defined by the Commerce Controlled List (CCL) require either an export license or a license exception from the DoC.

20302. Policy

It is U.S. government policy that all exports of defense articles and defense services require the approval of an export license or an exemption in accordance with the ITAR or EAR. Government-to-government transfers are processed in accordance with the procedures outlined in Part II, Chapter 1 as authorized by the AECA. DoN organizations that are tasked by Navy IPO to review export license applications will respond within seven business days of receipt per Vice Chief of Naval Operations (VCNO) and Assistant Secretary of the Navy (Research, Development & Acquisition) (ASN (RD&A)) direction. Delays in review of export license applications can jeopardize defense trade initiatives and can have an adverse effect on the U.S. industrial base; however reviewers need to ensure that DoN equities are adequately protected. **Although exports are not by definition “foreign disclosures,” the same foreign disclosure considerations and security requirements that apply to foreign disclosure decisions shall also be applied in arriving at DoN recommendations to the Department of State or the Department of Commerce on export license applications.** However, DoN organizations shall not act as a transmittal agent on behalf of a private individual or firm, either as a convenience or to satisfy security requirements. Such individuals and firms are required to obtain an export authorization in compliance with references (w), (x), and with reference (o), if classified information is involved.

NAVY FOREIGN DISCLOSURE MANUAL

a. The transfer of defense articles and defense services to a lawful permanent resident or protected individual, as defined in Title 8 of the United States Code, is not subject to the export license process.

b. The transfer or disclosure of CMI or CUI to a foreign national who is an authorized employee of a DoN organization is not subject to the export license process and shall be handled in compliance with references (y) and (z) as implemented by references (u) and (l).

c. The transfer or disclosure of CMI or CUI to a foreign national who is an authorized employee of a U.S. contractor or other non-governmental organization (NGO) will be handled under the provisions of this chapter and the National Industrial Security Program Operating Manual (NISPOM), reference (o).

20303. Procedures

Reference (aa) gives Navy IPO the responsibility to coordinate the review of export licenses referred to the DoN. The following procedures apply:

a. Navy IPO reviews licenses received from DoD (Defense Technology Security Agency (DTSA)). Navy IPO will task the appropriate DoN offices to provide input on the export license request when there is insufficient technical expertise at Navy IPO to formulate a recommendation. The DoN offices are required to respond to the request within 7 calendar days.

b. DoN officials reviewing export licenses should consider whether the technology being proposed for export is in accordance with DoN, DoD, and national disclosure policies or if no policy exists, poses a threat to national security. If necessary, they should consult with their cognizant Designated Disclosure Authority (DDA) for interpretation of current DoD and DoN disclosure policy. Additionally, reviewers external to Navy IPO should provide a technical review of the license request. DoN officials can recommend approval, approval with provisos, disapproval with supporting rationale or that the license request be returned without action when there is insufficient information upon which to make a recommendation.

c. When reviewing the export license request it is important to ensure that approval of the request does not create a false impression. For example, it is important to ensure that an unclassified marketing license is not approved if DoN, DOD, and national policies would not support the ultimate export of the end item.

d. Navy IPO recommendations concerning export licenses will be in accordance with the criteria in Part II, Chapter 1.

e. Requests for use of ITAR exemptions (i.e., those requiring written direction from DOD) must be forwarded to Director, Navy IPO (Director, Export Licensing Division (IPO-01A)). This authority has not been delegated below Navy IPO.

20304. DoN ITAR Exemption Request Procedures

DoN offices may receive requests from U.S. industry to execute a foreign transfer under the aegis of an International Traffic in Arms Regulation (ITAR) exemption. The process below should be followed:

a. The recipient of a request for an ITAR exemption must review the request and draft a memorandum to the DoN ITAR exemption authority (Navy IPO-01A) proposing the use of an exemption. As a minimum, the memorandum should contain the following:

- (1) Justification (why the exemption is necessary in lieu of an export license)
- (2) Description of item(s) and copy of technical data
- (3) Disclosure review/approval by appropriate DoN DDA
- (4) End-user/Recipient of technical data
- (5) Proposed duration or end date
- (6) Method of transmission
- (7) Applicable ITAR exemption paragraph

b. The DoN ITAR Exemption Authority will review the proposal and conduct any additional coordination required. If the decision is made to grant an exemption, the DoN ITAR Exemption Authority will provide the exporter written authorization.

c. Navy IPO-01A will maintain a record of all ITAR exemption authorizations.

PART II - CHAPTER 4

INTERNATIONAL AGREEMENTS

- Ref: (c) DoD Directive 5230.11
(ab) SECNAVINST 5710.25B
(ac) OPNAVINST 5710.24
(ad) OPNAVINST 5710.25 (NOTAL)
(ae) DoD Directive 2015.4
(af) DoD Directive 5530.3, with Change 1 (NOTAL)

20401. General

International cooperative programs are implemented under various types of International Agreements (IAs). IAs set forth the terms and conditions under which participating governments agree to cooperate in military research; development; test and evaluation; standardization; production; in-service support; research, development, test, and evaluation (RDT&E); information and personnel exchanges; and operational arrangements. The various types of IAs are described below.

a. Acquisition IAs. These agreements involve the cooperative research, development, production, in-service support, test and evaluation, and loan of defense items. Acquisition IAs include Memoranda of Understanding or Agreement (MOU/MOA) and Project Arrangements (PA) executed under umbrella or framework MOU/MOAs.

b. Operational IAs. These agreements involve cooperative operations such as joint exercises, logistic support arrangements; military information and personnel exchange, and health and medical agreements. Operational MOU/MOAs are typically originated by the cognizant CNO sponsor or fleet representative, vetted through the CNO International Programs & Technology Transfer Office (N5IS), and reviewed by Navy Judge Advocate General (JAG) International Law (N09J- Code 10).

c. The Technical Cooperation Program (TTCP). TTCP was established by a MOU to improve the utilization of the combined technical resources of the five participating countries (the U.S., Australia, Canada, New Zealand, and the United Kingdom) through the exchange of information within its functional categories. The work of TTCP is accomplished through subgroups, and subordinate groups established by the subgroups, in specific key areas and designated as Technical Panels and Action Groups.

d. Information Exchange Program (IEP) IAs. IEPs are implemented through a bi-lateral or multi-lateral MOU or MOA. These MOU/MOAs involve two types of military information: (1) RDT&E information, and (2) operational information. Project- or subject-specific RDT&E IEP annexes are processed by Navy IPO-01 under references (c), (ac), (ad), and (ae). Operational IEP annexes are originated by the cognizant CNO sponsor, coordinated through N525, and reviewed by Navy JAG International Law (N09J- Code 10). Both RDT&E and

operational IEP annexes are coordinated with IPO-01 for a disclosure review and issuance of a DDL.

e. Personnel Exchange IAs. These MOU/MOAs involve cooperative exchange of personnel that include Foreign Liaison Officers (FLOs), Cooperative Program Personnel (CPP), Military Personnel Exchange Program (MPEP), and Engineer and Scientist Exchange Program (ESEP).

20402. Policy

Reference (af) governs the negotiation of international agreements and assigns responsibility for international agreements within the Department of Defense (DoD), its components, commands, or other organizational elements. Reference (c) requires DoD and its components to determine the foreign disclosure requirements prior to the negotiation of an international agreement. Therefore, DoN personnel shall not enter into discussions that imply a commitment to negotiate an agreement until negotiating authority has been obtained and foreign disclosure guidelines have been provided. International agreements, in and of themselves, do not authorize DoN officials to release specific CMI or CUI to foreign entities. DoN personnel shall not disclose CMI or CUI under an international agreement except pursuant to a DDL approved and issued by Navy IPO. DDLs provide disclosure authority and guidance to DoN Program/Project Managers and Technical Project Officers (TPOs) for implementation of international agreements. **Under no circumstances may the contents of DDLs be disclosed or acknowledged to foreign representatives.**

20403. Procedures

Disclosure of DoN information under an IA will be in accordance with a DDL or other disclosure authorization issued by Navy IPO to designated PMs, TPOs, and TTCP representatives.

a. Delegation of Disclosure Authority Letters (DDLs). The DDL contains specific disclosure guidance and/or restrictions associated with the disclosure of CUI and CMI. Navy IPO-01, the PM/TPO and their cognizant DDA develop the draft DDL. The draft DDL is formally coordinated with other cognizant offices as appropriate. Navy IPO will issue a final DDL.

(1) Under DDLs, designated PMs/TPOs may approve foreign visits and authorize the disclosure of U.S. information within the scope of their DDL and international agreement.

(2) Navy IPO and the pertinent PM/TPO shall review DDLs periodically for the purpose of incorporating the most recent disclosure policy decisions and for determining continued applicability. Changes require Navy IPO approval and issuance of a revised DDL.

b. Disclosure of Military Information under TTCP. DoN representatives to various TTCP Subgroups must submit material proposed for oral/visual disclosure or documentary release through TTCP subgroups, Technical Panels and Action Groups via the chain of command

NAVY FOREIGN DISCLOSURE MANUAL

to their cognizant DDA. Such requests shall be forwarded sufficiently in advance of scheduled meetings to permit required staffing (at least 30 days). Release must be confined to that necessary to realize the objectives of cooperative non-atomic research and development.

c. Reporting Requirements. Disclosure officials authorizing the disclosure of CMI under International Agreements will ensure that all disclosures and denials of classified information (during visits or by documents) are reported to the Security Policy Automation Network (SPAN) in accordance with Part II, Chapter 16.

PART II – CHAPTER 5**FOREIGN MILITARY SALES (FMS) AND LEASES**

- Ref: (c) DoD Directive 5230.11
 (f) Arms Export Control Act
 (n) DoD 5105.38-M, “Security Assistance Management Manual” (SAMM)
 (ag) Foreign Assistance Act of 1961
 (ah) OPNAVINST 4900.149
 (ai) Chairman JCS Manual 6510.06
 (aj) DoN Guide for the C4ISR Release Process

20501. General

This chapter covers disclosure policies and procedures for Foreign Military Sales (FMS) and leases. These programs are established by references (f) and (ag). Reference (n) provides policy and procedural guidance on these programs.

20502. Policy

References (c) and (n) require disclosure authorization from the appropriate DDA prior to sales, loans, leases, and grants of defense articles and services and prescribe transfer arrangements. Before responding to an FMS request, the cognizant DDA shall conduct a disclosure review to ensure that the response complies with existing national, DoD, and DoN disclosure policies, and the prescribed transfer arrangements have been approved by the responsible security office.

Creating a false impression of the U.S. Government’s willingness to make military materiel, technology, or information available to friends and allies in advance of obtaining full disclosure approval for a program or issue must be avoided. For more information see Part I, Chapter 1.

Release of information relating to an equipment transfer is generally limited to that information necessary to operate, maintain (at the operational level), or deploy the equipment. Hardware/software design data, source code, manufacturing and production data, and system vulnerabilities to countermeasures technology will normally not be released unless authorized by a DDA as a deliverable specified in the security assistance case.

20503. Procedures for FMS or Leases

a. Pre-case disclosures. Initial disclosures will be limited to general information usually no higher than the CONFIDENTIAL level on general capabilities, performance characteristics, support requirements, and price and availability until a formal purchase commitment has been made. No specific information on system countermeasures (CM) susceptibilities/vulnerabilities or counter-countermeasures (CCM) capabilities will be disclosed until the sale is consummated. Only a TTSARB decision or Navy IPO is authorized to grant exceptions.

b. Case approval process.

(1) A foreign government official Letter of Request (LOR) is required, which includes:

(a) System Nomenclature and/or sufficient description of the defense articles and services being requested; including training, logistic support, supporting documentation, etc. Include what platform the requested weapon system will be installed on and classification of equipment and documentation.

(b) Sufficient purpose and justification, including identification of platform and operational environment (e.g. ship class, mission areas/capabilities, and requirements for integration with other combat systems and communications links).

(c) If a request is for Significant Military Equipment/Major Defense Equipment (SME/MDE) a country team assessment (CTA) is required in accordance with reference (n). This CTA will also be used if an Exception to the National Disclosure Policy (ENDP) is required.

(2) If the LOR lacks the above information the Navy IPO Country Program Director (CPD) shall contact the requester and obtain this information. If the requestor doesn't know what specific weapon will meet their needs but they have a generic description of what is required, the CPD must obtain some technical assistance from the applicable DoN program office prior to requesting a disclosure determination from a DDA.

(3) Prior to Navy IPO-02 tasking an LOR to a Case Administering Office (CAO), the CPD must perform a preliminary review of TTSARB to assess whether the request appears to be feasible under current disclosure policy. If the request is not feasible a denial letter should be written by IPO-02 and coordinated through IPO-01D. If the request is feasible, it should be sent to the applicable CAO for coordination with the applicable Program or Case Manager, for programmatic data, and the SYSCOM DDA for a disclosure determination. The CAO will then prepare the draft Letter of Offer and Acceptance (LOA), lease, or Pricing and Availability (P&A) data. CAO and Case Manager responsibilities are outlined in reference (ah).

(a) Threat/Parametric Data. Special emphasis must be given to the consideration of possible intelligence disclosure implications in FMS decisions. Many modern weapon systems require computer programmed threat data that may be beyond the capability of the purchaser to supply. Therefore, coordination must be initiated with cognizant intelligence agencies prior to offer of such equipment to foreign governments. Additionally, Navy IPO-01 and NDPC approvals, known as Exceptions to National Disclosure Policy (ENDP), are required for the release of such data in conjunction with certain weapons systems sales.

(b) C4ISR. The Release/Disclosure of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Systems information, data and equipment, that requires Communication Security (COMSEC) equipment to function in a

secure mode, is under the direct control and authority of agencies outside of DoN. The release process is governed by and defined in reference (f). The Committee on National Security Systems (CNSS) is the ultimate authority for the release of COMSEC. In order to preclude any false impression of the U.S. Government's readiness to release COMSEC equipment prior to CNSS approval, all foreign customer requests for C4ISR equipment, that employ COMSEC, must be referred to Navy IPO (Strategic Planning Directorate) (IPO-03) for outside coordination prior to any discussions, commitments, or offers for sale being made to the potential FMS customer. A request for C4ISR equipment will require the Combatant Commander to validate an interoperability requirement between the U.S. and the foreign government. IPO-02 must delay processing the request through normal FMS channels until the Release in Principle is secured from CNSS. See reference (aj) for more information.

(4) When the SYSCOM DDA is tasked to provide a disclosure determination, the LOA/P&A draft package will include the basis of the determination as follows:

(a) If the release determination is within the tasked DDA's delegated disclosure authority, the DDA should make the determination for release and should state, "this draft [LOA/lease/P&A] has been approved by the [SYSCOM] Designated Disclosure Authority and is releasable in accordance with [specific policy]" in the Defense Security Assistance Management System remarks section to Navy IPO-02. "No objection to release" is not an acceptable statement. A release determination should be accompanied by sufficient justification (see Part II, Chapter 1).

(b) If the release determination exceeds the tasked DDA's delegated disclosure authority, a recommendation should be provided to Navy IPO, including:

- Whether this version of the weapon is releasable in accordance with the TTSARB ##-XX and whether the training and logistic support is also releasable.
- It should include a breakdown of the classification of hardware, software and documentation.
- If there is some additional equipment requested that is not addressed by the TTSARB, then provide rationale for why it is releasable. For example, state that release of this equipment is in accordance with the DOD Policy on Military Spread Spectrum Communications Systems and discuss the paragraphs within the policy documents that pertain to your disclosure analysis.
- Include a statement regarding the critical/sensitive components of the weapon system and why the DDA is recommending release or denial of the weapon system/information.
- Describe how the U.S. benefits from the sale or lease.

NAVY FOREIGN DISCLOSURE MANUAL

(c) If a denial is recommended it should not be based solely on historical precedent. Rationale for denial must be provided, including why it is not in the interests of the U.S. to change the DoN release policy or seek approval by higher authority.

(5) The recommendation for approval or denial by the applicable SYSCOM DDA will be provided by IPO-02 to IPO-01. Navy IPO-01 will provide the disclosure determination when it is the CAO or when the SYSCOM DDA cannot make a disclosure or release determination.

c. Case Execution. Disclosures related to a signed FMS case must adhere to the FMS case scope, terms, and conditions, and will normally be limited to basic operation, maintenance and training. Other areas of consideration follow:

(1) The following types of information, for example, shall not be released unless specifically identified in the FMS case:

(a) Information that would reveal the details of design, development, production, or manufacture

(b) Intermediate- or depot-level repair or maintenance information

(c) Software source code and related documentation

(d) Research and Development data

(e) Test results, such as OPEVAL and TECHEVAL reports and other sources of information that would reveal system susceptibilities and vulnerabilities.

(f) Tactical Training and information

To release specific items listed above a separate disclosure approval by the responsible DDA and an amendment to the FMS case is required.

(2) FMS case managers will ensure that the information and material being provided is consistent with the configuration approved for that country.

(3) Briefings and documentation that include information on U.S. systems or programs which are not part of the FMS case but are considered by the PM to be appropriate for release must undergo a disclosure review by the DDA.

(4) Case amendments and modifications that affect the scope of the case generally require a separate disclosure determination. FMS case managers should not make commitments to release system performance upgrades unless a disclosure review is performed by a DDA.

(5) Foreign visits to the U.S. associated with an FMS case must be processed via the Foreign Visits System (FVS) see Part II, Chapter 8.

PART II – CHAPTER 6**THE FOREIGN COMPARATIVE TESTING (FCT) PROGRAM**

Ref: (w) International Traffic in Arms Regulations (22 CFR 120-130)
 (ak) 10 U.S.C. 2350a(g)
 (al) DoD 5000.3-M-2
 (am) OUSD (AT&L) FCT Handbook

20601. General

This chapter pertains solely to the disclosure of Department of the Navy (DoN) Foreign Comparative Testing (FCT) project information and test results to foreign contractors who have provided their products to DoN activities for test and evaluation utilizing FCT funding. All DoN FCT officials should be familiar with the contents of this chapter.

The FCT Program is Congressionally mandated by reference (ak) and is funded under the Defense-Wide Research Development Test and Evaluation (RDT&E) Appropriation. The FCT Program Manager, working under the Deputy Under Secretary of Defense, Advanced Systems and Concepts (AS&C), Office of the Under Secretary of Defense, Acquisition, Technology and Logistics (OUSD (AT&L)), administers the overall FCT Program.

20602. Policy

The purpose of the FCT Program is to test U.S. allies' and other friendly nations' non-developmental items (NDIs) to determine if they satisfy U.S. Armed Forces requirements or correct mission area shortcomings per references (al) and (am). The associated foreign vendors are invited in many instances to witness and, to some degree, participate in the testing of their items. The FCT Program results in a test report, which is generally releasable to the foreign contractor and/or foreign government that provided the item for testing. If the final test report includes U.S. CMI or CUI, that information shall be reviewed for release by the cognizant DDA.

20603. Procedures

The following procedures shall be followed when reviewing FCT reports or data for release to the FCT project contractor or a third party¹:

a. At the earliest stage of the project the DoN FCT project manager shall provide the responsible DDA a description of the project, identification of the foreign vendor, extent of foreign vendor's expected involvement, a specific description of the U.S. information to be disclosed, and highest security classification level of U.S. information/materiel requiring access

¹ The U.S.-Canada Joint Certification Program (JCP) permits U.S. and Canadian certified contractors access to each other's unclassified technical data (including critical technology) directly from the originator. To determine if a Canadian contractor is certified under the JCP, FCT Project Managers may contact the Joint Certification Office in Battle Creek, Michigan at 269-961-7431. NOTE: Direct access by Canadian contractors to certain unclassified technical data is limited by reference (w) Section 126.5.

NAVY FOREIGN DISCLOSURE MANUAL

by the vendor. DDAs are responsible for determining whether the information/materiel involved in the test project is releasable to the foreign vendor. This would include access to U.S. information during visits to DoN commands or to DoD contractors for testing the foreign vendor's product.

b. There may be instances where portions of CMI or CUI test data or reports generated by the FCT Program are not releasable. In such cases, foreign contractors will not be provided those portions of the test data collected on their items. Requests by vendors to release their test data and reports containing U.S. CMI or CUI to any "Third Party" must be forwarded by the vendor's government to Navy IPO 01 for a disclosure approval. (See Appendix A for the "third party" definition.)

c. If the disclosure decision exceeds an acquisition command's delegated disclosure authority, the DDA will forward a fully justified recommendation to Navy IPO, who will reply with the final disclosure decision.

d. It is important that the above disclosure actions be initiated and processed expeditiously so the disclosure review does not lead to misunderstandings about what test data may be released to foreign vendors during the course of the DoN FCT project.

e. Any CMI generated by the FCT Program will be released on a government-to-government basis only, normally through the country's embassy in Washington, D.C. Any unclassified information can be released directly to the foreign vendor.

PART II – CHAPTER 7**TRANSFER OF U.S. NAVAL VESSELS TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS**

Ref: (an) SECNAVINST 4900.48

20701. General

The transfer of U.S. excess naval vessels (i.e. naval vessels that have been, or will be, removed from service) to eligible countries significantly improves their capabilities at a much lower cost than new construction while eliminating inactive excess ships from U.S. inventories. “Ship transfers” can also lead to the foreign acquisition of U.S. shipboard systems, equipment and services in support of the transferred vessel. The Chief of Naval Operations (CNO) is responsible for determining which naval vessels are available for foreign transfer consistent with the short and long term operational and mobilization requirements of the DoN. The CNO’s recommended allocation list is then forwarded for coordination. Congressional notice and, in accordance with 10 U.S.C. 7307, ship transfer-authorizing legislation may also be required. Navy IPO is the cognizant organization for providing management and oversight for the ship transfer process.

20702. Policy

It is DoN policy to transfer naval vessels to foreign governments and international organizations in support of U.S. foreign policy objectives. The cognizant DDA shall review systems and materiel associated with proposed transfers to ensure compliance with the DoN, DoD, and national disclosure policies. Reference (an) provides policy guidance and procedures for the transfer of excess U.S. naval vessels to foreign governments and international organizations.

20703. Procedures

a. After the approval of the ship allocation list, Navy IPO distributes the list to the cognizant U.S. Navy program managers. Based on the ship’s current inventory, the program manager will develop a proposed ship configuration in accordance with DoN, DoD and national disclosure policies. The proposed ship configuration list is reviewed and coordinated with the Designated Disclosure Authority (DDA) for the purpose of determining whether the items contained on the list are releasable to the prospective foreign entity. This disclosure review shall include all equipment, weapons, systems, support equipment, software, information, and documentation associated with the proposed transfer.

b. For weapons or systems that come under the cognizance of another Navy organization, the DDA shall coordinate the request with the cognizant Navy organization for a release recommendation.

c. If the SYSCOM DDA cannot make a determination on release of an item because it is not within their disclosure authority, then the DDA shall forward a recommendation to Navy IPO

NAVY FOREIGN DISCLOSURE MANUAL

01D and include whether or not a previously non-releasable item should be reconsidered for release (e.g., due to foreign availability, technology obsolescence, removal costs, etc.).

d. If a determination is made that some of the equipment is not releasable, then the (DDA) shall inform the program manager that the item must be removed from the ship, generally at DoN expense.

e. If a determination is made that some of the equipment needs modification (tailoring) then the DDA shall inform the program manager that the item must be modified in accordance with the guidance that the item manager provides, generally at the customer's expense.

f. After completion of the foreign disclosure review, the final ship configuration list, to include those items that must be removed, is sent by the Navy Program Manager to Navy IPO. Navy IPO is responsible for management oversight of the ship transfer process and providing guidance on equipment removals for compliance with disclosure policy.

PART II - CHAPTER 8**ONE-TIME AND RECURRING VISITS BY FOREIGN NATIONALS AND REPRESENTATIVES OF FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS**

- Ref: (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1) (NOTAL)
- (c) DoD Directive 5230.11
- (d) DoD Directive 5230.20
- (e) DoD Directive 4500.54
- (f) AECA
- (o) DoD 5220.22-M
- (t) Guide for Foreign Attaches Accredited to the Department of the Navy (NOTAL)
- (u) SECNAVINST 5510.30A
- (w) ITAR
- (z) DoD 5200.1-R
- (ao) DoD Directive 4500.54-G
- (bh) DUSD memo of 18 May 2004

0801. General

Reference (d) establishes the International Visits Program (IVP) and provides policy guidance for the control over visits of foreign nationals and foreign representatives of international organizations to Department of the Navy (DoN) activities and cleared contractor facilities. The disclosure processes implemented by reference (d) and this chapter are in accordance with references (b) and (c).

20802. Policy

Hosting official foreign national visitors and assigning foreign nationals to DoN organizations as foreign liaison officers, exchange personnel, or cooperative program personnel are necessary to establish or support bilateral or multinational agreements and programs. Official foreign visitor access must be controlled properly to avoid inadvertent or unauthorized disclosure. DoN organizations shall comply with the provisions of reference (d). Foreign nationals who visit or who are assigned to DoN organizations may be permitted access only to Classified Military Information (CMI) or Controlled Unclassified Information (CUI) that is authorized for disclosure to their government. Therefore, only Navy IPO, a Designated Disclosure Authority (DDA), or other official delegated authority by a Delegation of Disclosure Authority Letter (DDL) may approve access to CMI and CUI by visiting and assigned foreign nationals.

A foreign visit is any contact by a foreign national or foreign representative that involves substantive or technical discussions or the disclosure of CMI or CUI. Foreign visit requests are required for visits by official representatives of a foreign government or international organization to DoN activities and cleared contractor facilities (see paragraph 20803(a) for

exemptions). The purpose of the request process is to provide DoD and DoD contractor personnel disclosure guidance and to record the disclosure of CMI and CUI to foreign visitors. A DDA must approve a visit request prior to any disclosure of CMI or CUI to a foreign visitor. The final decision for scheduling and hosting foreign visits, however, remains the prerogative of the host command or facility.

20803. The Foreign Visit System (FVS)

The FVS component of the DoD Security Policy Automation Network (SPAN) provides staffing and database support for the processing and recording of visit requests by foreign nationals to DoD activities or authorized contractor facilities. The FVS consists of two different parts, an unclassified and a classified system. The unclassified system allows foreign embassies to submit foreign visit requests online to the appropriate military department where it is then drawn into a classified system. The classified system provides staffing capabilities to support the decision-making process. After a disclosure decision has been reached on a specific visit request, the FVS is able to transmit a visit confirmation message to the requesting embassy via unclassified means. The FVS also generates a record of the disclosure decision, which is automatically entered into the SPAN Foreign Disclosure System once the request is approved or denied.

a. Types of Official Visit Requests. The following types of official visits pertain to access by foreign nationals or their representatives, under the sponsorship of their government or an international organization, to a DoD component or DoD contractor facility.

(1) One-time Visits. A single, short-term visit to a single facility for a specific purpose. A one-time visit normally will not exceed thirty days.

NOTE: Emergency Visits. Emergency visits are those one-time, short notice visits that are submitted by the foreign government or international organization and are identified as such. An emergency visit request will be limited to situations in which failure to conduct the visit will jeopardize an official government project, program, or contract. In no case will the request be accepted less than one full working day prior to the visit. Since the concurrence of the host facility is always required, obtaining their tentative approval in advance will expedite the processing of the emergency visit request. Emergency visit requests should not be submitted in order to circumvent routine visit procedures. If circumvention is suspected, it should be reported to Navy IPO so that appropriate action can be taken to preclude such submissions in the future.

(2) Recurring Visits. Multiple visits to a single facility on an intermittent basis in support of an on-going international agreement, contract, or program. A recurring visit will not exceed one year's duration. With the exception of emergency visits, the pertinent foreign office or visitor(s) shall give the host activity at least 72 hours notice of the actual date and time the visit is intended, following approval of a visit. All activities have the right to refuse any visit if the visitor arrives without such advance notice.

(3) Extended Visits. A long-term visit to a single facility on an extended basis in support of an on-going international agreement, contract, or program. Extended visit

authorizations are to be used when a foreign national is required to be in continuous contact with a DoD Component or a DoD contractor facility beyond 30 days for such programs as a foreign government contract or joint program, a foreign liaison assignment, participation in an exchange program, or assignment as a cooperative program personnel. Activities will normally not refuse extended visitors since their assignment is normally linked to a joint or cooperative program previously agreed to by a representative of the U.S. See Part II, Chapter 9 for information on extended visits.

b. Visit Amendments. The requesting embassy may amend official visit requests. Amendments are limited to the date(s) of the visit and/or the names of the visitors. If any other element of the visit request requires an amendment, a new visit request must be submitted. Emergency visits may not be amended.

c. Unofficial Visits. Unofficial visits are visits by foreign nationals who are not representing their government in an official capacity, e.g., courtesy calls, public tours, and students. Access to DoN and its cleared contractor facilities by such persons will be handled on the same basis as visits by U.S. citizens without security clearances. Unofficial visits are outside the scope of the FVS and instead shall be processed in accordance with reference (u), which implements reference (z).

d. Office of Primary Responsibility (OPR). An OPR, as it relates to the foreign visit approval process, is the office with delegated disclosure authority over the technical content of the visit that has online access to the FVS and that makes the final decision on a foreign visit request. For approved visits, the OPR will enter into the FVS any applicable disclosure restrictions and guidance.

20804. FVS Exemptions

The following categories of visits are exempt from the foreign visit request process.

a. Visits by foreign nationals who are not representatives of their government in an official capacity are exempt from the visit request process. These visits shall be governed by local security practices in accordance with standard physical and operational security requirements. Access by such unofficial foreign nationals to DoN commands or contractor facilities shall be handled on the same basis as visits by U.S. citizens without security clearances. In almost all cases, only information that has been determined to be public information (which excludes CMI and/or CUI) may be disclosed.

b. Foreign nationals visiting under the terms of a DoD or DoN contract are not considered foreign visits and shall be cleared in accordance with the reference (o).

c. Visits conducted at DoN contractor facilities that involve access to only unclassified information. This exemption is subject to the following three limitations:

(1) In some cases, a government contract will require a contractor to administer all foreign visits to its facilities via the FVS. When a contractor has a contractual obligation of

this nature, then FVS visit requests must be submitted by the parent embassy of the proposed foreign visitor.

(2) The subject matter of the proposed visit must be unrelated to DoN programs.

(3) The contractor holds a valid export license, or the information to be disclosed does not require an export license.

d. The National Industrial Security Program Operating Manual (NISPOM) (reference (o)) regulates visits by foreign national employees of U.S. defense contractors. Access to export-controlled technical data by foreign national employees of U.S. contractors is authorized in accordance with an export license or by another written U.S. Government authorization that the employing contractor obtains. When these employees visit another contractor facility or DoN component, the employing facility should provide a copy of the export license or other written authorization to the security office or DDA of the facility to be visited.

e. Visits by foreign nationals to participate in security assistance training using Invitational Travel Orders (ITOs) provided by their in-country U.S. Security Assistance Office are exempt from the FVS. The Arms Export Control Act (AECA) (reference (f)) prohibits the provisioning of U.S. “defense articles and services” to a foreign government without payment. Training is a “defense service.” Within the DoN, the Foreign Visit System (FVS) shall not be used as a means to seek disclosure authorization for disclosing training course information to foreign governments, international organizations, or their representatives. Training-related disclosure guidance is covered elsewhere in this document (see Part II, Chapter 10) and other directives.

f. Visits by foreign nationals traveling on ITOs for Orientation Tours arranged under the Security Assistance Training Program (SATP) when CMI will not be disclosed are exempt from the FVS. If disclosure of CMI is required as part of the orientation tour, then an FVS request must be submitted by the foreign visitor’s embassy in Washington, D.C. in order to certify the visitor’s security clearance.

g. Unclassified visits by Canadian government officials and certified Canadian contractors through the U.S.-Canada Joint Certification Program (JCP) in accordance with the DoD “U.S.-Canada Joint Certification Program” Manual (JCP Manual) of December 1996, are exempt. For further information see paragraph 21112 for information on JCP.

h. Visits sponsored and administered by the U.S. European Command under its Joint Contact Team Program (JCTP) are exempt, provided that the visitors are traveling on ITOs and that no CMI will be disclosed.

i. Unclassified visits that fall under the auspices of Professional Development Orientation and Familiarization Tour Programs, conducted by Unified Commands or fleet commanders and funded by the use of Traditional COCOM Activities (TCA) resources, are exempt. If disclosure of CMI or CUI is anticipated, then a visit authorization is required.

j. The long-term unclassified employment of foreign nationals is exempt. Policy and procedures for employing foreign nationals can be found in section 6-12(n) of SECNAVINST 5510.30A, “DoN Personnel Security Program,” of March 10, 1999.

k. Chief of Naval Operations (CNO) Counterpart Visits are exempt. All arrangements for visits by the head of a foreign navy are the overall responsibility of CNO (Director of Naval Intelligence, Assistant for Foreign Liaison), hereafter known as CNO (N2L). Navy IPO will provide disclosure guidance, upon request, directly to CNO (N2L), via classified email (SIPRNET). CNO (N2L) will promulgate specific disclosure guidance, as required, to those activities hosting the CNO’s counterpart and entourage.

l. Visits to U.S. Navy and USMC facilities at overseas locations are exempt. Control of these visits will be in accordance with the guidance established by their chain-of-command (e.g., guidance as directed by COMPACFLT, COMLANTFLT, or other authority).

m. Visits to areas accessible to the general public, involving only public domain information, are exempt.

20805. Disclosures by U.S. Government Personnel During Travel

All DoN personnel shall ensure that CMI and CUI to be disclosed during visits and meetings with foreign national attendance have been approved in advance by the responsible DDA in accordance with the requirements of paragraph 21108 of this Manual. Reference (d) requires that DoD organizations designate an official to be responsible for approving visits by DoN personnel to overseas locations and shall ensure compliance with the foreign disclosure, security, and other requirements set forth in the directive. Reference (ao), the Foreign Clearance Guide (FCG), identifies specific visit clearance requirements for individual countries. DoN organizations shall establish procedures to implement references (e) and (ao).

20806. The FVS Request Process

a. The FVS request process begins when a foreign embassy located in Washington, D.C., or the designated office of an international organization, submits a request to visit a DoN component. All requests are required to be submitted no less than 21 working days prior to the first day of the proposed visit.

(1) Embassies with terminals connected to DoD’s Security Policy Automation Network (SPAN) FVS must submit their visit requests electronically. The FVS automatically forwards to Navy IPO visit requests to DoN commands, activities, and contractor facilities under contract to the DoN.

(2) Embassies or international organizations without FVS connectivity shall submit visit requests via facsimile to Navy IPO in accordance with the procedures set forth in reference (t). Navy IPO will then enter the requests into the FVS.

b. Staffing and Review. The Office of Primary Responsibility (OPR) shall staff the visit request to all stakeholders of the information to be disclosed. The OPR must use the policy guidance set forth in reference (b), other DoD and DoN disclosure policies, and this manual to evaluate whether the information requested or briefings to be provided can be authorized for disclosure to the visitor's government. Several databases are available within SPAN and on the Navy IPO classified website (www.nipo.navy.smil.mil) that can assist the OPR in making a disclosure decision. For those Navy IPO databases that are password-protected, contact information for requesting access is provided on the website. Foreign visit requests that require a level of disclosure that exceeds the OPR's authority will be transferred online to Navy IPO for action. When a transfer is necessary, the original OPR will include their disclosure recommendation and justification so as to preclude re-staffing. Foreign visit requests that have been incorrectly assigned and fall under the cognizance of another OPR shall be transferred online directly to the proper OPR.

c. Decision. The OPR will make a decision regarding each FVS visit request based upon the review of applicable policies and the recommendations received as a result of staffing.

(1) Approval. The OPR may approve the request. The OPR shall enter into the appropriate section of the request: the approval decision, the approved level of classified disclosure, and specific disclosure guidance that the host(s) of the visit intends to use. Additionally, all OPRs will include the following manuals in all of the disclosure guidance manuals that they issue: "THE RECIPIENT OF THIS VISIT APPROVAL NOTIFICATION IS REQUIRED TO DISSEMINATE THE DISCLOSURE RESTRICTIONS CONTAINED HEREIN TO THE U.S. PERSONS THAT WILL ACTUALLY HOST OR CONDUCT THIS VISIT." Once the OPR closes the request in the FVS, the system automatically notifies the embassy or international organization of the approval if the recipient has an online FVS capability. If the embassy or international organization is not online, the system generates a letter that can either be mailed or facsimiled to the requesting embassy or international organization. It is strongly recommend that a facsimile copy be sent so as to preclude notification delays. Simultaneously, the facility hosting the visit shall be notified by either facsimile, letter, Defense Message System (DMS) message, or the FVS, of the approved disclosure level for the visit as well as any specific disclosure guidance. It should be noted that the requesting foreign embassy only receives a simple approval notice and the contact information for the U.S. Point of Contact (POC) for the visit. The foreign embassy does not, however, receive any notice of the approval disclosure/classification level for the visit or any of the disclosure limits stipulated by the OPR.

(2) Denial. The OPR must judiciously apply this option because a denial may result in political, cultural, or military repercussions. An OPR may only deny a visit request when all of the information relating to the visit exceeds the disclosure classification level authorized for the visitor's government and that other alternatives for meeting the visit's purpose are not available. All denials will be coordinated with Navy IPO (IPO-01B) prior to transmission via the FVS.

(3) Returned without Action. If a visit request is incomplete or the visit cannot be approved for any reason besides that which is disclosure policy related, the OPR shall return the

request to the embassy with an accompanying explanation. By returning the request with comments, the visit can be edited and resubmitted by the sending embassy or organization without having to initiate an entirely new request. For example, if the return without action is due to a scheduling conflict, the OPR might wish to recommend alternative dates for the visit.

(4) Returned without Sponsorship (“non-sponsored”). If the visit request is for a visit to a contractor facility and the OPR cannot identify any specific DoN program or contract that supports the visit, the OPR may return the request without sponsorship. The lack of sponsorship does not prevent the visit, but merely denotes that the visit is not related to a DoN program or contract. Most non-sponsored visits simply provide an official foreign government certification of a visitor’s security clearance level.

NOTE: Non-sponsored visits may take place if the information to be disclosed is public domain information only, or if the contractor has a valid export license to disclose the information.

(5) Cancellation. Either the OPR or the requesting embassy may cancel a request. This is an administrative action that removes requests because of a change in schedule or other circumstances. It also allows either party to remove duplicate requests.

d. Reporting Requirements. For each approval or denial, the OPR is required to enter their decision into the FVS. This action also creates a permanent disclosure record in the SPAN Foreign Disclosure System (FDS) Database. Other visits, (i.e., those exempt from the FVS process per paragraph 20304) require a manual entry into the FDS Database when CMI is disclosed during a visit. (See Part II, Chapter 16 of this manual for FDS Database information.)

20807. Special Visit Conditions

The following visits necessitate additional considerations within the foreign visit request process.

a. Contractor Facilities. The disclosure of classified information or certain controlled technical data to foreign nationals qualifies as an export of defense articles under U.S. law and regulation.

(1) A State Department export license is required of all U.S. contractors for the export of classified and unclassified defense articles and services disclosed during foreign visits, unless a DoD component sponsors the visit or an export license exemption applies.

(2) DoD-sponsored foreign visits to U.S. contractors constitute an exemption from the export-license requirement under Sections 125.4 and 125.5 of the reference (w).

- DoN components will not sponsor foreign visits merely to enable contractors to avoid the licensing requirements of reference (w).

- DoN shall approve foreign visit requests to U.S. contractor facilities only when the proposed visit is directly connected to a specific current or proposed DoN program.
- Requests for visits that are not related to a specific DoN program with the foreign government or entity must be returned to the requester without sponsorship, per paragraph 20806(c)(4).

b. Visits to Shipbuilding Facilities Engaged in the Repair, Conversion, Overhaul or Construction of Naval Vessels. The Commander, Naval Sea Systems Command (COMNAVSEASYSCOM) has been delegated exclusive authority for approval and denial of all visits regarding shipbuilding facilities engaged in repair, conversion, overhaul, or construction. These visits present unique security problems. The overall scope, complexity and sheer size of shipbuilding, repair, overhaul, and construction projects are not always compatible with normal security control measures. Accordingly, the following guidance is established for visits to sites at which naval vessels are under construction, conversion, repair, or overhaul:

(1) No person shall be allowed to go on board naval vessels under construction, conversion, repair, or overhaul except under the authority of COMNAVSEASYSCOM or a field representative assigned supervision of the vessel.

(2) No person shall be allowed at the construction, conversion, repair, or overhaul sites, or adjacent areas (i.e., shops within naval or commercial shipyards, repair facilities, docks, or piers) except on authority of COMNAVSEASYSCOM or the field representative assigned supervision of the vessel.

(3) A visitor granted such access should comply with all conditions and controls imposed by the COMNAVSEASYSCOM. Non-compliance shall serve as sufficient justification to cancel a visit authorization previously granted.

(4) Requests for a foreign visit to a Naval or commercial shipbuilding facility shall be placed through the FVS by the visitor's embassy. Navy IPO will then transfer the request to COMNAVSEASYSCOM for further action as the OPR. Foreign exchange personnel serving aboard a U.S. ship that makes a short unscheduled visit to a shipyard are subject to the exception contained in paragraph 20908 of this manual.

c. U.S. Marine Corps (USMC) Commands/Facilities. The Commandant of the Marine Corps (CMC) has been delegated disclosure authority to approve one-time, recurring, and emergency visits involving the disclosure of USMC classified information. Foreign visits to USMC activities will be submitted through the FVS. Navy IPO will transfer the request to CMC (CIC) for action if the information for disclosure is within the scope of the authority delegated to CMC. Navy IPO will retain OPR authority for any visit requests that exceed the level of authority delegated to CMC.

d. Naval Intelligence. Upon receipt by Navy IPO, requests for visits to the Office of Naval Intelligence (ONI) will be transferred to ONI-333 for action. Any visit requests that

involve the potential disclosure of naval intelligence that would exceed the authority of the cognizant OPR will be transferred to ONI-333 for final action.

e. Visits to USN Operational Commands. Visits to COMLANTFLT, COMPACFLT, COMUSNAVEUR, COMUSNAVCENT, COMUSNAVSO, or any of their subordinate activities will be the responsibility of that command as an OPR, if those visits are within their DDL. In order to perform the functions of an OPR, the operational commands listed above must have access to SPAN's FVS via SIPRNET. The DDA appointed within each command will coordinate requests for visits to surface ships and submarines, nuclear or conventionally powered in accordance with paragraph 20807 (h). The level of classified information to be disclosed may never exceed the levels found in the charts contained in Appendix A of reference (b) or any applicable policy statements contained in Appendices B and C of reference (b).

f. Visits Involving Atomic Information, Naval Nuclear Propulsion Information, and Access to Nuclear Propulsion Spaces.

* (1) Atomic Information or Restricted Data and Formerly Restricted Data (RD/FRD) shall not be disclosed to foreign nationals except when the disclosure is completed under an agreement negotiated pursuant to reference (r) and is explicitly authorized personally by the CNO or VCNO. The disclosure of Atomic Information (RD/FRD) requires coordination with the Joint Atomic Information Exchange Group (JAIEG).

* (2) Naval Nuclear Propulsion Information (NNPI), whether classified or unclassified, shall not be disclosed to foreign nationals without prior personal approval of the CNO or VCNO. Requests for visits that include disclosure of NNPI must be endorsed by CNO (Director, Naval Nuclear Propulsion) prior to being presented to CNO or VCNO for approval.

* (3) Foreign nationals shall not have access to the nuclear propulsion spaces of nuclear-powered naval vessels without the prior personal approval of the CNO or VCNO in writing. When these visits are approved, the visitors will be limited to high-level political or diplomatic personages who have no technical background. NNPI shall be protected as directed by the disclosure authorization issued by the CNO or VCNO. The CNO or VCNO may impose his/her own reporting requirement for all visits of foreign nationals to nuclear propulsion spaces in addition to the requirements imposed by reference (c). Requests for visits that include access to nuclear propulsion plant spaces must be endorsed by CNO (Director, Naval Nuclear Propulsion) prior to being presented to CNO or VCNO for approval.

g. Embarkation in USN/USMC Aircraft. The Naval Component Commanders may authorize the embarkation of foreign nationals in USN/USMC aircraft for the purpose of practical demonstration and orientation under the guidance of sections 3.1 and 3.2 of OPNAVINST 3710.7R, "NATOPS General Flight and Operating Manuals." The disclosure of classified information in connection with such embarkations must be strictly limited to the pertinent disclosure guidance for the aircraft for the country involved.

h. Visits to Afloat Units. Basic policy concerning visits of personnel to afloat units is contained in references (i), (u), and (be). This manual does not affect the applicability of the

manuals concerning “Embarkation in U.S. Naval Ships.” The approving authority for visits of foreign nationals to afloat units is as follows:

* (1) Surface Ships.

- The commanding officer of a conventionally or nuclear-powered surface ship may authorize unofficial visits by foreign nationals while the ship is in port when there is no disclosure of CMI or CUI. Disclosure should be limited to public domain information only.
- The Naval Component Commanders, Numbered Fleet Commanders, Type Commanders, and Force Commanders may authorize visits to conventionally powered surface ships in their command involving the disclosure of CMI and CUI while the ship is in port or underway.
- The Naval Component Commanders, Numbered Fleet Commanders, Type Commanders, and Force Commanders may authorize visits to nuclear-powered surface ships in their command, less access to Nuclear Propulsion Spaces, involving the disclosure of CMI and CUI when the ship is in port or underway as long as there will be no disclosure of NNPI or RD/FRD.
- As discussed in paragraph 20807(f), only the CNO or VCNO (or DCNO (Naval Warfare), Director, Submarine Warfare Division, as delegated) may authorize visits by foreign nationals to Nuclear Propulsion Spaces or the disclosure of NNPI and/or RD/FRD. This authority may not be re-delegated.

(2) Submarines.

- The commanding officer of a submarine may authorize unofficial visits to the submarine when it is in port. No CMI, CUI, RD/FRD, or NNPI, may be disclosed, nor can access be granted to Nuclear Propulsion Spaces. The visit should be limited to public domain information. Only CNO (DCNO (Naval Warfare), Director, Submarine Warfare Division) may approve visits by large groups of foreign nationals to a U.S. submarine.
- The pertinent Naval Component Commander may authorize official visits by foreign representatives to a submarine in port involving the disclosure of CMI or CUI. However, the Naval Component Commander may not authorize the disclosure of RD/FRD or NNPI, nor can the Naval Component Commander grant access to Nuclear Propulsion Spaces. Only CNO (DCNO (Naval Warfare), Director, Submarine Warfare Division) shall approve visits by large groups of foreign nationals to a submarine.

- The Naval Component Commanders may approve visits by representatives of the North Atlantic Treaty Organization (NATO) or NATO member governments to underway submarines in their command. All visits to an underway submarine shall be treated as classified, since it is virtually impossible to preclude the disclosure of classified information to trained foreign observers during cruises in nuclear-powered submarines.

Each of the following criteria must be met for an underway visit to be approved in this manner:

- The visit does not exceed two days in duration.
- Fewer than ten foreign visitors are involved.
- The names and titles of personnel to embark shall be forwarded to CNO (DCNO (Naval Warfare), Director, Submarine Warfare Division) at least one week prior to embarkation.
- The visitors are not heads of state, cabinet level, media, intelligence, naval nuclear propulsion program personnel, or representatives from industry or academia involved in research related to submarine design or construction.
- Visitors shall not have access to submarine weapons, other systems, or to information pertaining to those systems, except in accordance with previously established disclosure policy. If no policy for a specific system exists, a formal request shall be forwarded to Navy IPO-01 via CNO (DCNO (Naval Warfare), Director, Submarine Warfare Division).

* (3) As discussed in paragraph 20807(f), only the CNO or VNCO (or DCNO (Naval Warfare), Director Submarine Warfare Division, as delegated) may authorize visits by foreign nationals to Nuclear Propulsion Spaces or the disclosure of NNPI and/or RD/FRD. This authority may not be re-delegated. Visitors shall not have access to the Nuclear Propulsion Spaces of the submarine under any circumstances, unless the prior personal approval of the CNO or VCNO is obtained in advance.

(4) Only the CNO, VCNO, DCNO (Naval Warfare), or the Director, Submarine Warfare Division (OPNAV N77) may approve a foreign visit to an underway submarine by representatives of other governments, NATO, or NATO member governments that do not satisfy all of the requirements of paragraph 20807(h)(2) above.

i. **Technical Project Officers.** The Technical Project Officers (TPOs) of Data Exchange Agreements (DEAs)/Information Exchange Agreements (IEAs) are authorized to approve foreign visits within the scope of the TPO's Delegation of Disclosure Authority Letter (DDL) to

the institutions identified in the DEA/IEA. Prior to September 2005, these directly arranged visits approved by the TPO were often conducted outside of the FVS. TPOs may only approve visits by foreign representatives that have been submitted by their embassy through the FVS and consistent with all other provisions of this Manual and of the DON Information Exchange Program Guidelines for Technical Project Officers (“TPO Handbook”).

20808. Procedures for the Hosting Command

The host command’s foreign visit obligations include the following:

a. The final decision for hosting and scheduling a specific visit is at the discretion of the host command or facility and does not obligate them to host a visit or to disclose information.

b. With the exception of emergency visits, the pertinent foreign office or visitor(s) shall give the host activity at least 72 hours’ notice of the actual date and time the visit is intended, following approval of a visit. All activities have the right to refuse any visit if the visitor arrives without such advance notice.

c. The visit disclosure authorization (i.e., the FVS visit approval) will be transmitted to the security office of the activity or contractor facility to be visited by letter, fax or DMS message. The authorization will either approve the disclosure of CMI or CUI, or limit the disclosure to public domain information. The authorization must be disseminated to the U.S. government or contractor personnel who will actually host the visitor(s) at the facility. (Hosting commands should also note that nothing in this manual should be construed as granting authority to override any applicable security or other requirement issued in order to protect personnel, information, and property at the facility to be visited.)

d. The specific restrictions contained in an approved visit should never be disclosed to the visitor(s). The visitor(s) may be advised, however, of the highest overall level of classified information that will not be exceeded during the visit. Also, the visitor(s) must be advised of the classification level of any information actually disclosed so that the visitor(s) can properly protect it.

e. The disclosure authorization will set a classification level that cannot be exceeded during a visit. If the objectives of the visit can be accomplished by the disclosure of information at a lower classification level than that authorized in the visit approval notification, it is the responsibility of the host(s) to limit the disclosure accordingly.

f. If the host(s) determines that the purposes of the visit cannot be accomplished within the limits of the disclosure authorization, then the host(s) must communicate this directly to the authority that approved the visit, in order to seek resolution prior to the start of the visit.

g. A visit authorization does not include authority to release classified documents to a visitor, unless that authority has been explicitly granted within the disclosure authorization. If a request for classified documents occurs during the visit, it should be processed in accordance with the procedures for the release of documents, Part II, Chapter 11, of this manual.

h. Any unusually persistent effort by the visitor to obtain information that is not authorized for disclosure should be reported to the disclosure-approving authority.

i. The requesting embassy may amend the visit request but only with respect to the date(s) of the visit and/or the names of the visitors. If any other element of the visit request requires an amendment, a new visit request must be submitted. When a visit is amended the FVS is updated to reflect the amendment; however FVS does not notify the OPR automatically. The OPR should review the FVS "Amendment" folder on a daily basis to see if any cases have been amended.

j. The host command or facility shall appoint a contact officer for each foreign visit. The U.S. contact officer will also serve as the point-of-contact for the requesting embassy. The contact officer is responsible for controlling the activities of the foreign visitor(s) and for ensuring that the disclosure of CMI and/or CUI strictly conforms to that approved by the designated disclosure authority. The contact officer MUST be provided a copy of the visit authorization prior to the visit, and should verify with the OPR via chain of command that the list of visitors is current, including amendments.

k. Foreign Visitor Accountability. In order to ensure compliance with reference (bh), all DON Components are responsible for ensuring that all foreign personnel under their cognizance are screened for terrorist and criminal associations prior to arrival, and that their arrival and departure dates are documented in an automated system that feeds specific foreign visitor data into the DoD Cornerstone system. This requirement is considered to be met when a foreign visit request (FVR) is submitted into OSD's Foreign Visit System (FVS) and subsequently approved. It should be further noted that reference (bh) also requires that all DoD Components shall cooperate with DoD intelligence, counterintelligence, law enforcement, and security elements to ensure the stay of DoD-hosted foreign personnel is as secure and safe as possible for all parties.

PART II - CHAPTER 9

EXTENDED VISITS AND ASSIGNMENTS OF FOREIGN NATIONALS AND REPRESENTATIVES OF FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS

- Ref: (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1) (NOTAL)
(d) DoD Directive 5230.20
(t) Guide for Foreign Attaches Accredited to the Department of the Navy (NOTAL)
(af) DoD Directive 5530.3
(ap) OPNAVINST 5700.7G
(bf) National Telecommunications and Information Systems Security Manual (NTISSI) No. 3013

20901. General

This chapter implements reference (d) and governs extended visits of foreign nationals and representatives of foreign governments and international organizations to Department of the Navy (DoN) commands and activities.

20902. Policy

Foreign nationals and foreign representatives may be approved for extended visits to DoN facilities when assigned as a Foreign Liaison Officer (FLO), a Defense Personnel Exchange Program (DPEP) participant, as Cooperative Program Personnel within a cooperative program, or other capacities. Extended visitors shall have access only to that information that is necessary to accomplish their authorized duties and that has been authorized for disclosure to their sponsoring government. Foreign visitors may have access to U.S. Classified Military Information (CMI) or Controlled Unclassified Information (CUI) only after a visit request placed through the Foreign Visits System (FVS) by their sponsoring embassy or international organization has been approved and a valid disclosure authorization has been issued by a Designated Disclosure Authority (DDA) and transmitted to the host facility.

All DPEP and Cooperative Program Personnel assigned to DoN facilities shall sign a certification form indicating that they will comply with all limitations on their access to information and all security regulations designed to protect U.S. information. These certifications are enclosed in reference (d). Some FLOs may be required to sign a similar certification when a requirement is contained in the MOU that establishes the position.

Pursuant to Section 1082 of the National Defense Authorization Act for Fiscal Year 1997 (Public Law 104-201), training may not be conducted under the DPEP except as necessary to familiarize, orient, or certify DPEP personnel regarding unique aspects of the positions to which they are assigned. FLOs and Cooperative Program Personnel shall not receive training unless the U.S. Government is reimbursed for the costs of such training.

20903. Procedures

The visit request submission and processing requirements for extended visits are the same as those established for one-time, recurring, and emergency visits, (Part II, Chapter 8 of this manual) except all extended visits should be submitted a minimum of 45 days in advance of the commencement date of the assignment. A visit request is required for all extended visitors defined in this chapter. A Delegation of Disclosure Authority Letter (DDL) will not be issued unless a visit request has been submitted by the visitor's embassy or sponsoring international organization. The visit request will not be approved for an extended visit until a DDL has been issued. These requirements will be promulgated to the foreign embassies by issuance of reference (t).

Activities will ensure compliance with the contents of the DDL applicable to an extended visitor assigned to their activity. The contents of the disclosure authorization shall not be disclosed to the foreign visitor, with the exception of any certification form requiring the visitor's signature. This prohibition does not preclude the host from informing the visitor of the upper limit of the access being authorized during the assignment, in general terms. However, under no circumstances will specific disclosure limitations be revealed to the extended visitor.

a. Extended visitors shall be granted unescorted access to DoN facilities or areas of DoN facilities where access is controlled only when

(1) Security measures are in place to control access to applicable information and operations areas within the facility; and

(2) A badge or pass clearly identifies the bearer as a foreign national and is valid for the facility only during normal duty hours.

b. Extended visitors may be authorized access to any space for which they are appropriately cleared when the host facility's Commanding Officer has determined that they have an operational need. The Commanding Officer is ultimately responsible for securing any information within those spaces that is not releasable to the visitor.

c. The host command must ensure that the foreign visitor is clearly identified as a foreign national when dealing with others through oral, written, and electronic communications. If provided an email account, it must clearly identify him or her as a foreign national, including current assignment and country of origin. The email address shall comply with established DoD naming conventions. Specific and detailed guidance will be provided in the DDL issued.

d. The visitor shall not have access to automated information systems (AIS) unless all materials on the AIS are sanitized or protected such that the only materials available to the visitor are authorized for release to the visitor's parent government. Prior to granting access, compliance with local, DoN, and DoD information assurance and computer security guidance must be confirmed by the appropriately responsible local personnel. Specific and detailed guidance will be provided in the DDL.

NAVY FOREIGN DISCLOSURE MANUAL

e. Foreign visitors shall not have uncontrolled access to classified message traffic, library facilities, card catalogues, or databases. They shall not have access to bibliographies with listings of classified publications.

f. SIPRNET access is not authorized for any foreign visitor, regardless of the visitor's status.

g. Controlled access to a Secure Telephone Unit III (STU-III) may be permitted in accordance with reference (bf) including Annex C, provided the terminal is keyed for the visitor's classification level and a visual identifier denotes the user's status as a foreign national. The supervising official must ensure that the calling party or party called is informed of the extended visitor's access limits. Authority to authorize access will be contained in the DDL.

h. Foreign visitors shall only have access to cryptographic spaces, equipment, or material when authorized by the National Security Agency (NSA) or the Director of Central Intelligence (DCI) in coordination with Navy IPO and CNO (N6/N7).

i. Foreign visitors are not to take possession of classified information unless explicitly authorized in the DDL. They shall not have custody of CMI or CUI except during normal duty hours at their place of assignment, when the access is necessary to perform their assigned duties and when the information is authorized for disclosure.

20904. Procedures For Foreign Liaison Officer (FLO)

A FLO is a representative of a foreign military organization assigned by his or her government to a USN/USMC activity with DoN approval. A FLO works only for that foreign government and represents its interests to DoN. A FLO may not perform U.S. Government duties or responsibilities.

a. FLOs are further categorized into three types:

(1) Security Assistance FLOs may be assigned to DoN activities to oversee Foreign Military Sales (FMS) implementation. These assignments must be covered through either an FMS Letter of Offer and Acceptance (LOA) that establishes a FLO requirement or an international Memorandum of Understanding (MOU).

(2) Operational FLOs may be assigned as an interface between their command elements and a U.S. command in support of operational matters such as combined operations and planning. These assignments must be implemented via an MOU that establishes the FLO requirement. The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) shall be responsible for the establishment of Operational FLO MOUs for their respective Services. The authority to establish Operational FLO MOUs may be further delegated as deemed appropriate by CNO and/or CMC.

(3) National Representative FLOs may be assigned to their national embassy or diplomatic mission as military attachés to conduct liaison activities with DoN. These FLOs do

not require extended visit authorizations. They do require, however, an approved visit authorization per Part II, Chapter 8 of this Manual when making one-time or recurring visits to DoN facilities. However, an accredited attaché does not require an approved visit request if the purpose of the visit is for a courtesy call only. Substantive or technical discussions are not authorized during courtesy calls.

b. The MOU or LOA formally establishes the legal basis for the FLO position(s) and covers such matters as the responsibilities and obligations of the governments, authorized activities, security requirements, financial arrangements, and claims.

c. The duties of a FLO shall be limited to representational responsibilities for their government as described in the MOU or LOA governing their assignment. They shall not perform activities that are the responsibility of an employee of the U.S. command or facility to which they are assigned.

d. A FLO may not represent DoN in any capacity. A FLO may not enter into any contracts on behalf of DoN or the U.S. Government. They may not be provided nametags, badges, email addresses, codes, or titles that would imply that they are U.S. Government personnel.

e. FLOs may not assume custody of documentary information except as couriers. FLOs may only act as couriers when they are authorized in writing to serve their government as couriers and when the documentary information has been approved for release to their government.

f. A FLO may have access to U.S. CMI or CUI only after a DDL has been issued by a DDA.

g. Extended visit authorizations for a FLO will usually be limited to the command or activity to which the individual is assigned and any subordinate commands. All visits by FLOs to commands and activities other than the one to which they are assigned require the approval of a foreign visit request submitted by the visitor's sponsoring government or international organization.

h. Visits and assignments to shipyards will be in accordance with paragraph 20908.

20905. Procedures For Defense Personnel Exchange Program (DPEP)

The DPEP encompasses all of the exchange programs that include the assignment of foreign nationals to positions within DoD components under an approved billet or position description. Under the terms of a bilateral personnel exchange agreement, exchange personnel and host organizations share professional experiences, knowledge, and doctrine in order to strengthen the harmonious relationships between the respective Services of the participating governments.

NAVY FOREIGN DISCLOSURE MANUAL

a. For the purpose of this Manual, the following DPEP programs provide for the assignment of foreign nationals to DoN components:

(1) Military Personnel Exchange Program (MPEP). This program includes all assignments of foreign military personnel to authorized USN/USMC billets, normally on a reciprocal basis. In the USN, the MPEP is referred to as PEP, while in the USMC the MPEP is referred to as the Marine Corps Foreign Personnel Exchange Program (MCFPEP).

(2) Engineer and Scientist Exchange Program (ESEP). This program includes all assignments of civilian and military engineers and scientists to DoN Research, Development, Test, and Evaluation (RDT&E) facilities

(3) Administrative Personnel Exchange Program (APEP). This program includes all assignments of civilian and military specialist personnel to administrative, logistics, finance, health, legal, and planning billets within DoN.

(4) Defense Intelligence Personnel Exchange Program (DIPEP). This program includes all assignments of military intelligence analysts within DoN intelligence communities. The Director, Defense Intelligence Agency (DIA) has been designated as the Executive Agent for this program and is responsible for the promulgation of procedures consistent with references (d) and (af). All DIPEP assignments to DoN activities are coordinated through CMC (CIC) or the Office of Naval Intelligence (ONI) as appropriate. DDLs will be issued in accordance with DIA-provided direction and procedures.

b. Whether military or civilian, foreign personnel assigned to DPEP positions shall be treated as members of the U.S. workforce at the DoN host organization. They shall neither act as representatives of their parent government nor act as a conduit for the exchange of CMI or CUI.

c. DPEP participants shall not be assigned to positions that would result in their access to CMI or CUI which has not been authorized for release to their parent government or which exceeds the levels authorized for release by NDP-1.

d. DPEP participants shall not exercise responsibilities that are reserved by law or regulation for an officer or employee of the U.S. Government. For example, DPEP participants shall not perform the responsibilities of a contracting officer's representative (COR), contracting officer's technical representative (COTR), classified document custodian, security officer, escort for foreign nationals, or senior watch officer.

e. Navy IPO, or the applicable DDA identified in subparagraph a. above, shall conduct a disclosure review of each proposed billet/position description. One purpose of this review is to prevent a DPEP participant from being assigned to a billet in which a foreign national will be unable to perform a critical function due to disclosure limitations. Another purpose of the review is to prevent access to non-releasable information associated with non-critical functions. All disclosure issues must be resolved prior to the approval of the billet description.

NAVY FOREIGN DISCLOSURE MANUAL

(1) All proposed ESEP and APEP position descriptions are prepared by the host command and forwarded to Navy IPO via the applicable DDA.

(2) For MPEPs, the proposed billet/position description will generally be prepared by the host command and forwarded to Navy IPO via the Deputy CNO (Manpower & Personnel) (N130F) or HQMC, Manpower & Reserve Affairs (MPO 40), as appropriate. Navy IPO and CNO (Director, Politico-Military Affairs) shall review the proposed billet description for a MPEP billet prior to it being presented to the foreign government or international organization for their concurrence.

(3) Until such time as DIA promulgates direction and procedures for the DIPEP, CMC (CIC) and ONI are responsible for required disclosure actions associated with the establishment and assignment of foreign DIPEP personnel to USMC and USN activities respectively. For disclosure purposes, as a minimum, a DDL must be issued to each activity in which foreign DIPEP participants are assigned.

g. Extended visit authorizations for a DPEP participant will usually be limited to the command or activity to which the individual is assigned and any subordinate commands.

(1) For DPEP participants, visits to DoN commands or activities not subordinate to the host command and to appropriate DoD contractor facilities may be authorized and arranged by the individual's U.S. Contact Officer when the purpose of the visit falls within the scope of the visitor's billet description, using the guidance contained in the DDL and subject to paragraphs 20908 and 20909, if appropriate. The Contact Officer is authorized to communicate directly with the activity to be visited and arrange the visit, subject to that command's concurrence. The Contact Officer must ensure that the security office and the officials who will actually host the visit are provided a copy of the original DDL prior to the visit.

(2) For visits by DPEP participants to commands and activities that are for a purpose outside the scope of their billet description, the foreign visitor shall inform their embassy that a visit request is required. However, since DoD policy prohibits a DPEP participant from acting in the dual capacity as a FLO while assigned to a DoD component, such requests should be rare, and such a request will normally be denied except under very unique conditions.

20906. Cooperative Program Personnel

Cooperative Program Personnel are foreign nationals (military or civilian employees of the counterpart foreign government defense establishment(s)) assigned to bilateral or multilateral program offices that are hosted by a DoN activity as part of an international management team responsible for the implementation of a bilateral or multilateral project or program. For additional information on cooperative programs see Part II, Chapter 6.

a. To qualify as Cooperative Program Personnel, foreign government representatives

NAVY FOREIGN DISCLOSURE MANUAL

(1) must be assigned to an international program office hosted by a DoN component pursuant to the terms of an international agreement for armaments cooperation, and

(2) must report to and take direction from a DoD-appointed U.S. Program Manager (or Program Manager equivalent), and

(3) must NOT be foreign government representatives described as liaison officers or observers (such individuals shall be treated as FLOs, except as described in subparagraph c. below).

b. An international agreement for armaments cooperation shall generally describe or identify the functions of Cooperative Program Personnel assigned to the program. The DDL issued for the cooperative program shall govern the disclosure of information to Cooperative Program Personnel.

c. Cooperative Program Personnel shall not act in a dual capacity as an official/employee in the international program office and a liaison officer for their government (e.g., FLO) while assigned to a DoN component. In extraordinary cases, requests for exceptions must be accompanied by a request from the parent government of the individual and submitted in writing to Navy IPO by the pertinent international program office via the DDA in their chain of command. The request must contain sufficient justification as well as separate disclosure guidance and safeguards for the individual's two distinct roles. When justified, Navy IPO will seek formal approval from the Office of the Under Secretary of Defense (Policy).

d. Cooperative Program Personnel shall not be assigned to positions that could result in their access to CMI or CUI that has not been authorized for release to their government. Cooperative Program Personnel serving as couriers between the DoN and a foreign government for requests and transmissions of CMI and CUI shall act in accordance with the terms of the cooperative program's Program Security Manual.

e. Cooperative Program Personnel shall not be assigned to positions reserved by law or regulation for an officer or employee of the U.S. Government. For example, they shall not perform the responsibilities of a U.S. contracting officer's representative (COR), component duty officer, classified document custodian, security officer, or escort for foreign nationals.

f. U.S. Contact Officers must be assigned to all foreign Cooperative Program Personnel and shall ensure compliance with the requirements contained in the DDL.

g. Extended visit authorizations for Cooperative Program Personnel will usually be limited to the command or activity to which the individual is assigned and any subordinate commands. All visits by Cooperative Program Personnel to commands and activities other than the one to which they are assigned require a visit request be submitted by the visitor's embassy.

h. Visits to shipyards will be in accordance with paragraph 20908.

20907. Other Extended Visits

In rare circumstances, Navy IPO may issue a disclosure authorization for an extended visitor who is not a participant in one of the established programs discussed in this chapter. This will occur only after careful review and determination by Navy IPO that it is in the best interests of the U.S. to do so. For example, an extended visit request may be approved to support the assignment of employees of a foreign contractor to a cooperative project when the foreign contractor is directly under a DoN contract. Disclosures for this example would be in accordance with terms of the cooperative program DDL.

20908. Visits to Navy and Commercial Shipyards

a. Shipyards. The Commander, Naval Sea Systems Command (COMNAVSEASYSCOM) has been delegated exclusive authority for approving official visits to all DoN and commercial shipbuilding and repair facilities. Foreign personnel assigned to an afloat command, however, can anticipate short, unscheduled shipyard visits in the course of their assignment. The prior approval of COMNAVSEASYSCOM is required for foreign personnel to enter a shipyard or repair facility. See paragraph 20806b. for further details.

(1) DPEP participants with shipboard assignments. If a short shipyard visit is imminent, the Contact Officer shall make direct contact with COMNAVSEASYSCOM (Security Office) to secure the entry of DPEP participants assigned to a ship or submarine. If the Contact Officer cannot obtain authorization for DPEP participants to accompany the host command into a shipyard, the host command shall contact CNO (N130F) or CMC (I) to coordinate a temporary transfer. Navy IPO will provide additional assistance only if direct liaison with COMNAVSEASYSCOM is not feasible.

(2) FLOs and Cooperative Program Personnel. Prior to arrival at the shipyard, the FLO or Cooperative Program Personnel must arrange to have a formal visit request submitted by his or her embassy to obtain authorization for entry. This request should be submitted a minimum of 21 working days in advance of the arrival, and preferably sooner if at all possible.

20909. Visits to U.S. Government Facilities other than DoN

The U.S. Contact Officer is authorized to arrange visits by DPEP participants to the commands and activities outside of the jurisdiction of DoN when those visits are within the scope of the visitor's billet description. The Contact Officer shall comply with the procedures of the host organization in order to secure its authorization for the visit. Prior to the visit, the Contact Officer must provide the security office and the officials who will actually host the visit a copy of the original DDL issued for the DPEP's assignment. In some instances, the host organization will require that an official foreign visit request be submitted by the DPEP's embassy into the Foreign Visit System (FVS).

PART II – CHAPTER 10

DISCLOSURE TO FOREIGN NATIONALS IN NAVAL TRAINING

Ref: (c) DoD Directive 5230.11
(f) AECA

21001. General

Students representing a foreign country, including military personnel, contractors, or government representatives (herein referred to as “foreign students”) may take part in DoN training. Any Classified Military Information (CMI) presented to foreign students must first be authorized for foreign disclosure by the Navy International Programs Office’s Technology Assessment, Exchanges and Disclosure Division (Navy IPO-01B) or a DoN Designated Disclosure Authority (DDA).

Section 47(5) of reference (f) defines training as formal or informal instruction of foreign students in the U.S. or overseas by officers or employees of the U.S. Government, contract technicians, and contractors (including manual at civilian institutions). Training methods include correspondence courses; technical, educational or information publications/media of all kinds; training aids; orientations; training exercises; and military advice to foreign military units and/or forces.

Care should be taken to ensure that foreign students are not given access to information, material, equipment, or capabilities not approved for disclosure to their government. Any sensitive, unique, or U.S.-only features of any weapons, systems, or equipment used or referenced in the training of U.S. personnel, but not approved for disclosure to the foreign student’s government, must be protected from inadvertent disclosure.

21002. Policy

a. Foreign students may **receive** training on U.S. equipment, weapons, or systems (herein referred to as “equipment”) that involves the disclosure of CMI if the equipment is already in the inventory of the foreign government, or if there is an expectation that the equipment will be acquired. The DoN accepts the “expectation provision” as met when the foreign government has concluded an international agreement or signed a letter of offer and acceptance (LOA) with the U.S. to acquire the equipment or training. The Navy International Programs Office, Technology Security and Cooperative Programs Directorate (Navy IPO-01), may authorize, on a case-by-case and country-by-country basis, training on equipment not in the receiving country’s inventory or where there is no expectation for acquisition if such training is accompanied by substantial justification from the proponent and is in the best interest of the U.S.

b. Foreign nationals may **conduct** training on U.S. equipment if the item has been sold or approved for disclosure to the foreign national’s government. Care should be taken to ensure

NAVY FOREIGN DISCLOSURE MANUAL

that foreign nationals are not given access to information, material, or capabilities not approved for disclosure. Disclosure approval does not imply equipment or training facility availability.

c. Tactics training by DoN schools shall be limited to the content and scope of tactical publications approved for release to the receiving country or as authorized by the Naval Component Commander with cognizance over the receiving country's normal areas of operation.

d. Foreign students scheduled to receive security assistance training within the DoN must have an Invitational Travel Order (ITO), form DD2285, issued by the U.S. Security Assistance Office (SAO) in their country or the cognizant U.S. activity if the foreign student is stationed in the U.S. The Foreign Visit System (FVS), detailed in Part II, Chapter 8 of this Manual, shall not be used as a vehicle for scheduling or providing disclosure authorization for security assistance training. The Naval Education and Training Security Assistance Field Activity (NETSAFA) and the Marine Corps Training and Education Command (TECOM) shall direct DoN schools to deny training on any classified curriculums that have not been reviewed and received a formal disclosure authorization.

e. Foreign students will not be authorized to receive Communications Security (COMSEC) information or cryptographic equipment maintenance training unless permitted under the provisions of the cryptographic equipment's release to the student's parent government.

f. Foreign students shall not be permitted to enroll in courses involving Atomic Information (Restricted Data/ Formerly Restricted Data (RD/FRD)) or Naval Nuclear Propulsion Information (NNPI), classified or unclassified, unless Navy IPO-01 specifically authorizes their access to such information.

g. DoN activities responsible for the development and/or operation of computer-based training devices that are potentially applicable to a Foreign Military Sales (FMS) program or to foreign training in general, should, to the greatest extent possible, design and develop such systems in a modular fashion or in a fashion that may be easily tailored or sanitized. Training courses whose curriculums are upgraded from hard copy to computer-based systems, and that have a history of curriculum presentation to foreign students, must have computer-based training devices designed and developed in a manner capable of tailoring or sanitizing course content for foreign students.

h. The training disclosure process will not normally be used as a method for permanently transferring hard copy versions of CMI to foreign governments via their students. As such, foreign students are not eligible for enrollment in classified DoN correspondence courses or extension courses.

21003. Procedures for Classified Training Disclosure Reviews

The procedures outlined in this paragraph apply to formal schoolhouse training courses, structured on-the-job training courses, and mobile training team curricula provided to foreign students. NETSAFA or TECOM will not confirm foreign student training quotas for DoN

NAVY FOREIGN DISCLOSURE MANUAL

classified courses until each course has undergone a disclosure review and a Delegation of Disclosure Authorization Letter (DDL) has been issued to the school.

a. Once it is proposed that a foreign student attend a classified DoN training course, NETSAFA/TECOM shall instruct the cognizant school to upload the normal course content (the curriculum taught to USN/USMC students) into the Navy IPO Foreign Military Training (FMT) website (<https://www.nipo.navy.mil/fmt>). Following upload, DoN commands and activities with a potential interest in the information proposed for disclosure may be asked to review the course content. Reviewer responses may range from recommending the course be taught, “as is,” to sanitizing specific content, to recommending the complete removal of certain material. Navy IPO or TECOM shall consolidate the responses and provide the school a delegation of disclosure authority letter (DDL) for the course, specific to the country(ies) proposed for attendance. Navy IPO shall provide a copy of their training DDLs to NETSAFA. TECOM shall provide a copy of their training DDLs to Navy IPO-01B.

b. When changes are made to the normal course content of a course previously attended by a foreign student, only the changed items are reviewed for disclosure and the previously issued DDL will be amended if appropriate.

c. When an additional country proposes to attend a course that has previously been authorized for foreign students from other countries, the addition of the additional country must be reviewed by the cognizant DoN DDA, who will determine if a complete review of the course content by other commands and activities with a potential interest in the information proposed for disclosure is required. The DDL for the course shall be updated if appropriate.

d. DoN schools are to avoid the proliferation of bibliographic and reference material pertaining to classified information that is clearly not releasable to the parent governments of the foreign students receiving training. The disclosure or release of bibliographies and lists of classified documents is discouraged unless each classified document listed is determined to be releasable.

e. DDLs for classified training courses will contain certain standard language:

(1) “Disclosure will be on an oral and visual basis only. Oral and visual disclosure is defined as to brief orally, expose to view, or permit use under U.S. supervision in order to permit the transfer of knowledge or information. Oral and visual disclosure does not allow the physical transfer of documents, material, or equipment to a foreign government or its representatives.”

(2) “Classified manuals and reading material provided to international students must remain under U.S. control at all times. Unmonitored access by students is strictly prohibited. In order to comply with these restrictions, a monitor must be physically present in the classroom or labs when international students use or have access to classified manuals and reading material.”

(3) “International students must be briefed that all controlled unclassified manuals and reading material provided to them must remain under their control at all times; that it may not be copied, reproduced, or distributed to anyone else, and that all controlled unclassified material must be returned to the school at the conclusion of the training course.”

(4) “Disclosure is limited to the information, publications, training aids, equipment, and other materials provided [in the FMT database] for this course with the following restrictions: [as appropriate].”

21004. Other Training Disclosure Procedures

a. Unique Curriculum Development. As U.S. technology continues to improve at a different rate than that of our friends and allies, information that may have been disclosed in the past might no longer be appropriate for disclosure in the present or future. In such cases, an offer to provide training may require retraction when the teaching aids and systems cannot be modified to accommodate foreign training. DoN activities participating in discussions and proposals for foreign training should concentrate their discussions on the foreign government’s training objectives (vice attendance at specific DoN courses). If an initial review of the proposed training determines that a substantial amount of the course content may require removal for a particular country, or if a computer-based curriculum cannot be sanitized, then a unique course for that country may be required. Creation of the new course would be at the receiving country’s expense.

b. Sale of DoN Course Curricula. In general, the DoN discourages the sale of course curricula to foreign governments, particularly if the curricula include U.S. classified information. Once sold, the DoN loses both configuration control over the content as well as the interoperability and cross-cultural experience gained by foreign student attendance at DoN schools. In cases where a sale is justified, Navy IPO-01B will require written certification from all DoN activities with cognizance over the course content that they have reviewed the material and have no objection to its release.

c. Student Notes. Student notes (which may be written in any language) and other training material (unclassified or classified that falls within the disclosure authorization) may be returned to the student at the conclusion of the training course as described below.

(1) At the discretion of the commanding officer of the training activity, student notes derived from unclassified courses will either be given to the student or be forwarded directly to an address designated by the student. Postage is the responsibility of the student or his or her government.

(2) Student notes derived from classified courses will be reviewed and marked with the appropriate U.S. security classification markings. Student notes that cannot be reviewed because they are written in a foreign language should be marked with the highest classification of information released during the course. All classified materials will be conspicuously marked by stamp, or other means, to indicate the (1) highest classification of included material, (2) date review completed, (3) name and rank of reviewing official, (4) name of cognizant activity, (5)

NAVY FOREIGN DISCLOSURE MANUAL

training course involved, and (6) student's name and service. After being marked appropriately, the classified material will be forwarded directly to the SAO in the student's parent country for further transmittal to the foreign government. In the case of ship's crew training, classified student notes may alternatively be delivered directly to the ship. All students will be cautioned that classified notes must be safeguarded in a manner appropriate to the classification. Classified material, which contains COMSEC information, must be forwarded via Commander, Naval Security Group (COMNAVSECGRU) who will forward the material to the appropriate authority in-country.

PART II - CHAPTER 11**DISCLOSURE OF DOCUMENTARY INFORMATION**

- Ref: (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1) (NOTAL)
(i) SECNAVINST 5510.36

21101. General

The purpose of this Chapter is to provide guidance for the disclosure of any information capable of being printed or published on paper or saved in any electronic format. Documentary information includes directives and other publications, correspondence, spreadsheets, databases, graphical slides, briefs and briefing notes, technical drawings, photographs, film or videotapes, audio recordings, software code, etc., that convey Classified Military Information (CMI) or Controlled Unclassified Information (CUI) material or information. For the purposes of this chapter, we will generally refer to documentary information as “documents.” In general, the disclosure of documents is of particular concern because they are easily referenced, reproduced, or passed to a third party.

21102. Policy

Documentary disclosure requests must be closely reviewed for both benefit and risk to the U.S. These requests must be evaluated in the context of established international programs (e.g., Foreign Military Sales (FMS) or International Agreements) and national, DoD, and DoN disclosure policies, when such exist. Disclosures will be limited to the information that minimally satisfies the purpose of the disclosure, if necessary by sanitization. Automatic distribution of classified DoN material to foreign entities is not authorized. DoN information deemed to be in the public domain by a DoN Public Affairs Officer should be released without a foreign disclosure review.

21103. Procedures for Reviewing Documents

The DDA should closely review the purpose and justification of the release, the information proposed for disclosure, and all relevant DoN and national disclosure policies. In those cases where a disclosure request exceeds the DoN or National Disclosure Policy, a less sensitive document may be proposed as a substitute to satisfy the requirement.

a. Review of Documents (General). Documents, excluding Naval Warfare Publications, may be released in accordance with the terms of established international programs (e.g., Foreign Military Sales (FMS), international cooperative research and development, or Data/Information Exchange Agreements). The information contained in these documents must be within the scope of the program, within the program’s delegated disclosure authority (if applicable), and satisfy the program’s purpose. Documents may also be released for the purpose of informing allies and coalition partners about DoN organization, personnel, operations, facilities, programs, and activities.

NAVY FOREIGN DISCLOSURE MANUAL

(1) Documents will not normally be released without the consent of the originator and other offices with cognizance over the subject matter.

(2) If a document, excluding Naval Warfare Publications, is for information only, is requested on a one-time basis, or is not part of an established international program, it must contain a false impression statement printed or stamped on the inside cover or in a prominent location using the wording contained in paragraph 21109.

(3) After consummating a sale, lease, loan, or grant of a DoN-sponsored weapon, system, or piece of equipment, documentary information may be disclosed to the receiving country on a government-to-government basis to include information up to the level necessary for operation, basic employment, maintenance, and training, but not tactical employment information. The exact information disclosure limits are normally stipulated in the Technology Transfer and Security Assistance Review Board (TTSARB) decision or the export license, as appropriate. Tactical employment information may only be authorized for release by Delegated Disclosure Authorities (DDAs) at the Naval Component Commander level or higher.

(4) The DoN does not automatically distribute to foreign governments new or revised publications that contain CMI or CUI, even when those foreign governments have received previous versions of those publications. The release of documentary information to foreign entities does not imply or guarantee that future updates, modifications or alterations (or in the case of publications, changes, corrections or new editions) may be released. Any updates, modifications or alterations must be treated as new releases, which require a disclosure authorization on a case-by-case basis by a DDA. There are two exceptions: multinational manuals specifically designed for international distribution and cooperative program manuals written for international participants by the cooperative program office. Other exceptions to allow automatic distribution of a document series may be approved only by Navy IPO-01.

(5) DDAs performing a disclosure review of documents previously released to a given country, but subsequently revised, modified, updated, or corrected will focus their review only on the revisions or changes unless otherwise warranted. The unchanged portions of the document may be presumed to be approved for release based on precedent.

(6) If required, documents must be sanitized according to the procedures outlined in paragraph 21103. The DDA approving or denying the request shall ensure that each documentary release decision, along with any sanitization instructions, are recorded in the DoD Classified Military Information (CMI) database according to the provisions of paragraph 21602. Failure to record this information may result in the duplicate staffing if future requests are received for the identical document. Naval Warfare Publication sanitization instructions must also be provided to Navy IPO and recorded in the Navy Tactical Publications Disclosure Database (NTPDD).

b. Review of Naval Warfare Publications, Allied Warfare Publications, and Other Tactical Publications.

(1) Naval Warfare Publications. Certain classified and unclassified Naval Warfare Publications may be released to foreign governments. These releases are subject to the limitations imposed by reference (a), Navy disclosure policies, and the sanitization guidance contained in the SIPRNET-based Navy IPO NTPDD. (This database contains current releasability data on specific publications and is available at www.nipo.navy.smil.mil/comtac.)

(a) If a command wants to disclose a Naval Warfare Publication or information contained within it, that command should consult the NTPDD. The NTPDD will indicate whether the publication has previously been approved for disclosure to various countries. NTPDD will indicate whether a publication has been approved for hard-copy release, oral/visual disclosure only, or a sanitized form of either. If there is no entry in the database, this signifies no current authority to disclose information to that country; the command proposing disclosure may submit a request via the DDA in its chain of command to Navy IPO (IPO-01B2). The request should include detailed justification and should identify whether the disclosure will be in hard copy, electronic copy, or by oral/visual means only. The request will be processed using the procedures outlined in this chapter.

(b) Authorization to disclose information from a Naval Warfare Publication applies only to the specific version of the document indicated in the NTPDD. If the document proposed for disclosure is older or newer than the version listed in the database, or if the document has been revised, re-categorized, or otherwise changed since the most recent sanitization instructions were issued, then the entry does not authorize disclosure.

(c) The DoN does not automatically distribute new or revised Naval Warfare Publications to foreign governments, even when they have received previous versions of that publication. A DDA must review and authorize a new or revised publication for disclosure before it may be provided to a foreign government.

(d) Hard-copy or electronic-copy releases should only be considered when temporary oral/visual disclosure cannot adequately satisfy the request. Only a DDA or Navy IPO may authorize the release of hard-copy or electronic-copy Naval Warfare Publications.

(2) Classified Allied Doctrine Publications. A command may disclose an Allied doctrine publication, in the version and format stipulated in the NTPDD, when the publication has been previously authorized for oral/visual disclosure or release to the proposed recipient government. Proposals to release Allied doctrine publications to countries that do not have a release precedent indicated within the NTPDD require the approval of the cognizant multinational authority. Requests of this nature will be submitted via the chain of command to the Navy Warfare Development Command (NWDC), Tactical Doctrine Program Manager, 686 Cushing Rd., Sims Hall, Newport, R.I., 02841-1207, with a copy to Navy IPO (IPO-01B2). NWDC will then coordinate with Navy IPO and the cognizant control authority to obtain a disclosure decision. Sponsors of such requests should ensure that their proposal is written so that the members of the multinational organization can easily understand the request and that it

NAVY FOREIGN DISCLOSURE MANUAL

contains complete and understandable justification for the release. Since approximately three months will be required to process each request, it should be submitted to NWDC as far in advance of the proposed release date as possible.

(a) The supporting rationale must

i. Identify the objectives to be accomplished by the release. If the objectives are not in direct support of a NATO-approved activity, then the activity must be described in detail;

ii. Identify the specific information that is the minimum necessary to meet the requirements that necessitate the release.

iii. Describe the benefits that will accrue to the alliance (not merely to the U.S.);

iv. Explain why, if a releasable EXTAC publication or Multinational Manual exists, the release of that publication is insufficient;

v. Verify that an appropriate security agreement is on file at the NATO Office of Security; and

vi. Describe how, in the case of oral/visual disclosure, the information will be safeguarded.

(b) All NATO publications are automatically releasable to NATO countries. Any U.S. supplements to these publications must be reviewed by a DDA prior to disclosure to any foreign government. Publications releasable to NATO are not presumed to be releasable to other treaty Allies that are not members of NATO.

(c) The NATO Multinational Manual series has been created for the express purpose of distribution to non-NATO militaries. These manuals may be released to a non-NATO member by the fleet commander with cognizance over the receiving country's normal Area of Operational Responsibility. These manuals do not require sanitization or special markings prior to release.

(3) TACMEMOs, TACNOTEs, and LESSONS LEARNED. These publications are written with the understanding that they are internal DoN documents reflecting experimental tactics and/or lessons learned, and do not reflect approved DoN doctrine. They originate from diverse commands throughout the DoN providing field commander's comments on new tactics or procedures, or deficiencies in current doctrine, and often with an unknown or untested consequence on official doctrine. Their unofficial nature provides good reason to limit their widespread foreign dissemination. Tactics, however, may be released at the discretion of Naval Component Commanders and there may be occasions when new or experimental tactics may warrant release. Naval Component Commanders are encouraged to coordinate any release of

TACNOTEs and TACMEMOs with their counterparts in other theaters in order to assess the broader consequences of the release, if any.

c. Review of Briefings and Other Documents for Meetings, Symposia, Seminars, Conferences. No foreign national shall be invited to any meeting whether in the U.S. or abroad with the potential for disclosing U.S. CMI or CUI until an appropriate DDA has completed a review of the information to be discussed or presented and has issued a disclosure decision and guidance. The disclosure authorization will normally restrict the information or presentation to that level and those subjects approved for all countries in attendance (“the lowest common denominator”).

(1) Disclosure reviews of briefings prepared by individuals unfamiliar with a topic’s disclosure limits are one of the more difficult types of disclosure reviews performed by DDAs. The person preparing the brief often does not account for all of the information to be presented and expects the DDA to anticipate the actual disclosures based upon the briefing slides alone. It is incumbent on the DDA to orient their personnel on the procedures to use for preparing briefs intended for foreign audiences. Such an orientation may allow DDAs to better explain their role and expertise in the field of disclosure, and to explain that they are not subject matter experts in the myriad of fields within the Department of Defense.

(2) The following items should accompany each brief submitted for a disclosure review:

(a) The purpose of the brief (be as specific as possible), including the four or five key points that the briefer intends to convey to the audience.

(b) The audience to receive the brief, including positions, nationalities, and technical competencies.

(c) Proposed disclosure limitations (general and specific).

(d) The entire presentation including speaker notes and source listing (if applicable).

(e) Anticipated follow-on questions and answers.

(f) The location of the brief. Classified briefs must be given in government or contractor facilities cleared to the level of classification of the brief. (Foreign government or their contractor facilities are also acceptable briefing locations so long as the facility is cleared to the comparable U.S. classification level and the country has an active classified information protection agreement (e.g., GSOMIA) in place with the U.S..) Classified briefs are not permitted in uncleared spaces or in hotel ballrooms or meeting facilities.

(3) As with other disclosure reviews, DDAs should staff CMI and CUI briefs for review to the command with original classification authority or with primary responsibility over a document, in addition to other subject matter experts (“reviewers”). Their comments should be

NAVY FOREIGN DISCLOSURE MANUAL

factored into the DDA's disclosure decision. A consensus disclosure decision is generally desired.

(4) The disclosure of U.S. CMI at multinational classified forums for the sole purpose of providing parity with foreign participants who are providing classified briefs is not sufficient justification to warrant a disclosure authorization.

(5) DDAs shall not authorize the briefing of information, even at the unclassified level, about systems that are not authorized for release to the recipient country. Only Navy IPO may authorize such briefings. Such briefs must contain an untitled slide – normally immediately following the title slide – with the false impression statement contained below.

(6) DoD distribution statements or export control statements located on the cover slide of a brief shall be removed prior to disclosure to a foreign audience.

(7) Briefs intended for oral/visual disclosure shall be footnoted on the cover or false impressions slide, "Paper or electronic copies of this brief are not authorized for release."

(8) False Impressions Statement. All levels of the chain of command must ensure that DoN activities avoid creating a false impression of the U.S. Government's willingness to make available military materiel, technology, or information to friends and allies in advance of obtaining all necessary disclosure approvals for the overall program or issue. Although it is preferable that all necessary disclosure approvals be obtained in advance of providing any information on a program or issue, it is recognized that exceptions do arise. Navy IPO-01 is the only approving authority for such exceptions within the DoN. All disclosures approved in this fashion must contain the following warning to the foreign audience:

This [brief or document or information] contains references to U.S. Government military capabilities that may not be authorized for release to foreign governments. Mention of these capabilities in no way implies that the U.S. Government will release or consider release of them, or of any additional associated classified or unclassified information pertaining to them. This [brief or document or information] may also contain references to U.S. Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments.

d. Updates and Creation of New Publications

(1) Some DoN publications, such as tactical or procedural manuals, are generally known to be of interest to foreign governments. Originators of these documents should keep in mind the strong likelihood of foreign release, while they are creating or revising such DoN publications. In particular, originators are encouraged to identify and maintain records concerning those portions that they anticipate would be for U.S. use only and would only be released to foreign governments under extraordinary circumstances. The originators of such

DoN publications should avoid creating documents that are impossible or impractical to sanitize. Designated Disclosure Authorities (DDAs) and the originators of new documents are strongly encouraged to work together to facilitate this process.

(2) When creating or updating publications, the use of “Not Releasable to Foreign Nationals (NOFORN)” and related markings must be appropriately observed. The application of NOFORN and similar markings has been widely misunderstood. The use of the NOFORN marking shall not be used except as authorized by reference (b), namely for certain types of military intelligence and for Naval Nuclear Propulsion Information (NNPI).

(a) When properly applied, NOFORN markings are used to identify intelligence that the originator has determined may not be disclosed or released without originator’s approval, in any form, to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens. The application of the marking does not necessarily imply that the material could not be authorized for release by appropriate intelligence disclosure authorities.

(b) NOFORN shall not be used simply to attempt to restrict information from foreign disclosure. Conversely, the absence of the marking does not imply that it is acceptable to automatically release the material to foreign governments.

(c) The NOFORN marking may be used for NNPI. In light of the national policy prohibiting foreign disclosure of NNPI, special distribution control markings are used on correspondence and documents containing classified or unclassified NNPI.

(d) Documents or correspondence containing CMI and CUI, other than intelligence and NNPI, may apply one of the following warnings in lieu of a NOFORN marking:

i. A distribution statement in accordance with Exhibit 8A of reference (i). Distribution statements are applied to the first page footer of documents. Distribution statements may be applied to documents, correspondence, or other written products regardless of whether there is technical content or not, if the intent is to control the distribution of the document. Distribution Statement B (U.S. Government agencies only) and Distribution Statement D (DoD and DoD Contractors only) are the most common distribution markings.

ii. Any of the notices or markings listed in Chapter 6 of reference (b) as appropriate.

iii. A warning in paragraph 1 or the closing paragraph of the correspondence, preferably as bold text, such as:

"1. (U) THE CONTENTS OF THIS [LETTER/ENCLOSURE/ETC.] ARE NOT AUTHORIZED FOR DISCLOSURE TO FOREIGN PERSONNEL OR REPRESENTATIVES OF FOREIGN GOVERNMENTS."

or

"This document is not releasable to foreign nationals. It contains information exempt from mandatory disclosure under FOIA. Exemption (B) (2) applies."

21104. Procedures for Staffing Documents

Normally, a review of a document proposed for release to a foreign government shall reflect the consensus of the commands with cognizance over the subject matter to be disclosed (e.g., SYSCOM, OPNAV resource sponsor, Office of Naval Research, Fleet tactics squadron). The command with original classification authority or with primary responsibility over a document, in addition to other subject matter experts ("reviewers"), shall perform the review of the request, including contributing to the development of sanitization manuals, for the subject document. The command that performs the sanitization will use the procedures outlined in paragraph 21105 to modify the document prior to release.

a. DDAs, when requesting reviewers to provide input on a document's releasability and to develop sanitization manuals, should provide each reviewer some disclosure guidance to assist in the review. This guidance may include past disclosure precedents, DoN or DoD policies, or the delegated disclosure limits specified by reference (b), as appropriate.

b. In accordance with referene (b) disclosure criteria, the disclosure of information shall be limited to the minimum necessary to accomplish the purpose for the disclosure. Therefore, the release of documents requires the removal of unnecessary information. DDAs should inform reviewers that if they propose sanitization manuals, it is often preferable and more practical to delete entire chapters or sections of a document before deleting specific paragraphs, sentences, or words. Discretion must be used when applying this rule. For instance, it is not acceptable to delete an entire section because one sentence or paragraph refers to non-releasable information. However, if a chapter primarily covers a specific subject that is not authorized for disclosure, then delete the entire chapter.

c. Reviewers should be informed that the casual mention of weapon systems or equipment not authorized for release may be appropriate, in accordance with the conditions of subparagraph 21105(b).

21105. Procedures for Sanitization of Documents

The disclosure of documents often requires text, charts, graphs, and even entire sections to be removed before being provided to foreign governments. In the DoN, this procedure is generally termed "sanitization."

a. Sanitization may be accomplished in a variety of ways:

(1) Entire pages, chapters, or sections may be completely removed from the document. Whenever possible, this is the preferred method. Alternatively, exact words, sentences, paragraphs, or portions of pages may be removed from the document. This alternative

may result in a more useful document but is labor-intensive and requires an extensive knowledge of the information being reviewed.

(a) When hard-copy documents are sanitized, the proper procedure is to blank out the non-releasable information completely and then reproduce the page in its sanitized form. Use of this technique should not allow the reader to see non-releasable information. It is important that the reverse side of a sanitized page must also be reproduced if the intent is to keep the document flowing like a book. The sanitized pages are then substituted for the original pages. This is an expensive and time-consuming procedure and is not normally feasible.

(b) Electronic documents may be edited, then printed from the source computer file with the non-releasable portions of the document removed. There is some concern that electronically editing a computer file and then saving the edited file to a disk or CD-ROM may not completely sanitize a document, because the recipient may have the technological capability to restore the original file from the sanitized version. Printing the edited file to paper is the safest means to deliver a sanitized electronic document.

(2) Under no circumstances shall sanitization be attempted by marking out non-releasable portions (i.e., using pencil, ink, tape, etc.), since that is not an effective means of removing information.

(3) In all cases, the table of contents, indices, lists of effective pages, etc., must be appropriately sanitized to remove references to deleted portions of a sanitized document. Additionally, reference lists, bibliographies, and distribution lists should be removed unless all of the documents identified have been reviewed and determined releasable. Requests for the disclosure of documents that are reference lists or bibliographies should normally be denied.

(4) A sanitized document shall add the subtitle “(Edited for *Country Name*).”

b. Under certain circumstances, the casual mention of weapon or system names for weapons or systems that are not authorized for release may be authorized when to remove such references would be resource intensive. This type of casual mention is generally unclassified and should reveal no system vulnerabilities, performance parameters, or specific variants released to foreign countries, and does not violate any DoN or DoD policy concerning the mentioned weapon or system.

c. If the document contains non-releasable information and its removal is not feasible (e.g., the sanitized document would not serve the intended purpose, or it is impossible to eliminate the non-releasable content), then the request for disclosure of that document must be denied.

21106. Procedures for Document Transmittal

a. Marking. Any CMI or CUI document authorized for release to a foreign government shall be marked on the cover or the first page inside the cover with the following statement prior to transmittal:

"This information is furnished upon the condition that it or knowledge of its possession will not be released to another nation without specific authority from the Department of the Navy of the U.S.; that it will not be used for other than military purposes; that individual or corporate rights originating in the information, whether patented or not, will be respected and; that the information will be provided the same degree of security afforded it by the Department of Defense of the U.S.. Regardless of any other markings on this document, it may not be declassified or downgraded without the written approval of the originating U.S. agency."

The marking above is in addition to any classification or special handling markings that may be required in accordance with other applicable directives. In addition, the subtitle marking "(Edited for *Country Name*)" must be included on the title page or equivalent of sanitized documents. The responsibility for applying this marking rests with the office or command performing the sanitization and shall be verified by the releasing authority.

b. Classified information that has been determined by a DDA to be releasable to a foreign government or international organization may be marked with the "REL TO" control marking and an approved trigraph (three letter) or tetragraph (four letter) country code. The "REL TO" marking was previously only authorized for use on intelligence information but has now been approved for all classified military information. References (i) and (y) will be updated to provide specific guidance on the use of the REL TO marking on DoN and DoD documents. Interim guidance can be found at the CNO N09N2 website at www.navysecurity.navy.mil

c. CMI or CUI transmitted via in-country DoN or DoD liaison personnel and addressed to the foreign government may be delivered to that government if the material is accompanied by a release authorization from Navy IPO-01 or a DDA and the appropriate markings have been applied.

21107. Alternate Procedures for Disclosure of Documents to Foreign Governments

a. Defense Technical Information Center (DTIC). DTIC is the central DoD activity for providing access to and facilitating the exchange of scientific and technical information. DTIC offers a wide variety of products and services designed to assist its users, including foreign entities, in obtaining the information they need. Although DTIC has no disclosure authority for DoN information, they have established a streamlined process for the handling of disclosure requests for classified, unclassified, and limited distribution documents in the DTIC library collection for several closely allied countries including Australia, Canada, France, South Korea, the Netherlands, and the United Kingdom. DTIC uses "DTIC Form 55B" as the cover sheet for controlling the streamlined release process, which includes:

(1) DTIC forwards a copy of any classified or distribution statement limited documents to a DoD activity with cognizance over the document to coordinate a disclosure review.

(2) The reviewing offices will follow the procedures in paragraph 21103 to review the release request and sanitize the document as necessary. If the reviewer is a DDA, then the disclosure may be approved at that level, recorded on the DTIC Form 55B and returned to DTIC and recorded in the Foreign Disclosure System. If the reviewer is not a DDA, or if denial is recommended, then the package should be forwarded to the cognizant DDA for action based upon the reviewer's recommendation and sanitization manuals.

b. U.S./Canada Joint Certification Program (JCP) (reference (bb)). The Joint Certification Program benefits both U.S. and Canadian defense and high technology industries by facilitating their access to unclassified critical technology in the possession or under the control of the U.S. DoD or Canadian Department of National Defence (DND). Certification under the JCP establishes the eligibility of a U.S. or Canadian contractor to receive unclassified technical data governed in the U.S. by reference (bg), "Withholding of Unclassified Technical Data From Public Release," and in Canada by the "Technical Data Control Regulation (TDCR)." The U.S./Canada Joint Certification Office (JCO) is located at and managed at the Defense Logistics Services Center, Battle Creek, Michigan.

(1) Both U.S. and Canadian contractors agree that as a condition of receiving DoD or DND controlled technical data, that they will only use the data in the ways described by reference (bg) or the TDCR, respectively. Once certified by the JCO, the contractor may:

(a) Request unclassified technical data controlled by the DoD or DND;

(b) Respond to U.S. and Canadian government defense-related contracts whose specifications involved unclassified technical data releasable only to JCP-certified contractors;

(c) Attend restricted gatherings where unclassified technical data are presented (i.e., symposia, program briefings, meetings designed to publicize advance requirements of the contracting agency, pre-solicitation, pre-bid, pre-proposal, and pre-award conferences); and

(d) Arrange unclassified visits directly with other JCP-certified U.S. or Canadian defense contractors or U.S. and Canadian military facilities, in accordance with JCO guidance.

(2) JCP-certified U.S. and Canadian contractors may also access unclassified technical information for other legitimate business purposes which include:

(a) Providing or seeking to provide equipment or technology to a foreign government with the prior approval of the U.S. or Canadian Government, as applicable;

(b) Bidding or preparing to bid on a sale of surplus property;

NAVY FOREIGN DISCLOSURE MANUAL

(c) Selling or producing products for the U.S. or Canadian commercial domestic marketplace, or for the commercial foreign market place, providing that any required export license is obtained from the appropriate U.S. or Canadian licensing authority;

(d) Engaging in scientific research in a professional capacity for either of the two defense establishments; or

(e) Acting as a subcontractor for a concern described in (a) through (d) above.

(3) The DoD also exempts certified Canadian contractors from the need to obtain approval from DoD for unclassified visits to DoD contractor installations to obtain unclassified military critical technical data. Canada's Industrial Security Program procedures also allow for direct contractor-to-contractor arrangements for such visits by U.S. certified contractors. As a result, JCP-certified U.S. and Canadian contractors may make visit arrangements involving only unclassified technical data directly with another JCP-certified contractor.

(4) The JCP does not authorize the transfer of company proprietary technical data that is not controlled by DoD or DND. Therefore, it does not govern private exchanges of industry-generated export-controlled technical data. In these cases, contractors must follow the guidelines established in U.S. or Canadian export control regulations, as applicable.

(5) More information about the U.S.-Canada Joint Certification Program may be found at <http://www.dlis.dla.mil/jcp/>.

PART II - CHAPTER 12**DISCLOSURE OF FOREIGN GOVERNMENT INFORMATION**

- Ref: (i) SECNAVINST 5510.36
 (y) DOD 5200.1-R
 (aq) Executive Order 12958, "Classified National Security Information," of 20 Apr 95
 (ar) Presidential Directive on Safeguarding Classified National Security Information of 14 Aug 99
 (as) DoD Directive 5100.55
 (at) OPNAVINST C5510.101D
 (au) OPNAVINST 5510.100B

21201. General

Foreign Government Information (FGI) is classified or unclassified information that has been either provided by a foreign government or an international organization or has been produced cooperatively between the U.S. and other nations. If the information is provided or produced on the condition that it will be held "in confidence," it shall be protected in accordance with references (i) and (y), which references (aq) and (ar) implement within the Department of Defense (DoD) and the Department of the Navy (DoN). NATO information shall be protected in compliance with reference (as), which references (at) and (au) implement within the DoN. The U.S. shall protect FGI in accordance with the terms of international agreements. These agreements include the NATO Security Agreement, signed by all NATO member nations; bilateral general security agreements; and the various international program agreements that include provisions mandated by the Arms Export Control Act concerning security, retransfer, end-use, and protection.

21202. Policy

Reference (i) specifies that the U.S. will provide protection of FGI equivalent to that provided by the originating foreign government or international organization. The requirements for protecting and marking FGI are specified in references (y), (aq), (ar), (as), (at) and (au). The disclosure of FGI in any form to any third party entity, which includes foreign national employees of the DoD and U.S. defense contractors, is prohibited without the prior consent of the originating foreign government or international organization, unless specifically permitted by the terms of a treaty, agreement, or other bilateral arrangement. No commitments, expressed or implied, will be made to a third party and the identity of the originating foreign government or international organization will not be revealed or acknowledged pending disclosure approval.

21203. Procedures

A Designated Disclosure Authority (DDA) shall not authorize DoN personnel to disclose FGI to a third party except with the specific written authorization of the originating foreign government. DoN organizations proposing the release of FGI shall provide the appropriate DDA sufficient background and justification including the following information:

NAVY FOREIGN DISCLOSURE MANUAL

- a. the specific information that is proposed for third-party disclosure and the related source from which the information was derived (e.g., MOU);
- b. the country, countries, or international organization to which the information would be disclosed;
- c. the foreign government or international organization that originated the information;
- d. the benefits to be derived by the U.S., by the recipient, and by the originating foreign government or international organization;
- e. the channels, procedures, and methods (i.e., oral, visual, documentary, or equipment) by which the information will be disclosed, including the specific security arrangements; and
- f. the event and the planned date for which the third-party disclosure is required. Keep in mind that a response may take up to six months to process.

The DDA shall provide to the requesting DoN organization the response from the originator of the information (foreign government or international organization). If the request is approved, or approved subject to conditions, the response from the DDA must convey the necessary disclosure or transfer manuals.

PART II - CHAPTER 13**DISCLOSURE OF RESTRICTED DATA AND FORMERLY RESTRICTED DATA
(ATOMIC INFORMATION)**

Ref: (r) Atomic Energy Act of 1954, as amended (42 U.S.C. 2121, 2153, 2164)
(av) DoD Directive 5030.14

21301. General

The foreign disclosure of atomic information (i.e., U.S. RESTRICTED DATA (RD) and FORMERLY RESTRICTED DATA (FRD)) is normally associated with arrangements that involve the development of nuclear weapons or with nuclear planning matters involving countries and international organizations with which the U.S. has entered into Agreements for Cooperation. However, such information may also be associated with other matters, such as the hardening of communications systems against electro-magnetic pulse emanations from nuclear detonations. The Secretaries of Defense and Energy, per reference (av), established the Joint Atomic Information Exchange Group (JAIEG) to review proposed disclosures of atomic information to ensure that the information falls within the terms of a pertinent agreement.

21302. Policy

The Atomic Energy Act (reference (r)) specifies that atomic information may be disclosed to foreign governments and regional defense forces (e.g., international organizations) only in accordance with an Agreement for Cooperation (a normal MOA/MOU does not suffice), which is subject to legislative review, and a statutory determination that the cooperation will not constitute an unreasonable risk to national defense and common security. The JAIEG must authorize the disclosure of atomic information to any foreign national prior to the information's release.

21303. Procedures

Proposals to disclose atomic information to a foreign government or international organization shall be forwarded to Navy IPO-01, who shall coordinate the proposal with the JAIEG. Proposals will be submitted as described below.

a. Documentary Disclosures. Proposals for the release of documents containing atomic information (e.g., with RD/FRD markings) to a foreign government or international organization shall contain at least two copies of the pertinent documents and be forwarded to Navy IPO-01 with the following supporting information:

(1) The portions of the document that are proposed for release, including any proposed restrictions or provisos.

(2) The identity of the foreign government or international organization to which release is proposed.

NAVY FOREIGN DISCLOSURE MANUAL

(3) The identity of the agency or office of the proposed recipient foreign government or international organization.

(4) The justification to support the need-to-know of the proposed recipient, to include the identification of the applicable program of cooperation and the identification of the supporting agreement.

(5) The identification of the portions of the proposed release that are under the jurisdiction of the DoN as well as any portions that are under the jurisdiction of another government, international organization, or another U.S. department or agency.

Navy IPO-01 will forward the document or documents to the intended recipient, if JAIEG approves the release.

b. Oral and Visual Disclosures. Any atomic information proposed for oral/visual presentation must be provided to Navy IPO in its full written text. Two copies of all presentations that contain atomic information proposed for disclosure must be forwarded to Navy IPO-01 at least 60 days prior to the date of the proposed disclosure. The material to be forwarded to Navy IPO-01 shall include the supporting information described in paragraph (a), and all graphic material, visual aids, and documents intended for use in the presentation. Navy IPO-01 shall convey the JAIEG response, as well as any additional guidance necessary, to the DoN organization that submitted the request.

c. Reporting Requirement for Oral and Visual Disclosures. A report shall be submitted directly to Navy IPO-01 within 14 days following the presentation for which the disclosure was requested. If information was authorized for disclosure but was not disclosed, a report is still required. Reports pertaining to presentations where atomic information was or was not disclosed shall contain only the information listed below (do not include project reports, program reports, or similar material). The required information includes

(1) the date and place of the presentation;

(2) the Navy IPO-01 letter serial number under which the atomic information was authorized for disclosure;

(3) the name, nationality, and organization of all persons who attended the presentation; and

(4) an exact description of the atomic information actually disclosed; or, if no atomic information was disclosed, a statement that no atomic information was disclosed and the rationale supporting that decision.

21304. US/UK Polaris Sales Agreement and Polaris Trident II Technical Arrangement

A Delegation of Disclosure Authority Letter (DDL), which authorizes the transmittal of specified atomic information under this program, has been issued to the Director, Strategic Systems Program (SSP). Proposed changes to the scope of atomic information that is authorized under the DDL shall be submitted to Navy IPO-01 in accordance with paragraph 21303.

21305. Unauthorized Disclosure

Unauthorized disclosure of atomic information to foreign nationals shall be reported immediately to the Naval Criminal Investigative Service (NCIS) and Navy IPO-01. The report shall include an exact description of the atomic information that was disclosed, the identity of the foreign national(s), and the circumstances under which the disclosure occurred.

PART II - CHAPTER 14

**PARTICIPATION BY FOREIGN CONTRACTORS IN DEPARTMENT OF THE NAVY
PROCUREMENTS**

- Ref: (a) SECNAVINST 5510.34A
(w) International Traffic in Arms Regulations (22 CFR Parts 120-130)
(aw) Competition in Contracting Act of 1984 (10 USC 2304)
(ax) Federal Acquisition Regulation (FAR)

21401. General

This chapter pertains solely to the disclosure of Department of the Navy (DoN) CMI or CUI to foreign contractors who may desire to act in the capacity of prime contractors on DoN procurements. The disclosure of information by a U. S. prime contractor to a foreign subcontractor shall be processed under the Department of State licensing requirements identified in reference (w). The provisions of this chapter apply to foreign contractors and U.S. contractors under foreign ownership, control, or influence (Chapter 15 contains further guidance on U. S. contractors under foreign ownership, control or influence). All DoN procurement and contracting officials shall comply with the contents of this chapter.

21402. Policy

a. Consistent with reference (aw), it is Department of Defense (DoD) policy to ensure full and open competition in solicitations leading to the award of DoD contracts. Foreign contractors from countries with whom the DoD has a reciprocal procurement Memoranda of Understanding (MOU)² shall be afforded the opportunity whenever possible to participate in solicitations and negotiations leading to the award of DoD equipment contracts. Additionally, contractors from countries who have not concluded of a reciprocal procurement MOU with the U.S. may also be considered for participation in DoN procurement. In order for any foreign contractor to participate, however, all information necessary to perform as a prime contractor must be releasable to the government of their country of origin pursuant to reference (q) and the provisions of U. S. statutes. For example, statutes may prohibit foreign participation for national security, mobilization and emergency purposes, when sensitive technology is involved, or for small business set-asides.

b. There may be instances when access by the government of a foreign contractor to Classified Military Information (CMI) or Controlled Unclassified Information (CUI) is not permissible under the National Disclosure Policy (NDP-1), Navy, or other disclosure policy. In this case, foreign contractors may be considered non-qualified suppliers under reference (ax), Part 9, thus preventing their participation as a prime contractor. However, non-qualified suppliers from a country with which DoD has a reciprocal procurement MOU may be given the

² Currently, these countries include Australia, Austria, Belgium, Canada, Denmark, Egypt, Finland, France, Germany, Greece, Israel, Italy, Korea, Luxembourg, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, and the United Kingdom.

opportunity to participate as a subcontractor, provided the required information is authorized for disclosure to the contractor's government.

c. Contracting activities shall initiate a foreign disclosure review with their Designated Disclosure Authority (DDA) and other internal cognizant offices in order to determine whether or not foreign participation will be permitted, and if so, the extent of foreign participation that will be permitted. This review should take place before announcing a solicitation, to avoid subsequent delays in the procurement process and in fairness to all potential contractors. If the foreign disclosure review results in restrictions on foreign participation, limitations on full and open competition shall be published in the solicitation announcement. Under no circumstances will unusual technical or security requirements be imposed solely for the purpose of precluding the acquisition of defense equipment or services from foreign firms.

21403. Procedures

The following procedures shall be followed when reviewing foreign contractor requests for information on DoN contracts³:

a. Cognizant DoN commands/activities shall determine, at the earliest stage of the acquisition cycle, if a requirement exists for disclosing CMI and/or CUI during any phase of a competition, negotiation, contract award, or contract performance that may preclude a foreign contractor's participation. This would include participation in bidder conferences, release of technical data packages, visits to DoN commands or to DoD contractors, and for testing/maintenance operations.

b. The foreign disclosure review shall include

(1) a description of all phases of the program,

(2) the identification of countries whose contractors are likely to participate, and the specific contractors if known,

(3) the extent of the foreign contractors' expected involvement at each phase, including access to controlled facilities,

(4) a specific description of CMI that would have to be disclosed with the security classification levels involved and the identification of technical data that is CUI, and

(5) whether or not U.S. production information (as defined by paragraph 10302d) would have to be disclosed.

³ The U.S.-Canada Joint Certification Program (JCP) permits U.S. and Canadian certified contractors access to each other's unclassified technical data (including critical technology) directly from the originator. Direct access by Canadian contractors to unclassified technical data is limited to those U.S. Munitions List categories authorized by reference (w). A foreign disclosure review must be conducted on all contracts to ensure there is positively no requirement for access to classified or other ITAR proscribed information.

NAVY FOREIGN DISCLOSURE MANUAL

c. Although the authority to include or exclude foreign contractors from participating in DoN procurement resides with the contracting officer, DDAs are responsible for determining whether the information/materiel involved in the procurement is releasable to the government(s) of the foreign contractor(s). Disclosures of classified information, and commitments concerning likely participation, shall not be made to foreign contractors or their governments pending disclosure authorization by the DDA, Navy IPO, and/or the National Disclosure Policy Committee (NDPC).

d. If the disclosure decision exceeds a DDA's delegated disclosure authority, but the DDA recommends approval of the disclosure, the DDA will forward a fully justified recommendation to Navy IPO, who will reply with the final decision. It is the responsibility of the DDA to notify the contracting officer of the final disclosure decision.

e. Bid packages and other contract related documentation containing classified information may be requested by foreign contractors and, if approved for disclosure, shall be released on a government-to-government basis only through the foreign government's embassy in the U.S. unless other procedures are approved by Navy IPO.

f. It is important that the above disclosure actions be initiated and processed expeditiously so the disclosure review does not delay the DoN procurement process.

PART II - CHAPTER 15**DISCLOSURE OF CLASSIFIED AND CONTROLLED UNCLASSIFIED
INFORMATION TO U.S. COMPANIES UNDER FOREIGN OWNERSHIP, CONTROL
OR INFLUENCE (FOCI)**

Ref: (o) DoD 5220.22-M of Jan 95 (NOTAL)
(ay) DoD 5220.22-R of Dec 85 (NOTAL)

21501. General

All U.S. companies (including foreign-owned U.S. firms incorporated in the U.S.) are subject to all U.S. export laws and regulations, including the requirement to obtain an export license before releasing export controlled data to foreign employees, officers, or owners of the company. U.S. companies are particularly susceptible to foreign ownership, control, or influence (FOCI) at any time as a result of mergers, acquisitions, or takeovers. This vulnerability presents a need for awareness of specific policies and procedures affecting the disclosure of export controlled information under FOCI. In accordance with references (o) and (ay), any company that is owned, controlled, or influenced by a foreign interest is ineligible for a facility security clearance. If a foreign firm acquires or merges with a U.S. company that holds a current facility clearance, the clearance will be suspended or revoked until the unacceptable aspects of FOCI are negated or mitigated to a level acceptable to the Department of Defense (DoD). These measures are necessary because foreign ownership, control or influence may result in the compromise of classified or controlled information that could jeopardize U.S. national security interests.

21502. Background

The Committee on Foreign Investment in the U.S. (CFIUS) reviews the filings of proposed acquisitions of U.S. companies by foreign companies or mergers of foreign and U.S. companies. The DoD portion of this review is for the purpose of determining if the proposed merger or acquisition will have an adverse impact on National Security. This process occurs prior to the implementation of FOCI policies and procedures.

a. CFIUS is chaired by the Department of the Treasury, which coordinates the interagency reviews. Filed CFIUS cases are required to have U.S. Government reviews completed within 30 days. The Department of Treasury sends them to the Department of Defense coordinator who sends them to the Department of the Navy (DoN) coordinator, usually within 2-3 days of filing. Navy IPO currently coordinates these cases for the DoN and must notify the Department of Defense coordinator by the 20th day regarding the DoN position on the proposed acquisition or merger. DoN may choose one of two recommendations: (1) no objection; or (2) recommend a 45-day further investigation (This is recommended if the acquisition is of such concern that even the normal FOCI negation methods will not be considered adequate or no FOCI negation agreement can be reached between the U.S. government and the parties to the transaction). The latter is only used in rare cases because the 45-day further investigation requires that the case be sent to the President of the U.S. at the end of the investigation for a final decision.

b. A separate industrial security review is carried out in parallel by the Defense Security Service (DSS) for those companies having classified contracts. DSS will determine if the proposed corporate acquisition will require FOCI negation or mitigation (see paragraph 21503), notify the parties to the proposed acquisition, and request their preliminary acceptance of DSS's recommended remedy in order to retain their facility security clearance.

21503. Policy

The DSS, as the administrative agent for the Defense Industrial Security Program, executes all arrangements made on behalf of the U.S. Government to grant facility security clearances to U.S. companies under FOCI. The following FOCI policies and procedures are mandated by references (o) and (ay) and implemented by the DSS for the DoD and DoD components. These policies and procedures are not augmented or amplified by the DoN. There are several alternative remedies that provide for a company under FOCI to gain or retain a facility security clearance by preventing the foreign interest of the company from having access to export controlled information. These remedies include a Voting Trust, Proxy Agreement, Board Resolution (Corporation), Special Security Agreement (SSA), Security Control Agreement (SCA), or in some cases, a Limited Facility Clearance.

a. A Voting Trust, Proxy Agreement, or Board Resolution are used to negate the FOCI. Under these legal constraints, the foreign owner retains financial interest in the company but relinquishes management and operational control. Companies granted facility security clearances via any of these arrangements are entitled to work on classified contracts and conduct their work in the same manner as cleared U.S. companies.

b. An SSA establishes unique security arrangements within which a company under FOCI is permitted to perform under a classified program or contract. Programs with an SSA normally involve export-controlled information that is not releasable to the controlling foreign interest. An SSA allows the foreign interest to exercise general control of the company; however, the company and the foreign interest must agree to allow only U.S. citizens to be placed in key company positions. SSAs do not permit foreign nationals to have access to export controlled information unless authorized by the Department of State under an export license. SSAs are individually tailored to meet the unique security requirements of each company. Companies cleared via a SSA may not have access to "proscribed information" (Top Secret, Restricted Data, Formerly Restricted Data, Communications Security Information, Special Access Program or Sensitive Compartmented Information) without special authorization. Access to "proscribed information" is permitted only if the Government authority having cognizance over the information makes a favorable National Interest Determination (NID). There must be compelling evidence that the release of the "proscribed information" to the company cleared under the SSA arrangement would advance the security interests of the U.S.. Within the DoN, the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RD&A)) makes this determination. An SSA would then be amended to include the necessary security enhancements. Under an SSA, a company's clearance is valid for use by all departments or agencies that may have a need to contract for classified work, subject to the

limitations of each applicable agreement. An SCA is similar to an SSA; it may be used in those cases where there is less than majority foreign control, power, and authority.

NOTE: U.S. firms that have implemented one of the legal arrangements in paragraph (a) or (b) for mitigating or negating the effects of FOCI are no longer considered FOCI firms; they are to be treated as U.S. firms and no additional foreign disclosure decision is required for the release of information to them.

c. In the absence of a legal arrangement in paragraph (a) or (b) to negate or mitigate FOCI, these firms continue to be treated as if they were foreign firms. These firms may still compete for and perform under classified U.S. defense contracts if they obtain a Limited Facility Clearance and if appropriate foreign disclosure approvals have been made. A foreign disclosure authorization is required for any information to be disclosed. Only in the case of a Limited Facility Clearance is a "foreign disclosure" decision required for a U.S. firm (see Part II, Chapter 14).

(1) A Limited Facility Clearance may be granted only upon satisfaction of the following criteria: (a) There is an Industrial Security Agreement with the foreign government of the country from which the foreign ownership is derived; (b) Access to classified information will be limited to performance on a contract, subcontract or program involving the government of the country from which foreign ownership is derived; and (c) Release of classified information must comply with the U.S. National Disclosure Policy.

(2) For a variety of reasons, a Limited Facility Clearance is rarely chosen as a remedy for FOCI. Access limitations are inherent with the granting of Limited Facility Clearances. In order for DSS to grant a Limited Facility Clearance, they must obtain a request from the Department of the Navy signed by an "empowered official," an appropriate senior official able to represent the command (e.g., program manager, Program Executive Officer (PEO), or flag officer). The requesting command must: cite the compelling need, acknowledge that a Limited Facility Clearance is not a mitigation of FOCI, and accept the security risks involved. Only Navy IPO or a Designated Disclosure Authority (DDA) may authorize the release of export-controlled information to those companies with a Limited Facility Clearance.

(3) Personnel representing or employed by companies with a Limited Facility Clearance who must visit a DoD-controlled facility must submit a visit request in accordance with reference (o). Access to export-controlled information by such personnel is restricted to that which is otherwise releasable to the foreign countries associated with the FOCI company. Requests for visits by such personnel to DoN commands and activities cannot be originated by foreign embassies because the companies are not performing foreign government sponsored work.

PART II - CHAPTER 16**SECURITY POLICY AUTOMATION NETWORK (SPAN)**

- Ref: (c) DoD Directive 5230.11
(d) DoD Directive 5230.20
(s) DoD Directive C-5230.23
(az) DoD Manual 5230.18
(ba) DoD Directive 2040.2

21601. Purpose

Reference (az) implements the Foreign Disclosure and Technical Information System (FORDTIS), which has subsequently been renamed the Security Policy Automation Network (SPAN), as a DoD automated information tracking, storage, and retrieval system. The use of SPAN assists Designated Disclosure Authorities (DDA) in making decisions to approve or deny classified and Controlled Unclassified Information (CUI) and technology to other nations and international organizations by providing a precedence database covering all DoD disclosure decisions. SPAN is also a tool for researching and recording all DoN disclosure cases. DDAs also use SPAN to fulfill DoN disclosure decision responsibilities assigned by the National Disclosure Policy (NDP). Furthermore, SPAN supports the implementation of DoD policies and procedures set forth in references (c), (d), (s), and (ba)

21602. Policy

All classified disclosure decisions (both approvals and denials) must be recorded in SPAN by the DDA who made the decision. Since one step in the disclosure authorization process is to verify the existence of any precedent for the current disclosure proposal, the use of SPAN is essential. The cognizant DDA should review the SPAN databases (see paragraph 21603 below) to determine whether the information requested by a foreign government or international organization has previously been authorized for disclosure to that same country or others. This review should also identify what stipulations, if any, were attached to any past disclosures. Strict DoN compliance with SPAN reporting will produce a comprehensive historical record of foreign disclosure decisions (to include visits, document releases, training, data exchanges, export licenses, and exceptions to National Disclosure Policy) that will expedite the disclosure authorization process.

21603. Primary SPAN Components

a. Foreign Disclosure System (FDS). All decisions that approve or deny the disclosure of CMI to a foreign national, a foreign government, or an international organization shall be reported in the FDS by the authority that approved the disclosure. An FDS record shall thus be created to record each foreign disclosure decision relating to CMI regardless of the means of transfer (oral/visual/documentary). These records shall include decisions concerning document releases, training, and data exchanges (foreign visits are reported to FDS automatically, as described in paragraph b.).

b. Foreign Visits System (FVS). The FVS component of SPAN provides staffing and database support for the processing and recording of visit requests by foreign nationals to DoD activities or cleared contractor facilities. The FVS consists of two different parts, an unclassified and a classified system. The unclassified system allows foreign embassies to submit foreign visit requests online to the appropriate military department where it is then drawn into a classified system. The classified system provides staffing capabilities to support the decision-making process. After a decision has been reached on a specific visit request, the DDA, using the FVS classified system, shall transmit the visit authorization to the DoN facility/command where the visit shall take place. The FVS is able to transmit a confirmation of a visit decision to the requesting embassy via unclassified means. The FVS also maintains a record of the disclosure decision, which is automatically entered into the FDS once the request is approved or denied, satisfying the SPAN reporting requirement.

c. Technology Protection System (TPS). The Munitions List and Commerce Control List databases within the TPS process and record each export license application for the export of CMI and CUI via nongovernmental organizations (NGOs). See Part II, Chapter 3 for more information regarding export licenses. TPS maintains a record of the disclosure decision, satisfying the SPAN reporting requirement.

d. National Disclosure Policy System (NDPS). The National Disclosure Policy System (NDPS) database records all exceptions to NDP-1 that are granted by the National Disclosure Policy Committee (NDPC). Access to NDPS is limited to Navy IPO.

21604. Reporting Procedures

a. Input. All DoN DDAs shall ensure that CMI disclosure decisions made under their authority are recorded in SPAN. DDAs without access to the SIPRNET-based SPAN shall create disclosure decision records which shall be submitted via the chain of command to their next senior DDA with online connectivity. This DDA will then input the records into SPAN on their subordinate's behalf.

b. CMI Disclosure Decision Records. Each CMI disclosure decision record must contain the following data:

(1) The requestor, date of request, correspondence reference information, and reason for the request (may be verbatim or paraphrased).

(2) The disclosure decision (approval or denial), date of decision, level of disclosure authorized, and NDP category or categories of classified information authorized for disclosure, and the justification for the disclosure including the decision's correspondence reference information and the text of the authorization (including any limitations or provisos that were placed on the disclosure) or denial.

(3) The appropriate security classification markings for the text of the disclosure decision record.

c. Connectivity. All DoN DDAs with SIPRNET connectivity should maintain SPAN connectivity. Disclosure officials without SIPRNET should record their disclosure decisions via the offline software. Information about establishing a network connection to SPAN and user accounts may be obtained from the Office of the Deputy Under Secretary of Defense for Policy Support, Security Policy Automation Directorate (SPAD). Training for the use of SPAN may be obtained directly from the SPAD office.

21605. Output Records

The SPAN databases are capable of providing users with output reports for data that have been submitted. These output reports should be used to support the objectives stated in paragraph 21601 above. For output reports, interested parties must provide in writing a detailed description of the information requested and the desired output format to their next senior DDA with online connectivity. Requests for an output report must be accompanied by sufficient information to conduct a thorough search of the relevant databases.

GLOSSARY

Case-by-Case Basis. The principle that a disclosure authorization is restricted to individual events or occasions to prevent confusion with permanent and repetitive disclosure delegations.

Classified Military Information (CMI). Information originated by or for the DoD or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL. CMI may be in oral, visual, or material form and has been divided into eight categories. Military information may also be embodied in equipment, software, firmware, databases, imagery, or other forms.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Compromise. An unauthorized disclosure of classified information.

Contact Officer. A DoN official designated in writing to oversee and control all contacts, requests for information, consultations, access, and other activities of foreign nationals who are assigned to, or are visiting, a DoN Component or subordinate organization. For Defense Personnel Exchange Program (DPEP) assignments, the host supervisor may be the contact officer.

Controlled Unclassified Information (CUI). CUI is unclassified information to which access or distribution controls have been applied in accordance with national laws, policies, and regulations. CUI is a term used to collectively describe unclassified information that has been determined to be exempt from mandatory disclosure to the public pursuant to the Freedom of Information Act (5 U.S.C. 552) or that is subject to U.S. export controls. *Within the DoD most of this information is marked “For Official Use Only” or “FOUO”; however, there are exceptions to the FOUO marking. Unclassified Controlled Nuclear Information (UCNI) is marked as such; personnel and medical files are marked with privacy statements; contractor information marked “PROPRIETARY” or “Business-Sensitive” will be handled as FOUO when provided to DoD/DoN; and there are special distribution and export control warning notices that are applied by DoN Components to DoN documents that contain “critical technology” with a military or space application.*

Cooperative Program Personnel. Foreign government personnel, assigned to a multinational program office that is hosted by a DoN Component in accordance with the terms of a cooperative program international agreement, who report and take direction from a DoN-appointed program manager (or program manager equivalent) for the purpose of carrying out the multinational project or program. Foreign government representatives described in such agreements as liaison officers or observers are not considered Cooperative Program Personnel and are treated as FLOs.

Critical Technology. See Technology, Critical.

Defense Articles. Weapons, weapon systems, munitions, aircraft, boats, or other implements of war; property, installations, material, equipment, or goods used for the purposes of furnishing military assistance or making military sales; any machinery, facility, tool, material, supply, or other items necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any other defense article or component or part of any articles listed above. Defense articles do not include merchant vessels, major combatant vessels, or as defined by the Atomic Energy Act of 1954, as amended (Title 42 U.S.C. 2011), source material, by-product material, special nuclear material, production facilities, utilization facilities, or atomic weapons or articles involving Restricted Data.

Defense Personnel Exchange Program (DPEP). A program under which military and civilian personnel of the Department of Defense and military and civilian personnel of the defense ministries and/or military services of foreign governments, in accordance with the terms of an international agreement, occupy positions with and perform functions for a host organization to promote greater understanding, standardization, and interoperability.

Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate Designated Disclosure Authority (DDA) (normally Navy IPO) to a designated DoN official explaining classification levels, categories, scope, and limitations of information under a DoN Component's disclosure jurisdiction that may be disclosed to a foreign recipient. Under no circumstances may the contents of DDLs be disclosed or acknowledged to foreign representatives. DDLs are general or subject-specific.

- Navy IPO issues general delegations of disclosure authority to Designated Disclosure Authorities (DDAs) (e.g., the Chief of Naval Operations, the Commandant of the Marine Corps, and the commanders of Navy commands).
- Subject-specific DDLs are issued to specified DoN components, typically on a project-by-project basis. For example, a DDL is typically issued for DEA/IEA Annexes, MOAs, and MOUs.

Designated Disclosure Authority (DDA). An official at a DoN organization (e.g., command, agency, staff element) that has been granted a general delegation of disclosure authority by Navy IPO and is responsible for controlling disclosures of CMI and CUI at that organization. Normally, the designated official is nominated by the head of his or her organization and is approved by Navy IPO by issuance of the general delegation of disclosure authority to the named official.

Disclosure. Conveying controlled information, in any manner. For the purposes of this manual, "disclosure" connotes oral, visual, electronic or physical transfer ("release") of controlled information or material. (See Foreign Disclosure.)

Documentary Information. Any information, which is recorded on paper, film, transparency, electronic medium, or any other medium. This includes, but is not limited to printed publications, reports, correspondence, maps, audiotapes, email, spreadsheets, databases and graphical slides, technical drawings, software code, and information embodied in hardware.

Export. The International Traffic in Arms Regulation (ITAR) defines “export” as:

- Sending or taking a defense article out of the U.S. in any manner, except by mere travel outside of the U.S. by a person whose personal knowledge includes technical data; or
- Transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the U.S. or abroad; or
- Disclosing (including oral or visual disclosure) or transferring in the U.S. any defense article to an embassy, any agency or subdivision of a foreign government (e.g. diplomatic missions; or
- Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the U.S. or abroad; or
- Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the U.S. or abroad.
- A launch vehicle or payload shall not, by reason of the launching of such vehicle, be considered an export for purposes of this [ITAR] subchapter. However, for certain limited purposes, the controls of this [ITAR] subchapter may apply to any sale, transfer or proposal to sell or transfer defense articles or defense services.

Export License. The authorization issued by the State Department, Office of Defense Trade Controls, or by the Department of Commerce, Bureau of Industry and Security, which permits the export of ITAR or EAR controlled articles, technical data, or services.

Export License Application. A request submitted by U.S. persons and foreign government entities in the U.S. to export ITAR/EAR controlled technical data, services, or articles to a foreign person (see “Foreign Person”).

Foreign Disclosure. The disclosure of CMI or CUI to an authorized representative of a foreign government or international organization. (NOTE: The transfer or disclosure of CMI or CUI to a foreign national who is an authorized employee of the U.S. Government or a U.S. contractor technically is not a “foreign disclosure,” since the disclosure is not made to the person’s government. For contractors, access by such persons will be handled under the provisions of the Arms Export Control Act or Export Administration Act and the National Industrial Security Program Operating Manual. For DoN organizations, access by such persons are handled in compliance with DoD Regulation 5200.2-R and DOD Regulation 5200.1-R implemented by SECNAVINST 5510.36 and SECNAVINST 5510.30A.)

Foreign Disclosure Point Of Contact (FDPOC). FDPOCs are DoN officials who are appointed by the Chief of Naval Operations, the Commandant of the Marine Corps, Component Commanders, Commanders of Systems Commands, and the Chief of Naval Research for the coordination of foreign disclosure reviews and to facilitate a complete and timely response to foreign requests for CMI or CUI representing the consolidated organization position. FDPOCs do not hold disclosure authority, unless also appointed as a DDA (see definition of DDA).

Foreign Government Information (FGI). Information provided to the U.S. by a foreign government or governments, an international organization, or any element thereof, with the expectation that the information, the source of the information, or both are to be held in confidence; produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or information received and treated as FGI under the terms of Executive Order 12958.

Foreign Liaison Officer (FLO). A foreign government military member or civilian employee authorized by his or her government and certified by a DoD Component to act as an official representative of that government in its dealings with a DoD Component in connection with programs, projects, or agreements of interest to that government. There are three types of FLOs:

- a. **Security Assistance.** A foreign government representative who is assigned to a DoD/DoN Component or contractor facility in accordance with a requirement that is described in a Foreign Military Sales (FMS) Letter of Offer and Acceptance (LOA).
- b. **Operational.** A foreign government representative who is assigned to a DoD/DoN Component in accordance with a documented requirement to coordinate operational matters, such as combined planning or training and education.
- c. **National Representative.** A foreign government representative who is assigned to his or her national embassy or delegation in the U.S. (e.g., an attaché), to conduct liaison activities with the DoD and the DoD Components.

Foreign Military Sales (FMS). The portion of U.S. security assistance authorized by the Foreign Assistance Act of 1961, and the Arms Export Control Act. The recipient typically provides reimbursement for defense articles and services transferred from the U.S. This includes cash sales from stocks (inventories, services, training) by the DoD, sales implemented by contract, and authorized military assistance.

Foreign National. A person who is not a citizen or national of the U.S.

Foreign Person. A foreign natural person who is not a lawful permanent resident as defined by 8 U.S.C. 1101 (a)(20), or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the U.S., as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

Foreign Representative. A person, regardless of citizenship, who represents a foreign interest in his or her dealings with the U.S. Government, or a person who is officially sponsored by a foreign government or international organization. A U.S. national shall not be treated as a foreign person except when acting as a foreign representative.

Foreign Visit. Any contact by a foreign representative with a DoN organization or contractor facility. Such visits are of two types, based on sponsorship:

a. **Official Foreign Visit.** Contact by foreign representatives under the sponsorship of their government or an international organization with a DoD component or DoD contractor facility. Only official visitors may have access to classified or Controlled Unclassified Information.

b. **Unofficial Foreign Visit.** Contact by foreign nationals with a DoD/DoN command or activity for unofficial purposes, such as courtesy calls and general visits to commands or events that are open to the public, and without sponsorship of their government. Such visitors shall have access only to information that has been approved for public disclosure.

NOTE: Foreign nationals not sponsored by their government, visiting under the terms of a DoD/DoN contract are not considered foreign visitors and will be cleared in accordance with the National Industrial Security Program Operating Manual Section 5, paragraph 10-507.

Government-to-Government Transfer. The principle that classified information and material will be transferred by government officials through official government channels (e.g., military postal service, diplomatic courier) or through other channels expressly agreed upon in writing by the governments involved. In either case, the information or material may be transferred only to a person specifically designated in writing by the foreign government as its designated government representative for that purpose.

International Organization. An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies. This typically refers to the North Atlantic Treaty Organization (NATO), or one of its elements.

Lawful Permanent Resident. An individual having been lawfully accorded the privilege of residing permanently in the U.S. as an immigrant in accordance with the immigration laws, such status not having changed. See U.S. National.

Naval Nuclear Propulsion Information (NNPI). Information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities. Information concerning equipment, components, or technology which are applicable to both Naval nuclear and conventional propulsion plants is not considered to be NNPI when used in reference to conventional applications only, provided no association with naval nuclear propulsion can be

directly identified from the information in question. In cases where an association with naval nuclear propulsion can be directly identified from the information in question, designation as NNPI is mandatory.

Non-Governmental Organization. Refers to a nonprofit, voluntary, formal, nonviolent, nonpolitical, tax-exempt organization whose objective is to respond to perceived needs such as promoting development and social change.

Oral/Visual Disclosure. To brief orally, to expose to view, or to permit use under U.S. supervision in order to permit the transfer of knowledge or information, but not to physically transfer documents, material, or equipment to a foreign government or its representatives.

Principal Disclosure Authority (PDA). The PDA oversees compliance with this manual within the DoN and is the only DoN official other than the Secretary or Under Secretary of the Navy who is authorized to deal directly with the Secretary or Under Secretary of Defense regarding such matters as DoN requests for exceptions to the National Disclosure Policy. The PDA for the DoN is the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)). Navy IPO has been designated by ASN (RD&A) to act on his behalf as the PDA for the Navy.

Release. The physical transfer of documents, material, or equipment to foreign governments, international organizations, or a recipient of a licensed export. The definition of “disclosure” includes “release.”

Restricted Data (RD) and Formerly Restricted Data (FRD).

a. RESTRICTED DATA (RD) includes all data concerning: (a) the design, manufacture or use of atomic weapons, (b) the production of special nuclear material, or (c) the use of special nuclear material in the production of energy, but does not include data declassified or removed from the RESTRICTED DATA category under Section 142 of the Atomic Energy Act of 1954 as amended.

b. FORMERLY RESTRICTED DATA (FRD) is information removed from the RESTRICTED DATA category upon joint determination by the Atomic Energy Commission (subsequently Department of Energy) and the DoD that such information relates primarily to the military utilization of atomic weapons and that it can be adequately safeguarded as classified defense information. Such information is, however, treated the same as RESTRICTED DATA for purposes of foreign dissemination.

Security Assurance. Written confirmation requested by and exchanged between governments of the security clearance level and eligibility of their employees or national contractors to assume custody of classified information on behalf of the recipient government. There are two additional types of security assurances.

a. **Facility Security Clearance Assurance (FSCA).** A certification provided by a government on a contractor facility under its territorial jurisdiction which indicates that the

facility is cleared to a specific security level and has suitable security safeguards in place at the specified level to safeguard classified information.

b. **Personnel Security Clearance Assurance (PSCA)**. This pertains to an individual who is to be employed by a government or its contractors and requires a personnel security clearance (i.e., a Limited Access Authorization in the U.S.). It is a statement provided by the security authorities of the individual's country of citizenship concerning the individual's eligibility for a personnel security clearance at a level equivalent to the level specified by the requesting (host) government. (See also DoD 5200.2-R)

Sensitive Compartmented Information (SCI). Information and material that require special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

Security Policy Automation Network (SPAN). A wide area computer network sponsored by the Office of the Under Secretary of Defense (Policy Support) (OUSD (PS)) consisting of a DoD-wide Secret classified network and a separately supported unclassified network that supports communications and coordination among DoD activities on foreign disclosure, export control, and international arms control and cooperation.

Technical Data.

(1) Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, manuals and documentation.

(2) Classified information relating to defense articles and services.

(3) Information covered by an invention secrecy order.

(4) Software directly related to defense articles.

(5) This definition does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

Technology. Information, including scientific information, which is necessary for the research, development, design, and manufacture of end products.

Technology, Critical. Also referred to as militarily critical technology. Technologies that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the U.S., consisting of

(1) arrays of design and manufacturing know-how (including technical data);

(2) keystone manufacturing, inspection, and test equipment;

(3) keystone materials; and

(4) goods accompanied by sophisticated operation, application, or maintenance know-how.

Third Party Transfer. The retransfer of a defense article by a foreign government or foreign entity, that was originally provided the article by the U.S. government or a U.S. entity, to any entity not an officer, agent, or employee of that government or entity. The USG generally limits the definition of "agent" to mean freight forwarders. Third party transfer includes the retransfer of a defense article by a foreign government or foreign entity, that was originally provided the article by the U.S. government or a U.S. entity, to a foreign government or foreign entity of the same origin but who is not an agent/employee of the original foreign government or entity.

U.S. Citizen. For the purposes of this manual, a person either naturalized as a U.S. citizen in accordance with U.S. Immigration and Naturalization laws and regulations or a person born in one of the following locations: any of the 50 states of the U.S., the District of Columbia, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands, Panama Canal Zone (if the father and/or mother was/were, or is/was a citizen of the U.S.), the Federated States of Micronesia, or the Republic of the Marshall Islands.

U.S. National. A citizen of the U.S. or a person who, though not a citizen of the U.S., owes permanent allegiance to the U.S., e.g., a lawful permanent resident of the U.S. Categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. are listed in 8 U.S.C. 1101(a) and 8 U.S.C. 1401, subsection (a) paragraphs (1) through (7). Legal counsel should be consulted when doubt exists as to whether or not a person can qualify as a national of the U.S.. NOTE: A U.S. national shall not be treated as a foreign person except when acting as a foreign representative.

MASTER REFERENCE LIST

- (a) SECNAVINST 5510.34A – “Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives” of 8 October 2004
- (b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (hereafter National Disclosure Policy or NDP-1) of 2 October 2000 (NOTAL)
- (c) DoD Directive 5230.11 – “Disclosure of Classified Military Information to Foreign Governments and International Organizations” of 16 June 1992
- (d) DoD Directive 5230.20 – “Visits, Assignments, and Exchanges of Foreign Nationals” of 22 June 2005
- (e) DoD Directive 4500.54 – “Official Temporary Duty Travel Abroad” of 1 May 1991
- (f) Arms Export Control Act (22 U.S.C. 2751)
- (g) Export Administration Act (EAA)
- (h) DoD 5400.7-R – “DoD Freedom of Information Act Program” of September 1998
- (i) SECNAVINST 5510.36A – “Department of the Navy Information Security Program Regulation” of 6 October 2006
- (j) SECNAVINST 5720.42F – “Department of the Navy Freedom of Information Act (FOIA) Program” of 1 January 1999
- (k) Public Law 98-94 (10 U.S.C. 130)
- (l) DoD Directive 5230.24 – “Distribution Statements on Technical Documents” of 18 March 1987
- (m) OPNAVINST 5510.161 – “Withholding of Unclassified Data from Public Disclosure” of 29 July 1985
- (n) DoD 5105.38-M – “Security Assistance Management Manual (SAMM)” of 3 October 2003
- (o) DoD 5220.22-M – “National Industrial Security Operating Manual (NISPOM)” of 24 September 2004
- (p) SECNAVINST 4900.46B – “The Technology Transfer and Security Assistance Review Board (TTSARB)” of 16 December 1992
- (q) DoD Manual S5230.28 – “Low Observable (LO) and Counter Low Observable (CLO) Programs” of 26 May 2005
- (r) Atomic Energy Act of 1954 (42 U.S.C. §§2011-2297)
- (s) DoD Directive C-5230.23 – “Intelligence Disclosure Policy” of 18 November 1983
- (t) Guide for Foreign Attachés Accredited to the Department of the Navy (NOTAL)
- (u) SECNAVINST 5510.30B – “Department of the Navy Personnel Security Program” of 6 October 2006
- (v) National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments (NSTISSP No. 8) of 13 Feb 97
- (w) International Traffic in Arms Regulations (ITAR) (22 CFR 120-130)
- (x) Export Administration Regulations (EAR) (15 CFR 730-799)
- (y) DoD 5200.1-R – “Information Security Program” of January 1997
- (z) DoD 5200.2-R – “Personnel Security Program” of January 1987

- (aa) ASN(RDA) memorandum, “Charter for the Deputy Assistant Secretary of the Navy (International Programs) and Director, Navy International Programs Office” of 11 May 2005
- (ab) SECNAVINST 5710.25B – “International Agreements” of 23 December 2005
- (ac) OPNAVINST 5710.24 – “International Agreements Navy Procedures” of 28 April 1978
- (ad) OPNAVINST 5710.25 – “International Agreements OPNAV Procedures” of 28 May 1978 (NOTAL)
- (ae) DoD Directive 2015.4 – “Defense, Research, Test and Evaluation (RDT&E) Information Exchange Program” of 2 February 2002
- (af) DoD Directive 5530.3, with Change 1 – “International Agreements” of 18 February 1991 (NOTAL)
- (ag) Foreign Assistance Act of 1961
- (ah) OPNAVINST 4900.149 – “Foreign Military Sales (FMS) Case Management” of 28 September 1984
- (ai) Chairman JCS Instruction 6510.06A – “Communications Security Releases to Foreign Nations” of 18 December 2006
- (aj) DoN Guide for the C4ISR Release Process of October 2001
- (ak) Cooperative Research and Development Projects: Allied Countries (10 U.S.C. 2350a (g))
- (al) DoD 5000.3-M-2 – “Foreign Comparative Testing (FCT) Program Procedures Manual” of 25 January 1994
- (am) OUSD (AT&L) Foreign Comparative Testing Handbook of August 2005
- (an) SECNAVINST 4900.48 – “Transfer of U.S. Naval Vessels to Foreign Governments and International Organizations” of 6 November 1990
- (ao) DoD 4500.54-G – “DoD Foreign Clearance Guide”
- (ap) OPNAVINST 5700.7G – “The U.S. Navy Personnel Exchange Program (PEP)” of 29 April 1991
- (aq) Executive Order 12958 – “Classified National Security Information” of 20 April 1995
- (ar) Presidential Directive on Safeguarding Classified National Security Information of 14 August 1999
- (as) DoD Directive 5100.55 – “United States Security Authority for North Atlantic Treaty Organization Affairs” of 27 February 2006
- (at) OPNAVINST C5510.101D – “NATO Security Procedures” of 17 August 1982
- (au) OPNAVINST 5510.100B – “Supplemental Manuals for the Control and Handling of NATO Classified Material by Control Points Under the Administrative Control of the Chief of Naval Operations Sub-Registry” of 8 September 1999
- (av) DoD Directive 5030.14 – “Disclosure of Atomic Information to Foreign Governments and Regional Defense Organizations” of 24 July 1981
- (aw) Competition in Contracting Act of 1984 (10 U.S.C. 2304)
- (ax) Federal Acquisition Regulation (FAR)
- (ay) DoD 5220.22-R – “Industrial Security Regulation” of December 1985 (NOTAL)
- (az) DoD Manual 5230.18 – “DoD Foreign Disclosure and Technical Information System (FORDTIS)” of 6 November 1984
- (ba) DoD Directive 2040.2 – “International Transfers of Technology, Goods, Services, and Munitions” of 17 January 1984
- (bb) U.S.-Canada Joint Certification Program (JCP) of December 1996

NAVY FOREIGN DISCLOSURE MANUAL

- (bc) OASD (NII) Department of Defense Global Positioning System (GPS) Security Policy of 4 April 2006
- (bd) OPNAVINST 3710.7T of 1 March 2004
- (be) OPNAVINST 5720.2L CH-1 of 6 August 2002
- (bf) National Telecommunications and Information Systems Security Manual (NTISSI) No. 3013
- (bg) DODDIR 5230.25 of 6 November 1984
- (bh) DUSD memo; Subj: Accountability of Department of Defense (DoD) Sponsored Foreign Personnel in the United States (U.S.) of 18 May 2004 (NOTAL)

INDEX

Annex A to NDP-1, 3, 21, 25
 Arms Export Control Act (AECA), 2, 22, 37, 55, 72
 Classified Military Information (CMI), 1, 13, 20, 22, 31, 52, 64, 72, 77, 78, 94, 103
 Communications Security (COMSEC), 13, 28, 32, 73, 103
 Contact Officer, 69, 71, 103
 Controlled Unclassified Information (CUI), 1, 5, 13, 22, 31, 52, 64, 77, 100, 103
 Cooperative Program Personnel, 41, 64, 69, 70, 71, 103
 Defense Personnel Exchange Program (DPEP), 64, 67, 103, 104
 Delegation of Disclosure Authority Letter (DDL), 9, 29, 41, 52, 55, 65, 92, 104
 Designated Disclosure Authority (DDA), 3, 5, 9, 10, 23, 38, 50, 52, 64, 72, 83, 89, 95, 99, 104
 Export Administration Act (EAA), 2, 22
 False Impressions, 4, 23, 26, 82
 Foreign Government Information (FGI), 2, 13, 24, 89, 106
 Foreign Liaison Officer (FLO), 5, 64, 66, 106
 Foreign Military Sales (FMS), 33, 43, 66, 73, 77, 106
 Foreign Visit, 29, 52, 55, 71, 73, 107
 General Security Agreement, 15, 27
 International Traffic in Arms Regulations (ITAR), 22, 37, 58
 National Disclosure Policy (NDP-1), 2, 56, 94
 National Military Information Disclosure Policy Committee, 26
 National Security Decision Memorandum 119 (NSDM-119), 2
 Naval Nuclear Propulsion Information (NNPI), 13, 31, 60, 73, 83, 107
 NDPC Policy Statements, 4, 30
 Principal Designated Disclosure Authority (PDA), 3
 Principal Disclosure Authority (PDA), 5, 8, 108
 Security Assurance, 8, 27, 109
 Security Policy Automation Network (SPAN), 5, 29, 42, 52, 56, 100, 109
 Sensitive Compartmented Information (SCI), 26, 30, 109
 Technology Transfer and Security Assistance Review Board (TTSARB), 9, 29, 35, 78