

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**



**DEPARTMENT OF THE AIR FORCE
MANUAL 16-201**

19 JANUARY 2021

**EGLIN AIR FORCE BASE
Supplement**

20 MARCH 2024

Operations Support

**DEPARTMENT OF THE AIR FORCE
FOREIGN DISCLOSURE AND
TECHNOLOGY TRANSFER PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/IAPD

Certified by: SAF/IAP
(Mr. James A. Dunn)

Supersedes: AFI16-201, 2 June 2015

Pages: 84

(EGLINAFB)

OPR: 96TW/IPF

Certified by:
(Dr. Gayle Blue-Keys)

Supersedes: AFI16-201_AFMCSUP_EGLINAFBSUP,
24 April 2014

Pages: 84

This Department of the Air Force Manual (DAFMAN) implements Department of the Air Force Policy Directive (DAFPD) 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*. This publication applies to all United States Department of the Air Force (DAF) civilian employees and uniformed members, including Regular Air Force, Space Force, Air Force Reserve, and the Air National Guard. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the DAF Records Information Management System. Refer recommended changes about this publication to the office of primary responsibility (OPR), the Deputy Under Secretary of the Air Force, International Affairs, Foreign Disclosure and Technology Transfer Division (SAF/IAPD), using Air Force Form 847,

Recommendation for Change of Publication; route Air Force Forms 847 from the field through the appropriate functional chain of command. This DAFMAN may be supplemented at any level, but all supplements must be routed to the OPR for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T3”) number following the compliance statement. See Department of the Air Force Instruction 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor’s commander for non-tiered compliance items. Compliance with the attachments in this publication is mandatory.

(EGLINAFB) DAFMAN 16-201, 19 January 2021, is supplemented as follows: This supplement applies to all activities assigned to Eglin AFB FL and associate organizations participating in Foreign Disclosure programs via formal support agreement. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*. Route AF IMTs 847 from the field through the appropriate functional chain of command. Ensure that all records created because of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management, and Information Governance Program*, and are disposed of in Records Information Management System.

SUMMARY OF CHANGES

This document has been converted from an AFI into a DAFMAN because of administrative revisions. No significant changes to the scope or intent have been made to the document.

(EGLINAFB) This document has been converted from an AFI into a DAFMAN because of administrative revisions. No significant changes to the scope or intent have been made to the document.

Chapter 1—FOREIGN DISCLOSURE AND TECHNOLOGY TRANSFER PROGRAM	7
1.1. Purpose and Objectives.....	7
1.2. Applicability.	7
1.3. Department of the Air Force Foreign Disclosure Authority.	8
Chapter 2—ROLES, RESPONSIBILITIES, AND DETAILED PROCEDURES	10
Section A—Roles and Responsibilities.	10
2.1. Deputy Under Secretary of the Air Force, International Affairs.	10
2.2. Deputy Under Secretary of the Air Force, International Affairs, Foreign Disclosure and Technology Transfer Program.	10
2.3. Deputy Under Secretary of the Air Force, International Affairs, Weapons Division.....	11
2.4. MAJCOM, Field Command, DRU, and FOA Commanders.	11

Section B—Detailed Procedures.	11
2.5. MAJCOM, Field Command, DRU, and FOA Foreign Disclosure Officers.	11
2.6. Installation and Garrison Commanders.	12
2.7. Installation and Garrison Foreign Disclosure Officers.	12
2.8. Commanders/Directors of Tenant Organizations.	13
2.9. Tenant and Element Foreign Disclosure Officers.	13
2.10. Security Cooperation Officers.	13
2.11. Foreign Disclosure Representatives.	14
2.12. DAF Contact Officers.	14
Chapter 3—DEPARTMENT OF THE AIR FORCE FOREIGN DISCLOSURE AUTHORITY	15
3.1. Introduction and Overview.	15
3.2. Disclosure Criteria.	15
3.3. Requests That Exceed DAF General Disclosure Authority.	15
3.4. Coordination of Disclosures Involving Military Equipment.	16
3.5. Delegation of DAF Disclosure Authority.	19
3.6. Documentation of Delegated Disclosure Authority.	19
3.7. Dissemination of Delegation of Disclosure Authority Letters.	20
Chapter 4—PROGRAM MANAGEMENT	22
4.1. Program Management Requirements.	22
4.2. Standard Suspense Requirements for Disclosure Activities.	22
4.3. Training Requirements.	22
4.4. Waivers to DAF Foreign Disclosure Policy.	23
Chapter 5—DISCLOSING INFORMATION	24
5.1. Introduction.	24
5.1. (EGLINAFB) Eglin FDOs must.	24
5.2. Methods of Disclosure.	24
5.3. Submitting Requests to Disclose Information.	24
5.4. Processing Requests to Disclose Information.	26
5.5. Approving Requests to Disclose Information.	26
5.6. Actions Prior to Disclosing Information.	27
5.7. Disclosures Not Requiring FDO Authorization.	28

5.8.	Foreign Contractor Attendance at Symposia, Conferences, and Contract-Related Meetings.	28
5.9.	Foreign Access to DAF Information Systems.	28
5.10.	Technical Orders.....	29
Chapter 6—	TECHNOLOGY TRANSFER	30
6.1.	Introduction.....	30
6.2.	International Trafficking in Arms Regulation Licensing Requirements.....	30
6.3.	Exemptions to Licensing Requirements.	30
6.4.	DAF Requests for Export Licenses.....	32
6.5.	Non-Sponsored Foreign Visits to U.S. Defense Industry.	33
Chapter 7—	VISITS TO DAF FACILITIES BY REPRESENTATIVES OF FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS.	34
7.1.	Introduction.	34
7.2.	General Visit Policies and Procedures.	34
7.3.	Submitting Visit Requests for Foreign Representatives.	36
7.4.	Coordinating Visit Requests for Foreign Representatives.	38
7.5.	Approving Visit Requests for Foreign Representatives.....	38
7.6.	Denying Visit Requests for Foreign Representatives.	39
7.7.	Visits Hosted by Foreign Tenants on DAF Installations or Garrisons.....	39
7.8.	DAF Personnel Visiting Foreign Government or International Organization Establishments Overseas.....	39
Chapter 8—	EXTENDED VISITS INVOLVING FOREIGN REPRESENTATIVES	40
8.1.	Introduction.....	40
8.2.	Categories of Extended Visits.....	40
8.3.	Authorities and Guidance for Extended Visits.	40
8.4.	Establishing Extended Visit Positions.	41
8.5.	Dual Assignment as a Cooperative Project Personnel and a Foreign Liaison Officer.....	42
8.6.	Coordinating Extended Visit Requests.	42
8.7.	Approving Extended Visit Requests.....	42
8.8.	Security Requirements for Extended Visits.....	43
8.9.	Extended Visitor Access to DAF Facilities, Installations, and Garrisons.	43

DAFMAN16-201_EGLINAFBSUP 20 MARCH 2024	5
Chapter 9—DAF PROCUREMENT ACTIVITIES INVOLVING FOREIGN INDUSTRY	45
9.1. Introduction.....	45
9.2. Reviewing Planned Procurements.	45
9.3. Appeals Regarding Decisions to Exclude Foreign Contractors.....	45
Chapter 10—SECURITY REQUIREMENTS	46
10.1. Introduction.....	46
10.2. Reporting and Processing Unauthorized Access to Classified Military Information.	46
10.3. Reporting and Processing Unauthorized Access to Controlled Unclassified Information.	46
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	47
Attachment 2—NATIONAL DISCLOSURE POLICY (NDP-1) FUNCTIONAL CATEGORIES OF INFORMATION	58
Attachment 3—DELEGATION OF DISCLOSURE AUTHORITY LETTER (DDL) EXAMPLE	60
Attachment 4—DISSEMINATING DDL INFORMATIONAL COPIES	62
Attachment 5—SUBMITTING FOREIGN DISCLOSURE REQUESTS TO SAF/IAPD	63
Attachment 6—FORMAT FOR AUTHORIZING DISCLOSURE OF CMI	64
Attachment 7—FORMAT FOR AUTHORIZING DISCLOSURE OF CUI	66
Attachment 8—SAMPLE LANGUAGE TO ADDRESS ADMINISTRATIVE RESPONSIBILITIES FOR EXTENDED VISIT POSITIONS	68
Attachment 9—INSTRUCTIONS FOR CREATING POSITION DESCRIPTIONS FOR EXTENDED VISIT POSITIONS	72
Attachment 10—SECURITY PLAN SAMPLE FORMAT	74
Attachment 11—SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES FOR DEFENSE PERSONNEL EXCHANGE PROGRAM PERSONNEL	76
Attachment 12—COMMITMENT REGARDING INVENTIONS MADE AND TECHNICAL INFORMATION DEVELOPED BY VISITING SCIENTISTS AND ENGINEERS	77
Attachment 13—SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES FOR COOPERATIVE PROJECT PERSONNEL (CPP)	78

Attachment 14—SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES FOR FOREIGN LIAISON OFFICERS (FLO)	79
Attachment 15—SAMPLE ITAR EXEMPTION CERTIFICATION REQUEST LETTER	80
Attachment 16—SAMPLE ITAR EXEMPTION CERTIFICATION CHECKLIST	82
Attachment 17—FOREIGN DISCLOSURE Exception to National Disclosure Policy PROCESS	84

Chapter 1

FOREIGN DISCLOSURE AND TECHNOLOGY TRANSFER PROGRAM

1.1. Purpose and Objectives. Military information is a national security asset that must be conserved and protected and may only be shared with foreign nationals when there is a clearly-defined advantage to the United States (U.S.). It is U.S. policy to avoid creating false impressions of its readiness to make defense articles, technologies, services or information available. DAF personnel must ensure compliance with this DAFMAN as part of the initial planning for international activities. Only designated foreign disclosure officers (FDOs) may approve the disclosure of controlled unclassified information (CUI) and classified military information (CMI) to foreign nationals. This DAFMAN documents the requirements of the Foreign Disclosure and Technology Transfer Program and its applicability to DAF organizations and activities. It outlines the authorities and responsibilities of the DAF, service headquarters, major commands (MAJCOMs), field commands, direct reporting units (DRUs), field operating agencies (FOAs), and FDOs at all command levels. It also provides guidance for authorizing disclosure of information that is not CMI or CUI and provides guidance on approving foreign national visits to DAF bases and facilities. This manual does not apply to disclosures regarding national intelligence; communications security and intelligence; special access programs, counterintelligence; DAF intelligence exchanges; military-to-military international intelligence agreements; atomic information; strategic planning and guidance; or narcotics intelligence. Other visits and disclosures that do not involve access to CMI or CUI are conducted under the authority of a base public affairs office.

1.2. Applicability. The guidance in this DAFMAN applies to:

1.2.1. DAF disclosures of CMI and CUI to foreign nationals in support of officially-approved international programs.

1.2.2. DAF decisions for disclosing information (including foreign government information) to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country.

1.2.3. DAF reviews of U.S. contractor requests to export defense articles, services, and technical data controlled by the Department of State's Directorate of Defense Trade Controls or the Department of Commerce's Bureau of Industry and Security.

1.2.4. Foreign government- or international organization- sponsored visits and assignments of foreign nationals or foreign government representatives to DAF facilities that involve access to CMI or CUI.

1.2.5. Notification and approval processes for foreign partner visits that are sponsored, controlled, administered, and recorded by U.S. European Command under its J5/8 Policy, Strategy, Partnering and Capabilities Directorate; U.S. Air Forces in Europe and U.S. Air Forces Africa; U.S. Southern Command; U.S. Northern Command; the Air Force Office of Scientific Research; or by the Department of State's Bureau of Educational and Cultural Affairs.

1.2.6. Unclassified visits by Canadian government officials and certified Canadian contractors under the United States-Canada Joint Certification Program.

1.3. Department of the Air Force Foreign Disclosure Authority.

1.3.1. 22 United States Code (USC) Chapter 39, *Arms Export Control* mandates the regulation of imported and exported defense articles, services, and technical data. 50 USC Chapter 58, *The Export Control Reform Act*, restricts the export of emerging and foundational technologies that can potentially be used for civilian and military purposes. SAF/IAPD and the Deputy Under Secretary of the Air Force, International Affairs Weapons Division (SAF/IAPW) formulate and recommend positions regarding exports of defense articles, services, and technical data to the Defense Technology Security Administration. DAF FDOs authorize disclosures of CMI and CUI under the National Disclosure Policy (NDP-1), *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*. NDP-1 delegates authority to disclose eight categories of CMI to authorized foreign governments and international organizations. See [Attachment 2](#), “National Disclosure Policy Functional Categories of Information,” for a full description of NDP-1 categories.

1.3.2. DAF disclosure authority for CMI. NDP-1 provides national policy and procedures to U.S. executive branch departments and agencies for the disclosure of CMI to foreign representatives. It also delegates general release authority for CMI to the head of the department or agency originating CMI. The Secretary of the Air Force designates the Deputy Under Secretary of the Air Force, International (SAF/IA) as the DAF principal disclosure authority, in accordance with Headquarters of the Air Force Mission Directive (HAFMD) 1-16, *Deputy Under Secretary of the Air Force, International Affairs*, and DAFPD 16-2. SAF/IA designates SAF/IAPD as the DAF designated disclosure authority for CMI.

1.3.3. DAF disclosure authority for CUI. Department of Defense Directive (DoDD) 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, and DoDI 5200.48, *Controlled Unclassified Information (CUI)*, require a positive foreign disclosure decision to be made before CUI is released to a foreign entity. The Secretary of the Air Force designates SAF/IA as the DAF principal disclosure authority in accordance with HAFMD 1-16 and DAFPD 16-2. SAF/IA designates SAF/IAPD as the DAF designated disclosure authority for CUI.

1.3.4. DAF disclosure authority parameters. Consistent with Paragraphs [1.3.2](#) and [1.3.3](#), SAF/IAPD develops and delegates disclosure guidelines for CMI and CUI originated by or for the DAF for purposes such as, but not limited to foreign military sales (FMS); exercises; military training; co-development or co-production programs; international armaments cooperation initiatives; visits of foreign nationals; information requests from foreign nationals; and munitions license requests.

1.3.5. With the consent of the originator, SAF/IAPD develops and delegates disclosure guidelines for CMI or CUI officially obtained from a foreign source, combined military information, joint information, information originated by or for any U.S. department or agency, and proprietary information.

1.3.6. DAF disclosure authority does not extend to the following information:

1.3.6.1. Information marked not releasable to foreign nationals (NOFORN) in accordance with Department of Defense Manual (DoDM) 5200.01V2, *DoD Information Security Program: Marking of Information*.

- 1.3.6.1.1. The dissemination marking “NOFORN” is an intelligence control marking used to identify intelligence that an originator has determined meets the criteria of DoDM 5200.01V2 and that may not be provided in any form to foreign governments (including coalition partners), international organizations, foreign nationals, or immigrant aliens without the originator’s approval. NOFORN is authorized for use only on intelligence and intelligence-related information and products under the purview of the Director of National Intelligence, in accordance with Director of National Intelligence policy, with three exceptions. The exceptions are Naval Nuclear Propulsion Information, the National Disclosure Policy Document (NDP-1), and cover support information in accordance with DoDI S-5105.63, *Implementation of DoD Cover and Cover Support Activities (U)*, each of which may be marked “NOFORN.” Other than these three exceptions, there is no authorized use for the NOFORN caveat on non-intelligence information.
- 1.3.6.1.2. If a security classification guide contains NOFORN as a dissemination caveat and there is a question regarding whether or not it is properly utilized, contact the original classification authority. The original classification authority will consult with AF/A2/6, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations to determine if NOFORN is properly applied in the security classification guide.
- 1.3.6.1.3. DAF personnel must review all material that is not intelligence information for proper markings. **(T-1)**. If dissemination controls are improperly applied, DAF personnel must remove or correct this error in accordance with AFI 16-1404, *Air Force Information Security Program*. DAF personnel will refer to the original classification authority for documents that are marked with “NOFORN” if the document was created from a security classification guide.. **(T-1)**. If it cannot be determined that the document was created from a security classification guide, then DAF personnel will refer the document to AF/A2/6 for guidance. **(T-1)**.
- 1.3.6.2. Information that is originator-controlled in accordance with Intelligence Community Policy Guidance 710.1, *Application of Dissemination Control: Originator Control*.
- 1.3.6.3. Information marked with the words, “Caution – Proprietary Information Involved” in accordance with 18 U.S. Code Section 1905, *Disclosure of Confidential Information Generally*.
- 1.3.6.4. Information marked with a special access required caveat in accordance with DoDM 5200.01V2.
- 1.3.6.5. Information marked Restricted Data or Formerly Restricted Data.
- 1.3.6.6. Information marked as Privileged Safety Information. This information is CUI for mishap prevention purposes only, and may be released in coordination and concurrence with AF/SE.

Chapter 2

ROLES, RESPONSIBILITIES, AND DETAILED PROCEDURES

Section A—Roles and Responsibilities.

2.1. Deputy Under Secretary of the Air Force, International Affairs. Pursuant to HAFMD 1-16 and DAFPD 16-2, the Deputy Under Secretary of the Air Force, International Affairs (SAF/IA) shall serve as the DAF principal disclosure authority. SAF/IA delegates SAF/IAPD as the DAF designated disclosure authority.

2.2. Deputy Under Secretary of the Air Force, International Affairs, Foreign Disclosure and Technology Transfer Program. SAF/IAPD will ensure that CMI and CUI disclosure actions originating within the DAF are consistent with applicable U.S. legislation and policy such as the NDP-1. (T-1). As the DAF designated disclosure authority, SAF/IAPD will perform the tasks listed in the following eleven paragraphs (T-1).

2.2.1. Be the DAF lead and voting member to the National Disclosure Policy Committee.

2.2.2. Be the DAF office of primary responsibility for service recommendations related to export license applications and matters concerning the Department of State's U.S. Munitions List and the Department of Commerce's Commerce Control List.

2.2.3. Be the DAF point of contact to the Joint Atomic Information Exchange Group.

2.2.4. Oversee DAF implementation of NDP-1, the International Traffic in Arms Regulation, and the Export Administration Regulation. This includes developing policies, procedures, and processes for implementation.

2.2.5. Delegate disclosure authority to MAJCOM, field command, DRU, and FOA FDOs through delegation of disclosure authority letters(DDLs). See [Attachment 3](#), which provides an example of a DDL for reference.

2.2.6. Train DAF FDOs to make decisions regarding disclosures of CMI and CUI.

2.2.7. Be the DAF OPR for policy guidance regarding the Security Policy Automation Network (SPAN).

2.2.8. Act as the office of coordinating responsibility for all support issues related to foreign disclosure and technology transfer functions of MAJCOM, field command, DRU, and FOA subordinate elements.

2.2.9. Be the DAF foreign disclosure office.

2.2.10. Approve or deny visits by foreign representatives to subordinate DAF organizations when a MAJCOM, field command, DRU, or FOA FDO is not connected to SPAN.

2.2.11. Approve or deny U.S. government-sponsored visits by foreign representatives to defense contractor facilities.

2.3. Deputy Under Secretary of the Air Force, International Affairs, Weapons Division. SAF/IAPW will carry out the functions detailed in the next two paragraphs. (T-1).

2.3.1. Serve as the OPR for coordinating initiatives within the DAF involving foreign military sales and direct commercial sales (DCS) of DAF systems as well as commercially developed, non-U.S. inventory systems. This coordination process creates baseline export positions. More information about baseline export positions and their waivers and modifications, also known as topline, can be found in [Paragraph 3.4](#).

2.3.2. Provide the DAF and the security cooperation enterprise with weapons system expertise and guidance regarding FMS and DCS.

2.4. MAJCOM, Field Command, DRU, and FOA Commanders. MAJCOM, DRU, and FOA commanders will perform the tasks enumerated in the succeeding four paragraphs. (T-1).

2.4.1. Designate, in writing, one or more individuals as command FDOs who report directly to supervisors in the grade of colonel (O-6) or higher, or GS-15 or higher.

2.4.2. Ensure command FDOs have access to senior command leaders in order to identify and resolve disclosure and technology transfer issues.

2.4.3. Ensure that FDOs have the appropriate number of manpower authorizations, office space, and equipment to effectively perform disclosure duties.

2.4.4. Assign FDOs at ranks or grades equivalent to other DAF personnel in the organization having responsibilities and authorities commensurate with the FDOs.

Section B—Detailed Procedures.

2.5. MAJCOM, Field Command, DRU, and FOA Foreign Disclosure Officers. FDOs at MAJCOMs, field commands, DRUs, and FOAs will fulfill the responsibilities listed in the following nine paragraphs. (T-1).

2.5.1. Authorize disclosures of CMI and CUI in accordance with this manual, established DAF procedures, and DDLs within delegated authorities.

2.5.2. Exercise their delegated disclosure authorities consistent with established DAF suspenses.

2.5.3. Implement DAF disclosure and technology transfer processes for their supported activities and develop local requirements, as necessary.

2.5.4. Further delegate disclosure authority to subordinate FDOs, as necessary, and when specifically authorized by SAF/IAPD.

2.5.5. Approve or deny visits by foreign representatives to their MAJCOM, field command, DRU, or FOA locations, as well as to their subordinate activities.

2.5.6. Forward recommendations to SAF/IAPD to approve or deny visits by foreign representatives to their MAJCOM, field command, DRU, FOA, or subordinate locations, when not electronically connected to the SPAN.

2.5.7. Establish foreign disclosure education and oversight programs for subordinate command FDOs and MAJCOM, field command, DRU, or FOA personnel.

2.5.8. Ensure that contact officers are in place and appropriately trained to support each approved visit in the Foreign Visit System.

2.5.9. Provide SAF/IAPD with current, accurate information on all appointed MAJCOM, field command, DRU, FOA, and subordinate command tenant and element FDOs. This information will include name, grade, functional address symbol, mailing address, telephone numbers, and classified and unclassified e-mail addresses.

2.6. Installation and Garrison Commanders. Installation and garrison commanders will perform the tasks detailed in the next three paragraphs. **(T-1).**

2.6.1. Designate, in writing, one or more individuals as installation or garrison FDOs, as required. Installation and garrison FDOs report directly to supervisors in the grade of colonel (O-6) or higher, or GS-15 or higher.

2.6.1. **(EGLINAFB)** The OPR for Foreign Disclosure for Eglin Air Force Base (EAFB) is the Eglin Foreign Disclosure Office (96 TW/IPF).

2.6.2. Ensure that foreign disclosure offices have the appropriate number of manpower authorizations, office space, and equipment to perform disclosure duties effectively.

2.6.2. **(EGLINAFB)** To provide better service to the Eglin community, 96 TW/IPF assigned Foreign Disclosure Officers (FDO) to various organizations on Eglin to include 96 TW, and 33 FW.

2.6.3. Assign FDOs at ranks or grades equivalent to other DAF personnel in the organization having responsibilities and authorities commensurate with the FDOs.

2.7. Installation and Garrison Foreign Disclosure Officers. Installation and garrison FDOs will carry out the duties enumerated in the succeeding five paragraphs. **(T-1):**

2.7.1. Authorize disclosures of CMI and CUI in accordance with this manual, established DAF procedures, and DDLs within delegated authority.

2.7.2. Implement DAF disclosure and technology transfer processes for their supported activities and develop local requirements, as necessary.

2.7.2. **(EGLINAFB)** FDOs will keep a record of all foreign disclosure/foreign visit activities in their respective units, to include:

2.7.2.1. **(Added-EGLINAFB)** Number of foreign visits processed and how long it took to process the visit.

2.7.2.2. **(Added-EGLINAFB)** Number of documents processed for release, the number approved for release, and how long it took to process the request.

2.7.2.3. **(Added-EGLINAFB)** Number of overseas travel packages (AFMC Form 193, *Foreign Travel Worksheet*) processed.

2.7.3. Approve or deny visits by foreign representatives to their supported organizations when electronically connected to SPAN, or make such recommendations to their MAJCOM, field command, DRU, or FOA FDO when SPAN Network is not available.

2.7.4. Establish an initial and refresher foreign disclosure education program for personnel assigned to supported organizations.

2.7.5. Ensure an assigned contact officer is in place and cognizant of the disclosure conditions and limitations for each approved visit in the Foreign Visit System.

2.8. Commanders/Directors of Tenant Organizations. Commanders/directors of tenant organizations are supervisors in the grade of colonel (O-6) or higher, or GS-15 or higher. Commanders/directors of tenant organizations will fulfill the responsibilities listed in the following five paragraphs. **(T-1).**

2.8.1. Designate FDOs for their own activities, as required.

2.8.2. Request the establishment of new foreign disclosure offices from their MAJCOM or field command disclosure office. Requests need to justify why support from existing FDOs is not practical.

2.8.3. Ensure that visits by foreign representatives to their organizations are processed consistently with installation and garrison foreign disclosure procedures.

2.8.4. Ensure that foreign disclosure offices have the appropriate number of manpower authorizations, office space, and equipment to perform disclosure duties effectively.

2.8.5. Assign FDOs at ranks or grades equivalent to other DAF personnel in the organization who have responsibilities and authority commensurate with the FDOs.

2.9. Tenant and Element Foreign Disclosure Officers. Tenant FDOs and element FDOs support DAF elements, as defined by AFI 38-101, *Manpower and Organization*. Tenant FDOs and element FDOs will perform the duties detailed in the next five paragraphs. **(T-1).**

2.9.1. Authorize disclosures of CMI and CUI in accordance with this manual, established DAF procedures, and DDLs within delegated authority.

2.9.2. Implement DAF disclosure and technology transfer processes for their supported activities and develop local requirements, as necessary.

2.9.3. Approve or deny visits by foreign representatives to their supported organizations when electronically connected to SPAN, or make such recommendations to their MAJCOM, field command, DRU, or FOA FDO when SPAN is not available.

2.9.4. Establish an initial and refresher foreign disclosure education program for personnel assigned to supported organizations.

2.9.5. Ensure an assigned contact officer is in place and cognizant of the disclosure conditions and limitations for each extended visit in the Foreign Visit System.

2.10. Security Cooperation Officers. Security cooperation officers (SCOs) are individuals designated in writing by the security cooperation office chief to oversee and maintain the custody of each Security Cooperation Information Portal token within the security cooperation organization. SCOs must fulfill the responsibilities enumerated in the succeeding three paragraphs. **(T-0).**

2.10.1. Report to SAF/IAPD any confirmed or suspected violations by foreign persons of U.S. government security conditions and requirements contained in applicable letters of offer and acceptance (LOAs), memoranda of understanding, memoranda of agreement, military information security agreements or other international agreements or written arrangements.

2.10.2. Advise representatives of foreign governments to submit their requests for visits or information through their embassy in Washington, D.C.

2.10.3. Submit all issues involving disclosure of DAF military information for resolution with SAF/IAPD and to the host government through the appropriate SAF/IA country director.

2.11. Foreign Disclosure Representatives. Contractors, otherwise known as foreign disclosure representatives (FDRs), may support NDP-1 functions, subject to the following criteria:

2.11.1. FDRs will not exercise foreign disclosure decision authority for disclosures of CMI or CUI, or any other duties considered to be inherently governmental, in accordance with the Federal Acquisition Regulation, Subpart 7.5, *Inherently Governmental Functions*. **(T-0)**.

2.11.2. FDRs are authorized to research and conduct analyses of technical, operational, policy, political, and military factors related to proposed international programs.

2.11.3. FDRs may draft supporting justification and disclosure guidance for international programs.

2.11.4. FDRs may perform administrative functions, such as coordination of disclosure initiatives and recordkeeping related to disclosure activities.

2.12. DAF Contact Officers. DAF contact officers are DAF officials designated as points of contact for extended visits by foreign representatives of governments or international organizations. In this role, contact officers will carry out the duties listed in the following five paragraphs. **(T-1)**.

2.12.1. Maintain a file for each extended visit for which they are the contact officer. At a minimum, the file includes a copy of the extended visit authorization, verification of the basis for the visit, the security plan, the certification form signed by the foreign national, and any coordination or approval records for visits to other locations.

2.12.2. Ensure the visitor understands his or her duties, the terms and conditions of physical access to the organization, and obligations, rights, and responsibilities.

2.12.3. Ensure the visitor signs the certification form (an example can be found in [Attachment 13](#) and [Attachment 14](#)).

2.12.4. Ensure the visitor only accesses CMI and CUI that has been authorized by the FDO in order to perform their assigned duties.

2.12.5. Ensure the visitor's coworkers are informed of the limitations on visitor's access to information.

Chapter 3

DEPARTMENT OF THE AIR FORCE FOREIGN DISCLOSURE AUTHORITY

3.1. Introduction and Overview. DAF FDOs authorize disclosures of CMI and CUI to foreign representatives. This chapter reviews disclosure criteria; processes for handling requests that exceed general DAF disclosure authority; coordination of disclosures involving military equipment; further delegation of DAF disclosure authority; documentation of delegated disclosure authorities; and dissemination of delegation of disclosure authority letters.

3.2. Disclosure Criteria. SAF/IAPD and DAF FDOs will ensure that all disclosures of CMI and CUI satisfy NDP-1 criteria. **(T-0)**. The following are those NDP-1 criteria:

- 3.2.1. Disclosure is consistent with U.S. foreign policy and national security objectives concerning the foreign government or international organization.
- 3.2.2. Disclosure is consistent with U.S. military and security objectives.
- 3.2.3. The foreign recipient ensures that the U.S. information will be given the same degree of security protection as would be provided by the United States.
- 3.2.4. Disclosure results in a clearly-defined benefit for the United States.
- 3.2.5. Disclosure is limited to the information necessary to the purpose for which disclosure is made.

3.3. Requests That Exceed DAF General Disclosure Authority. Requests for disclosure approval that exceed DAF disclosure authority may be authorized by the National Disclosure Policy Committee (NDPC) if they satisfy all disclosure criteria. The NDPC approves exceptions to NDP-1, which are often referred to as exceptions to National Disclosure Policy. An NDPC decision may be appealed to the Deputy Secretary of Defense.

3.3.1. SAF/IAPD and DAF FDOs must ensure that requests for exceptions to National Disclosure Policy contain elements required by the Department of Defense (DoD). **(T-0)**. The following eight paragraphs are those elements:

- 3.3.1.1. A concise statement of the action being proposed and why an exception to NDP-1 is needed.
- 3.3.1.2. A detailed, technical description of the equipment or information to be disclosed. The description will be provided by the office requesting disclosure approval.
- 3.3.1.3. An assessment of how each of the disclosure criteria and conditions in [Paragraph 3.2](#) is met. The assessment of criteria and conditions will be provided by the office requesting disclosure approval.
- 3.3.1.4. Identification of any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure timing, or other relevant caveats that may affect NDPC or Military Intelligence Disclosure Policy Committee approval or denial of the request.
- 3.3.1.5. A statement noting if the exception is continuing and subject to annual review, or a one-time exception.

3.3.1.6. A U.S. embassy country team assessment and theater combatant commander endorsement of the proposed disclosure. The country team assessment and combatant commander endorsement will be provided by the office requesting disclosure approval.

3.3.1.7. The recommendation of other interested departments or agencies, if joint service or shared information is involved in the disclosure request.

3.3.1.8. Any other information that would assist the NDPC members in evaluating the proposal.

3.3.2. SAF/IAPD coordinates with the NDPC and the agency originating the information as required to obtain disclosure authority. After receiving all required inputs from functional offices, SAF/IAPD usually requires 10 working days to complete coordination within the DAF before submission to the NDPC. The NDPC usually concludes its review in 10 working days.

3.4. Coordination of Disclosures Involving Military Equipment. Exports of military equipment, defense services, technologies, or capabilities constitute disclosures of information and are subject to the requirements of this manual. Disclosure initiatives that involve foreign military sales or direct commercial sales of DAF systems or commercially-developed, non-U.S. inventory systems are coordinated and approved in accordance with the DAF baseline for that commodity. SAF/IAPW is the DAF office of primary responsibility for DAF baselines. DAF baselines are solely a service position and function independently from NDP-1. Adjustments to DAF baselines are called topline and may be in the form of a permanent modification or a temporary waiver. Both permanent modifications and temporary waivers are staffed on a case-by-case basis when the DAF baseline does not appropriately address the specific commodity. A topline carries the same weight as the baseline for its specified duration and must be signed by the applicable authority, as delineated in the most current approved baseline. As a rule, waivers apply to a single event. There are limited instances where a waiver may be made to a baseline, as is the case for tactics waivers that allow a country to temporarily access higher-level tactics and information during a coalition exercise, e.g., Exercise RED FLAG. Baselines and topline are not widely disseminated and are held for in-person review by SAF/IAPW.

3.4.1. Baselines are foundational, Secretary of the Air Force-approved, enduring DAF policy positions on the export of weapons, weapons systems, and related technologies and information. Pursuant to HAFMD 1-16, HAFMD 1-4, *Chief of Staff of the Air Force*, and the MD ultimately assigned to the Chief of Space Operations. The Secretary of the Air Force has delegated authority to designate, approve, modify, or waive provisions of DAF export baselines and their associated topline to the Chief of Staff of the Air Force (CSAF), Chief of Space Operations, and SAF/IA in accordance with *Delegation of Authority Regarding Department of the Air Force (DAF) Export Baseline Positions* memo dated March 20, 2020 and signed by the Secretary of the Air Force. A copy of this memo can be provided by SAF/IAPD or SAF/IAPW.

3.4.1.1. Each proposed baseline is broadly coordinated by SAF/IA with the appropriate DAF agencies at the division and directorate level, as well as geographic component commands. Coordination staffing includes: Air Combat Command; Air Education and Training Command; Air Mobility Command; Air Force Material Command; Pacific Air Forces; U.S. Air Forces in Europe and U.S. Air Forces Africa; Intelligence Surveillance and Reconnaissance and Cyber Effects Operations (AF/A2/6); Operations, Plans, and Requirements (AF/A3); Logistics, Engineering, and Force Protection (AF/A4); Strategy Integration and Requirements (AF/A5); Plans and Programs (AF/A8); National Air and Space Intelligence Center; Administrative Assistant to the Secretary of the Air Force (SAF/AA); Acquisitions (SAF/AQ); Deputy Chief Information Officer (SAF/CN); Judge Advocate General (AF/JA); and General Counsel (SAF/GC), at a minimum, before baseline signature.

3.4.1.2. Baselines are used to represent DAF equities in key DoD interagency disclosure and technology release processes, to include the Office of the Secretary of Defense for Acquisition and Sustainment; the Low Observable/Counter-Low Observable Executive Committee, and the NDPC.

3.4.1.3. Baselines are anticipatory in nature and merge potential international partners' requests with current and developing positions, capabilities, and technologies.

3.4.1.4. Exports of military equipment and capabilities that are supported by an existing baseline do not require creation of a topline.

3.4.2. In the event that a DAF baseline requires modification, a topline is required to adjust the baseline position. If topline authority and coordination procedures are not stated in the baseline, the following topline procedures will apply:

3.4.2.1. SAF/IAPD and DAF FDOs will ensure that each proposed topline contains the elements required for approval. **(T-0)**. The following five paragraphs are those required elements:

3.4.2.1.1. A thorough description of what is proposed for sale. This description will be provided by the office requesting disclosure approval.

3.4.2.1.2. An explanation of the benefits for the United States. This explanation of benefits will be provided by the office requesting disclosure approval.

3.4.2.1.3. An evaluation of the risk of compromise or unintended end-use based, for example, on the existence of general security of military information agreement, NDPC country security surveys, and intelligence community assessments.

3.4.2.1.4. An assessment of foreign availability of similar weapons systems, technologies, or capabilities. This assessment will be provided by the office requesting disclosure approval.

3.4.2.1.5. A description of precedent cases, previous or related toplines, if applicable.

3.4.2.2. Specific staffing requirements for topline are often further refined within each applicable baseline. Absent additional clarification within the parent baseline, DAF members will coordinate topline through Air Combat Command; Air Education and Training Command; Air Mobility Command; Air Force Materiel Command; Pacific Air Forces; U.S. Air Forces in Europe and U.S. Air Forces Africa ; AF/A2/6; AF/A3; AF/A4; AF/A5; AF/A8; National Air and Space Intelligence Center; SAF/AA; SAF/AQ; SAF/CN; AF/JA, SAF/GC, and approved by CSAF. **(T-1)**. These staffing requirements apply for the following conditions:

3.4.2.2.1. Low observable and counter-low observable capabilities or technologies are involved.

3.4.2.2.2. The proposed sale results in foreign access to U.S. classified software source code.

3.4.2.2.3. The system, technology, or capability is unique to the United States, meaning no equivalent substitutes are available from foreign sources, and provides the DAF with a significant military advantage over potential adversaries.

3.4.2.2.4. The United States has no effective countermeasures or defenses against the system or capability.

3.4.2.2.5. The proposed recipient government's ability or willingness to protect U.S. military information or use it for the intended U.S. purpose is doubtful.

3.4.2.2.6. The system proposed for sale is derived from a special access program.

3.4.2.3. Absent clarification within the parent baseline, topline for proposed foreign sales initiatives that involve any of the following items are coordinated at the directorate level in SAF/AQ; SAF/CN; SAF/GCI; AF/JA; AF/A2/6; AF/A3; AF/A4, AF/A5, AF/A8; and approved by SAF/IA:

3.4.2.3.1. Aircraft and air vehicles.

3.4.2.3.2. Jet or rocket engines.

3.4.2.3.3. Precision-guided munitions and precision targeting systems.

3.4.2.3.4. Unmanned aerial vehicles.

3.4.2.3.5. Night and adverse weather terrain avoidance flight navigation systems.

3.4.2.3.6. Radars.

3.4.2.3.7. Intelligence collection systems.

3.4.2.3.8. Command, control, and communications systems.

3.4.2.3.9. Cyber operations and defensive countermeasure systems.

3.4.2.3.10. Ballistic missile defense systems.

3.4.2.3.11. Unclassified software source code for any of the aforementioned items.

3.4.2.4. In instances when the coordinating agencies cannot reach consensus on a proposed topline, dissenting recommendations are elevated to the appropriate assistant secretary or deputy chief of staff, or to CSAF (if necessary) for resolution.

3.4.2.5. If a coordinating office recommends non-concurrence with a proposed topline, they must provide a reason for non-concurrence that includes any conditions and limitations that can be placed on the proposed sale that would be sufficient for the coordinating office to concur with the proposed sale. **(T-1)**. The coordinating office must base justification for non-concurrence on substantiated risk to U.S. military security, national security, or foreign policy objectives. **(T-0)**.

3.5. Delegation of DAF Disclosure Authority. SAF/IAPD relies on delegation to ensure that disclosure decisions are made promptly and effectively. After satisfying the disclosure criteria identified in [Paragraph 3.2](#), or obtaining approval from the appropriate authority, SAF/IAPD may delegate specific disclosure authorities to be exercised by DAF FDOs. Delegation may occur as detailed below:

3.5.1. SAF/IAPD may delegate disclosure authority to MAJCOM, field command, DRU, or FOA FDOs.

3.5.2. MAJCOM, field command, DRU, or FOA FDOs may further delegate disclosure authority to their subordinate FDOs in order to support international programs, foreign requests for information, or foreign visits.

3.5.3. FDOs will notify DAF personnel responsible for implementation of international programs when they receive disclosure guidance related to their program. **(T-1)**.

3.6. Documentation of Delegated Disclosure Authority. SAF/IAPD is the approval authority for delegated disclosure authority to MAJCOM, field command, DRU, and FOA FDOs, in support of both one-time and continuing disclosure requirements. One-time disclosure authorizations may be documented in a specific memorandum or visit authorization. Requirements for continuing information disclosures are documented in the delegation of disclosure authority letter.

3.6.1. If disclosure of information is required to support an international program before a DDL is issued, SAF/IAPD will approve disclosure guidance to support the program until the DDL is approved.

3.6.1. **(EGLINAFB)** Submit Delegation Disclosure Letter (DDL) drafts to organizational FDOs for review and coordination.

3.6.2. To establish disclosure guidance for new international programs:

3.6.2.1. Proponents for international programs will identify program objectives, program information proposed for disclosure, the classification of the information, and the originator of the information proposed for disclosure to their supporting FDO. **(T-1)**.

3.6.2.2. Proponents will assist the FDO in documenting how the new international program satisfies the disclosure criteria in [Paragraph 3.2](#). **(T-0)**.

3.6.2.3. FDOs supporting international programs will participate in initial and continuing international program planning activities, as needed, to ensure that disclosure guidance will be developed and coordinated at the local levels and forwarded to SAF/IAPD in advance of program activities beginning. **(T-0)**.

3.6.2.4. Servicing FDOs will forward requests for initial or updated program disclosure guidance, including the evaluation of disclosure criteria, through their MAJCOM, field command, DRU, or FOA FDO to SAF/IAPD. **(T-0)**.

3.6.2.5. FDOs will coordinate requests for disclosure guidance with all command offices that have a functional interest in the program and the information to be disclosed, before forwarding the request to SAF/IAPD.

3.6.2.6. For international armaments cooperation programs, MAJCOM and field command FDOs will forward MAJCOM- and/or field command-approved DDLs to The International Armaments Cooperation Division, Directorate of Policy Programs & Strategy, Deputy Under Secretary for International Affairs as part of the coordination package.

3.6.2.7. The servicing FDO will prepare and forward proposed DDLs to SAF/IAPD through the MAJCOM, field command, DRU, or FOA FDO for international initiatives that originate within subordinate elements. **(T-1)**.

3.6.2.8. FDOs will ensure that proposed DDLs are consistent with the format in [Attachment 3](#). **(T-1)**.

3.6.2.9. SAF/IAPD will prepare and approve DDLs for disclosure initiatives that originate at the DAF and service headquarters level.

3.7. Dissemination of Delegation of Disclosure Authority Letters. SAF/IAPD limits dissemination of DDLs to FDOs only. DDLs cannot be disseminated to non-foreign disclosure officers unless explicitly permitted, in writing, by SAF/IAPD. Broader dissemination increases the risk of misinterpretation and disclosure approvals made by unauthorized individuals. However, in circumstances that warrant dissemination outside of FDO offices, the following guidelines apply:

3.7.1. MAJCOM and field command FDOs with delegated authority to disseminate the information in the DDL to subordinate FDOs may approve requests for information copy provisioning to DAF offices they support that are within their command.

3.7.1.1. Upon approval from SAF/IAPD, FDOs may provide information copies of DDLs to DAF offices to guide international program development; support assignment of foreign representatives in DAF organizations; or facilitate sanitization of information in preparation for disclosure review.

3.7.1.2. FDOs can only provide DDL copies outside of FDO channels with the explicit approval of Chief, SAF/IAPD. The approval decision is based on a program proponent's need for frequent access to the DDL in cases that physical separation from the FDO office makes it impractical to regularly review the DDL.

3.7.2. The FDO will transmit the DDL under a cover memo that specifically documents why the DDL is being provided. **(T-1)**. FDOs and non-foreign disclosure officers must ensure that the transmittal statement remains attached to the DDL. **(T-1)**. A sample transmittal memo is located in [Attachment 4](#).

3.7.3. For DDLs disseminated outside of FDO channels, FDOs must include in the transmittal memo the following statement, placed in a conspicuous location: "This DDL is for information only. It does not constitute authority to release equipment, technology, or information and may not be used for such purpose. This DDL may not be copied in whole or in part. Information contained in the DDL may not be incorporated into other documents." **(T-1)**.

3.7.4. Delegations of DAF disclosure authority outside of the DAF requires SAF/IAPD written approval. Proponents for such delegations must justify their requests, in writing, to SAF/IAPD using FDO channels. (T-1).

Chapter 4

PROGRAM MANAGEMENT

4.1. Program Management Requirements. National Disclosure Policy requires that all departments and agencies responsible for implementation of NDP-1 issue directives and instructions to assure that disclosure decisions are made promptly and that disclosure activities under their jurisdiction are carried out effectively. SAF/IAPD supports the implementation, management, and evaluation of MAJCOM, field command, DRU, and FOA Foreign Disclosure and Technology Transfer Programs, per AFI 90-201, *The Air Force Inspection System*. To this end, the following program management requirements have been developed:

4.2. Standard Suspense Requirements for Disclosure Activities. In order to respond promptly to disclosure requests made by supported activities, FDOs will track their response times for document requests and foreign visit requests. **(T-1)**.

4.2.1. SAF/IAPD will respond to document requests within 10 working days from the date of receipt. In this 10-day period, FDOs will approve, deny, return without action, coordinate an extension, or refer the request to the appropriate disclosure authority. **(T-1)**. FDOs will return without action requests lacking sufficient information to make a disclosure decision. **(T-0)**.

4.2.2. For foreign visit requests:

4.2.2.1. The DAF standard for responding to one-time visit requests is no later than 30 calendar days in advance of the visit start date.

4.2.2.2. One-time visit requests that are received less than 15 calendar days prior to the visit start date are considered to be emergency visits; and the approving official will process the request as quickly as possible, although processing is not guaranteed. **(T-1)**.

4.2.2.3. The approving official will respond to requests for recurring and extended visits within 30 calendar days of receipt of a visit request or prior to any visit or assignment of a foreign representative. **(T-1)**.

4.3. Training Requirements. Only trained FDOs are authorized to disclose CMI or CUI to foreign representatives. Prior to authorizing disclosures of CMI and CUI, FDOs must complete the DAF Foreign Disclosure Officer Training Course sponsored by SAF/IAPD or an equivalent MAJCOM or field command Foreign Disclosure Officer Training Course. **(T-1)**. In lieu of self-assessment communicators in the management control toolset, MAJCOMs and field commands shall establish foreign disclosure education and oversight programs and self-inspection programs for subordinate command/wing FDOs and MAJCOM, field command, DRU, or FOA personnel. **(T-1)**. The MAJCOM and field command FDOs will provide requisite training; certification, and recertification when required for FDOs of subordinate organizations within their chain of command. **(T-1)**.

4.4. Waivers to DAF Foreign Disclosure Policy. SAF/IAPD will consider and may approve DAF requests to waive disclosure policy and procedures when the policy will negatively affect an international DAF program and the waiver does not conflict with U.S. law, policy, or procedures. Only personnel in the grade of O-6 or higher or GS-15 or higher have authority to sign requests for waivers to this manual. Each waiver should be submitted through local FDO channels to SAF/IAPD. The requestor must identify in writing the requirements listed in the next four paragraphs. **(T-1).**

4.4.1. The specific policy to be waived.

4.4.2. The specific impact if the policy is not waived.

4.4.3. The reasons why the policy cannot be met.

4.4.4. The procedures that will be implemented until the waiver expires. Proponents must ensure that these procedures meet the intent of DAF disclosure and technology transfer policy. **(T-1).**

Chapter 5

DISCLOSING INFORMATION

5.1. Introduction. Foreign disclosure officers (FDOs) authorize disclosures of classified military information (CMI) and controlled unclassified information (CUI) to foreign representatives. DAF information that has been officially approved for public release or is unclassified and not controlled under U.S. export control regulations does not require FDO approval before being disclosed to a foreign government or international organization. Disclosures are made for various reasons, including:

5.1. (EGLINAFB) Eglin FDOs must. Grant approval before releasing Classified Military Information (CMI) or Controlled Unclassified Military Information (CUMI) documents or material to a foreign government or international organization. Approval is required regardless of the way the information is transmitted (e.g., in person, by telephone, correspondence, electronic means).

5.1.1. Responses to written requests for information related to FMS and/or DCS.

5.1.2. Armaments cooperation agreements.

5.1.3. General DAF activities.

5.1.4. Visits by foreign representatives.

5.1.5. Exercises or operational activities.

5.2. Methods of Disclosure. Information can be disclosed in oral, visual, or documentary methods. Documentary disclosures occur when control of information in tangible form (e.g., equipment or written materials) is transferred to a foreign government or international organization.

5.3. Submitting Requests to Disclose Information.

5.3.1. Deputy Under Secretary of the Air Force, International Affairs (SAF/IA) country directors submit foreign embassy requests for CMI or CUI to the MAJCOM, field command, DRU, or FOA FDOs with disclosure authorities over the requested information. SAF/IAPD will assist country directors, as necessary. Unless other government-to-government channels are established, foreign governments and international organizations should submit requests for information through their accredited attaché in Washington D.C. or their security cooperation officer (SCO) in country.

5.3.2. DAF personnel will submit requests to their servicing FDO for disclosures of CMI or CUI to foreign recipients in the U.S. or abroad. **(T-1)**.

5.3.2.1. Foreign representatives designated by their governments to conduct business with the DAF should use established procedures to submit requests related to specific FMS programs or international armaments cooperation agreements. Such requests are submitted through the in-country security cooperation office (SCO) to DAF individuals that have been appointed as case managers or technical project officers. The case manager or technical project officer will submit requests to the servicing FDO. **(T-1)**.

5.3.2.2. The actual transfer of U.S. technical data to foreign representatives is pursuant to an FMS case, loan, lease or grant agreement, export license, or cooperative agreement.

5.3.3. DAF proponents must provide a written request to their servicing FDO. **(T-1)**. Failure to provide sufficient information in the disclosure request may result in a request returned without action and a determination that more information is required.

5.3.3.1. The DAF proponent will provide the FDO with a detailed and concise foreign disclosure request to the SAF/IAPD workflow email. **(T-1)**. The request must include the following information:

5.3.3.1.1. The purpose for the specific information sought (e.g., third party transfer, FMS Case, request for data or information, briefing clearance, conference attendance, visits, etc.).

5.3.3.1.2. Requested completion date.

5.3.3.1.3. The defense article, service, or technical data proposed for disclosure. This should include specific information, such as the item's make, model, version, etc.

5.3.3.1.4. The highest level of classification of release sought for the defense article, service, or technical data.

5.3.3.1.5. The originator or owner for the defense article, service, or technical data (e.g., DAF, other service, commercial, international partner, etc.)

5.3.3.1.6. Information on what the foreign disclosure release will support (e.g., its relation to DAF, DoD, or U.S. government building partnership capacity initiatives).

5.3.3.1.7. The proposed end-use or end-user for this article.

5.3.3.1.8. Information indicating whether the defense article, service, or technical data was originally part of an FMS or DCS case; the original acquisition value; and the FMS case number, if applicable.

5.3.3.1.9. The DAF equities associated with the defense article, service, or technical data. If there are other services or agencies with equities, include points of contact from the respective service or agency.

5.3.3.1.10. Specific information on any other political or military factors that would further support the recommendation to disclose, deny, or defer the requested information.

5.3.3.1.11. Existing precedent for the case, previous related disclosure requests, and/or records of action that may be relevant to the case.

5.3.3.2. If the disclosure action is based on a written request from a foreign government or international organization, the sponsoring DAF proponent will not be required to submit an additional request. **(T-1)**. The request from a foreign government or international organization should contain the following information:

5.3.3.2.1. The proposed foreign recipient, including country, classification of information to be disclosed, and originator of the information.

5.3.3.2.2. The purpose of the disclosure (e.g., FMS program, armaments cooperation agreement, operational or exercise requirement, etc.).

5.3.3.2.3. The benefit the U.S. is expected to receive from the disclosure or the resulting impact expected if the request is denied.

5.3.3.2.4. For documentary disclosures, the sponsoring DAF proponent must provide a copy of the document to be disclosed and identify any portions of the document that are not part of the disclosure request.

5.3.3.2.5. For oral and visual disclosures, the sponsoring DAF proponent must provide written details identifying information to be discussed.

5.3.3.2.6. Requested release date.

5.3.3.3. DAF organizations will obtain assistance from their servicing FDOs when receiving requests directly from foreign governments and international organizations.

5.4. Processing Requests to Disclose Information. FDOs coordinate disclosure proposals with offices that have a functional interest, including interests within a geographic combatant command area of responsibility. This coordination ensures the evaluation of programmatic, policy, operational, technological, and security related issues. Enlisted subject matter experts should provide assessments within their functional area.

5.5. Approving Requests to Disclose Information.

5.5.1. FDOs approve disclosure requests consistent with their delegated disclosure authority. FDOs will ensure disclosure approvals are consistent with [Attachment 6](#) and [Attachment 7](#). (T-1).

5.5.1.1. When continuing authority is appropriate, FDOs will assist DAF proponents in requesting a new DDL or revising a current DDL, as required. (T-1).

5.5.1.2. If a request exceeds the FDO's delegated authority, the FDO will forward the request, including information from [Paragraph 5.3.3](#) through their MAJCOM, field command, DRU, or FOA FDO to SAF/IAPD. (T-1).

5.5.1.3. FDOs must include within disclosure requests the information required by [Paragraph 5.3.3.1](#). (T-1).

5.5.2. FDOs will ensure information from the next three paragraphs is contained in approvals to disclose information. (T-1).

5.5.2.1. Bibliographies, reference lists, and distribution lists are removed when these references are not, or would not be, approved for release to the recipient country.

5.5.2.2. The following statement, which must be stamped or typed on the front page or cover page of documents that contain CMI or CUI: "This information is furnished on the condition that it will not be released to another nation without specific authority of the Department of the Air Force of the United States; that it will be used for military purposes only; that individual or corporate rights originating in the information, whether patented or not, will be respected; that the recipient will report promptly to the United States any known

or suspected compromise; and that the information will be provided substantially the same degree of security afforded to it by the Department of Defense of the United States. Also, regardless of any other markings on the document, it will not be downgraded or declassified without written approval of the originating U.S. agency.”

5.5.2.3. The following statement is included at the beginning of electronic media containing CMI or CUI: “This information is furnished on the condition that it will be given substantially the same degree of security protection given to it by the United States and will not be released to another nation without Department of the Air Force authorization.”

5.5.3. FDOs will ensure the information in the next four paragraphs is included in all foreign disclosures. **(T-1)**.

5.5.3.1. “The U.S. government sponsor is responsible to ensure that U.S. participants, including government and contractors, that are involved in technical discussions of U.S. export-controlled or classified information during briefings, meetings, conferences, or events are provided advance notification of the approved scope and limitations of this disclosure decision.”

5.5.3.2. “To reduce the risk associated with latent metadata capture in digital products, documentary release is limited to paper copy only. When mission requirements dictate and are acknowledged by the responsible U.S. government authority, the release of digital products is permitted in read-only .pdf or .tif format.”

5.5.3.3. “Prepare the briefing by adding ‘Controlled Unclassified’ as a header and footer to the title page and each subsequent page containing CUI if appropriate.” Portion mark all CUI paragraphs, bullets, sub-bullets, and notes pages ‘CUI’ and all CUI graphic depictions, pictures, or charts ‘Controlled Unclassified,’ where applicable. Presentations must conform to the security classification marking requirements stipulated in AFI 16-1404.”

5.5.3.4. “Discussions and documentary release beyond the contents of this release authorization will require a separate disclosure review.”

5.6. Actions Prior to Disclosing Information.

5.6.1. DAF proponents will ensure that all disclosures to foreign representatives are consistent with guidance received from the servicing FDO. **(T-0)**.

5.6.2. DAF proponents will ensure that information not approved for foreign disclosure is removed from the materials prior to disclosure. **(T-0)**.

5.6.3. DAF proponents will verify to the servicing FDO the date that the disclosures of CMI and CUI were made. **(T-0)**.

5.6.4. CMI is transferred on a government-to-government basis. These transfers should be made through government-to-government channels, unless another channel is mutually agreed upon by the appropriate policy authorities of the sending and receiving governments. FDOs or DAF proponents will use Air Force Form 349, *Receipt for Documents Released to Accredited Representatives of Foreign Nations*, when transmitting CMI to a foreign government or international organization. **(T-1)**. DAF organizations releasing CMI must maintain forms as prescribed in the Air Force Records Disposition Schedule. **(T-1)**.

5.7. Disclosures Not Requiring FDO Authorization. When all of the following conditions are met, DAF personnel do not require FDO authorization to disclose unclassified information:

5.7.1. The intended recipient is a representative of a foreign government or international organization and the information is being provided for an official DAF purpose. DAF personnel must ensure any information to be provided to the general public, including foreign nationals, must be released in accordance with the provisions of AFI 35-101, *Public Affairs Operations*.

5.7.2. The information is related to the roles, missions, doctrine, organization, and general capabilities of the DAF, MAJCOMs, field commands, or any subordinate units; general information on the function, purpose, and general capabilities and characteristics of defense equipment or general scientific, mathematical or engineering principles commonly taught in schools, colleges, or universities.

5.7.3. The information is not CUI.

5.7.4. No access or distribution limitations have been applied to the information in accordance with applicable U.S. or foreign laws or regulations.

5.7.5. The disclosure is for informational purposes only. There is no U.S. government intent to sell, loan, lease, co-develop, or co-produce International Traffic in Arms Regulations (ITAR)-related defense articles.

5.7.6. The following statement is conspicuously displayed at the front or beginning information: “This briefing, presentation, or document is for information only. No U.S. government commitment to sell, loan, lease, co-develop, or co-produce defense articles or provide defense services is implied or intended.”

5.7.7. There is no foreign national participation in any operational or exercise activities, support for any current FMS or armaments cooperation program, or assignment of foreign nationals to DAF security cooperation-related organizations.

5.7.8. Originator consent for the disclosure is obtained.

5.8. Foreign Contractor Attendance at Symposia, Conferences, and Contract-Related Meetings. U.S. contractors are required to submit an export license or use an authorized ITAR exemption to sponsor a foreign contractor’s attendance at gatherings that include DoD-classified information or other ITAR-controlled information, if not already approved through an export license granted by the Department of State’s Directorate of Defense Trade Controls. The appointment of a DoD security sponsor for classified meetings involving foreign contractor participants does not exempt U.S. contractors from ITAR licensing requirements.

5.9. Foreign Access to DAF Information Systems. AFI 17-130, *Cybersecurity Program Management*, describes requirements for access to DAF information systems and is applicable to foreign nationals. Information owners determine foreign national access to DAF information systems with access guidance provided in the system security plan. For more details, see AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*. Foreign national approval to connect to the Secure Internet Protocol Routing Network, Non-classified

Internet Protocol Router Network, or other networks does not equate to authority to disclose data or access systems located on that network. Disclosure review by the servicing FDO is a prerequisite for access to information residing in Secure Internet Protocol Routing Network, Non-classified Internet Protocol Router Network, or other networks.

5.10. Technical Orders. DAF technical orders are government-furnished equipment and, in accordance with 22 USC Chapter 39, may not be exported except when they support sales of U.S. government furnished equipment.

5.10.1. DAF technical orders may be released to a foreign contractor after proper FDO review, in direct support of a DAF contract. DAF technical orders may also be released in support of FMS activities through the Security Assistance Technical Order Distribution System, only when the following conditions are met:

5.10.1.1. The FMS customer's system configuration is the same as the system documented in the technical order, or so similar to the U.S. system that the unrelated data does not complicate or confuse the operating or maintenance instruction.

5.10.1.2. All reference information in the technical order is releasable.

5.10.2. For safety reasons, FDOs will not sanitize DAF technical orders. **(T-1)**.

5.10.3. If these conditions cannot be met, a country standard technical order will be developed to match the FMS customer's configuration.

Chapter 6

TECHNOLOGY TRANSFER

6.1. Introduction. Controls are necessary to ensure that exports are consistent with U.S. national security interests. Defense articles and services, or commercially available items that have a military utility, are export-controlled by law. The Department of State controls exports of defense articles, services, technical data, etc., under the ITAR. The Department of Commerce controls exports of dual-use commodities with military utility under 15 Code of Federal Regulations Subchapter C, *Export Administration Regulations* (EAR). SAF/IAPD is the DAF OPR for developing positions on commercial exports of defense articles and services, dual-use technology, and technical data.

6.2. International Trafficking in Arms Regulation Licensing Requirements. U.S. government personnel and contractors must comply with the provisions of the ITAR before exporting defense articles, technical data, or defense services controlled by the ITAR. **(T-0).** The ITAR implements presidential authority, under 22 United States Code (USC) Section 2778, *Control of Arms Exports and Imports*, to control the export and import of defense articles and services.

6.2.1. DAF organizations are not authorized to export CMI or CUI without an export license. Exemptions to ITAR licensing requirements is located in [Paragraph 6.3](#).

6.2.2. U.S. industry needs a license or other approval prior to export of defense articles, services, or technical data, unless an ITAR exemption is applicable. The Arms Export Control Act and ITAR guidance require a license for export control and compliance. The Department of State issues licenses or other approvals to registered U.S. industry who apply for authority to export defense articles or furnish defense services. The Department of State may approve the application based on its own evaluation, or it may request recommendations from the Defense Technology Security Administration. If necessary, the Defense Technology Security Administration may request service or agency recommendations regarding proposed exports. SAF/IAPD is the DAF organization responsible for making recommendations on U.S. industry exports to Defense Technology Security Administration.

6.2.2.1. SAF/IAPD evaluates political-military, operational, technical, and security factors for proposed industry exports on a case-by-case basis.

6.2.2.2. SAF/IAPD coordinates industry export requests with subject matter experts, as needed.

6.3. Exemptions to Licensing Requirements. License exemptions are designed to ease the regulatory burden on government and industry without compromising essential trade controls.

6.3.1. DAF organizations are not required to obtain an export license when exporting defense articles, including technical data, or to perform defense services, in the following cases:

6.3.1.1. Exports pursuant to a grant, sale, lease, loan, or cooperative project under the Arms Export Control Act, as amended, or a sale, lease, or loan under the Federal Aviation Administration. Formal approval of FMS programs or international armaments agreements provides the basis for DAF exports of CMI or CUI to foreign governments or international organizations.

6.3.1.2. Exports of CMI or CUI to foreign representatives assigned to DAF organizations under the Military Personnel Exchange Program, Engineer and Scientist Exchange Program, Administrative and Professional Exchange Program, Cooperative Project Personnel agreements, or as a foreign liaison officer, under an FMS case.

6.3.1.3. Combined military operations and training.

6.3.1.4. Unilateral U.S. military operations abroad.

6.3.2. SAF/IAPD may validate ITAR exemptions, in accordance with DoD guidelines, for defense contractors or other relevant entities, on a case-by-case basis for the following cases:

6.3.2.1. The services of private U.S. persons or companies are needed pursuant to activities enumerated in [Paragraph 6.3.1.1](#).

6.3.2.2. The DAF requires the participation of private U.S. persons or companies in initial planning discussions or negotiations with foreign governments and international organizations pursuant to the activities enumerated in [Paragraph 6.3.1.2](#).

6.3.2.3. It is in the interest of the DAF to authorize private U.S. persons or entities to solicit subcontract proposals from foreign entities for the purpose of developing responses to service acquisition authority requests for quote or bid proposals.

6.3.2.4. Exports of classified and unclassified technical data in conjunction with classified and unclassified site visits.

6.3.3. In order to request an ITAR exemption validation for a U.S. person or company, the sponsoring DAF office forwards an official written request through FDO channels to SAF/IAPD. See [Attachment 15](#) for a sample request letter. The sponsoring DAF office must obtain a senior management official, in the grade of colonel (O-6) or higher, or GS-15 or higher, signature supporting the request. **(T-1)**. The sponsoring DAF office must submit the signed request along with a complete ITAR exemption validation checklist, an example of which is located in [Attachment 16](#). **(T-1)**. The sponsoring DAF office will identify the information in the next four paragraphs in the request for ITAR exemption validation. **(T-1)**.

6.3.3.1. The name of the U.S. person or company for which the ITAR exemption validation is requested.

6.3.3.2. The reason for requesting the ITAR exemption validation (e.g., cite letter of offer and acceptance (LOA) number, memorandum title or contract number, if applicable); benefit to the U.S. agency of request (critical program milestones or decision process) in lieu of normal ITAR processes; and status or relationship of the U.S. person or company to the export license or agreement.

6.3.3.3. An explanation of the details regarding defense articles, services, or technical data to be provided by the company in support of the activities listed in [Paragraph 6.3.3.2](#).

6.3.3.4. A copy of all briefings, documents, or information to be disclosed by the individual or company. If it is impractical to attach the actual information, a detailed description of the subject matter (including NDP-1 category and highest classification of the information) may be forwarded. Alternatively, the servicing FDO provides a statement certifying the material proposed for release is authorized for disclosure under an existing DDL (see [Attachment 16](#), ITAR Exemption Validation Checklist).

6.3.4. SAF/IAPD is the approval authority for ITAR exemption validation requests. ITAR exemption validations include the following items:

6.3.4.1. ITAR exemption number.

6.3.4.2. Name of the private U.S. individual or company for which the ITAR exemption validation is granted.

6.3.4.3. The reason or purpose for granting the ITAR exemption validation, benefit to the U.S. government, status of the U.S. individual or company's export license or agreement application.

6.3.4.4. Description of the specific defense article, service, or technical data exempted from the license requirement.

6.3.4.5. Conditions and limitations necessary to establish a clearly-defined scope for defense articles, services, and technical data authorized for export.

6.3.4.6. Expiration date, no more than one year from the date of issue.

6.3.5. Upon receipt of the approved ITAR exemption validation, the servicing FDO will complete the tasks in the following three paragraphs. **(T-1)**.

6.3.5.1. Record the decision to sponsor a foreign visit in the Security Policy Automation Network if a foreign visit is involved, and identify the SAF/IAPD-approved exemption as authority to sponsor the visit.

6.3.5.2. Review all briefings, documents, and other information proposed for release by contractors if the actual documents have not been provided to SAF/IAPD.

6.3.5.3. Ensure a DAF representative (military or civilian employee) familiar with the Foreign Disclosure and Technology Transfer Program is present at all activities to ensure contractor compliance with the terms and conditions of the ITAR exemption validation.

6.4. DAF Requests for Export Licenses. DAF disclosures and technology transfers are approved by designated FDOs pursuant to the conditions outlined in [Paragraph 6.3.4.5](#). Department of State export licenses are usually not required. However, circumstances may exist when DAF organizations may require a license. The following information provides guidance to determine when the DAF obtains an export license from the Department of State:

6.4.1. Foreign nationals require an export license when performing contract services. DAF contracting organizations, known as requiring activities, must obtain State Department approval through SAF/IAPD prior to employing or accepting contracted services from a foreign national in a position requiring CUI. **(T-1)**. The DAF contracting organization must include information from the next four paragraphs in the written request for the SAF/IAPD review of an export license. **(T-1)**.

6.4.1.1. The foreign national's name, citizenship, and identification number.

6.4.1.2. Justification for why the foreign national employment is essential to the national security of the United States.

6.4.1.3. Skills, knowledge, and abilities the foreign national possesses that are not otherwise available from domestic sources.

6.4.1.4. Proposed disclosure guidance to support the foreign national's access to CUI.

6.4.2. This license requirement does not apply to foreign nationals who have been granted permanent legal resident status in the United States.

6.5. Non-Sponsored Foreign Visits to U.S. Defense Industry.

6.5.1. FDOs will generally not sponsor foreign visit requests to U.S. defense facilities. **(T-0)**. If the visits are not sponsored by the U.S., contractors may only disclose CMI or CUI if the information is authorized for release pursuant to the ITAR or the EAR.

6.5.2. FDOs will only sponsor foreign visit requests to U.S. defense facilities after obtaining SAF/IAPD approval through an ITAR exemption certification, in accordance with **Paragraph 6.3. (T-0)**.

Chapter 7

VISITS TO DAF FACILITIES BY REPRESENTATIVES OF FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS.

7.1. Introduction. The Arms Export Control Act requires the U.S. government to obtain security, non-transfer, and end-use assurances from foreign governments and international organizations before transferring defense articles, services, or classified or unclassified technical data. Information disclosed under the auspices of a foreign visit may constitute a defense article, service, or technical data. The International Visits Program exists in support of the Arms Export Control Act to ensure that CMI and CUI information releases to foreign visitors are properly authorized for disclosure to the requesting government or international organization. Visits to DAF facilities should not interfere with the facility's mission requirements. Foreign governments and international organizations are required to provide validated security clearances, need-to-know verification, and government sponsorship regarding their citizens or representatives. FDOs are responsible for approving or denying the disclosure of CMI and CUI to foreign representatives during visits to DAF or contractor facilities, or when DAF personnel visit foreign facilities abroad or in the United States. In specific cases, FDOs approve disclosures to foreign representatives by U.S. contractors supporting DAF Programs (see [Paragraph 6.5.2](#) for guidance on sponsored visits). All visits subject to the requirements of this chapter can be defined as either one-time, recurring, or extended.

7.1.1. One-time visits are for a single, short-term occasion, normally less than 30 days, for a specific purpose.

7.1.2. Recurring visits are multiple, intermittent visits by a foreign national to a DAF organization or contractor facility over a specified period of time, not to exceed one year, in accordance with a government-approved contract or agreement or another program. Recurring visits are approved when the information to be disclosed has been defined and approved for disclosure in advance by the U.S. government.

7.1.3. Extended visits are single, continuous visits occurring for an extended period of time, normally up to one year, but can be extended to cover the entire duration of a Military Personnel Exchange Program (MPEP) or foreign liaison officer (FLO) tour of duty. Reference [Chapter 8](#) for information on extended visits.

7.2. General Visit Policies and Procedures.

7.2.1. DAF personnel may disclose CMI and CUI only to foreign representatives who possess an appropriate security clearance and need-to-know, as verified in their visit request and in accordance with disclosure guidance provided by the servicing FDO.

7.2.2. Visit authorization does not constitute the legal basis for providing defense articles, services including training, or technical data to foreign representatives.

7.2.3. Visit authorizations require signed LOAs, international agreements, or other appropriate legal arrangements to be in place.

7.2.4. Foreign governments submit visit requests for U.S. citizens acting on their behalf when visiting DAF facilities.

7.2.5. The U.S. contact officer for any foreign visit must ensure physical controls limit visitor access to only the information authorized for disclosure. **(T-1)**. SAF/IAPD does not generally require written security plans for one-time or recurring visits. However, SAF/IAPD or other functional program managers may require U.S. contact officers to prepare security plans on a case-by-case basis for one-time or recurring visits, in response to specific circumstances.

7.2.6. DAF organizations must issue badges or passes that clearly identify the bearer as a foreign representative. **(T-1)**.

7.2.6. **(EGLINAFB)** While on Eglin AFB, foreign nationals must wear foreign visitor badges issued by Security Forces Pass & Registration. It is the visit POCs responsibility to ensure foreign nationals wear their badges and are escorted while in Eglin work areas and facilities. Escorts are not required in public areas such as the BX, commissary, shoppettes, etc. Military foreign visitors must wear their uniforms while conducting official government business on Eglin AFB. Organizational FDOs are responsible for:

7.2.6.1. **(Added-EGLINAFB)** Monitoring the Foreign Visit System (FVS) and downloading requests as required.

7.2.6.2. **(Added-EGLINAFB)** Reviewing and coordinating visit requests with visit U.S. contact officer. Once the U.S. contact officer coordinates on the visit, the FDO enters the information into the FVS.

7.2.6.3. **(Added-EGLINAFB)** Sending memos to 96 SFS/S-5 requesting visitors be issued Foreign National visitor badges upon their arrival to the base.

7.2.7. Installation security forces control installation access for visits, and garrison security forces control garrison access for visits. The U.S. contact officer will coordinate and follow local base security procedures regarding access to the installation or garrison by foreign representatives. **(T-1)**. The contact officer must coordinate with cognizant FDOs and security personnel to prevent unauthorized access to CMI or CUI. **(T-1)**. DAF military or civilian personnel assigned to the organization will escort foreign representatives in areas where access to CMI or CUI may occur. **(T-1)**. U.S. contractors, foreign representatives, or U.S. citizens representing foreign nations cannot serve as escorts for these areas. For escort requirements outside of DAF facilities, FDOs will follow guidance from local security forces to determine proper base escort procedures for these areas. **(T-1)**.

7.2.7. **(EGLINAFB)** Organizational POCs will ensure personnel escorting or encountering foreign visitors are properly briefed on security requirements during the visit, to include recovering the foreign visitor badges at the end of the visit and returning them to the East Gate Visitor Control Center. Foreign nationals are not authorized to act as escorts. Additionally, foreign nationals are not authorized to be sponsors for base access in an official business capacity. Escorts for foreign representatives to and within other facilities are subject to local base security procedures.

7.2.8. DAF contact officers shall inform organizers of professional military education activities or lectures that foreign nationals are in attendance and that the information presented will require disclosure review and approval from the servicing FDO prior to presentation if CMI or CUI is involved. **(T-1)**.

7.2.9. DAF contact officers organizing foreign guest lecturers for professional military education activities will brief students regarding disclosure guidelines prior to the arrival of foreign guest lecturers. **(T-1)**.

7.3. Submitting Visit Requests for Foreign Representatives. DAF will submit foreign national visit requests to SAF/IAPD, as required by the circumstances detailed under paragraphs **7.3.1, 7.3.2, and 7.3.3. (T-1)**. Foreign proponents of foreign national visits should follow the same procedures.

7.3.1. For visits to DAF organizations, installations, and garrisons:

7.3.1.1. Foreign visit requests should be submitted at least 30 working days prior to the start date of the visit.

7.3.1.2. The DAF will not process foreign visit requests submitted less than 10 working days, or 14 calendar days, prior to the requested start date of the visit. **(T-1)**. The DAF will immediately return without action visit requests submitted less than 10 working days, or 14 calendar days, prior to the requested start date of the visit. **(T-1)**. This suspense allows the hosting U.S. government facility the necessary time to properly prepare the hosting location for the proposed visit.

7.3.1.3. The only exceptions to the 10-working day suspense requirement are visits to the Air Force Secretariat and service headquarters staff, or visits deemed mission essential or time sensitive by the DAF. In order to utilize this exception, the requesting organization must submit to the approval authority a waiver memo with supporting justification signed by a colonel (O-6) or higher, or GS-15 or higher, . **(T-1)**.

7.3.1.4. The online computer-based Foreign Visit System (FVS) is the primary method to submit foreign visit requests. If an embassy cannot access FVS, they should submit the request to the appropriate SAF/IA country director. Installation of FVS and associated instructional training on the use of FVS is available at no cost to the embassies. Contact the Office of the Secretary of Defense for Policy, International Security Directorate, regarding the installation and administration of FVS at the embassy location.

7.3.1.5. Foreign governments submit requests under the International Visits Program for visits proposed by their representatives and when invited by a DAF organization, at least 30 working days prior to the visit start date, in accordance with DoDD 5230.20, *Visits and Assignments of Foreign Nationals*. FVS automatically assigns visit responsibility to SAF/IAPD. Foreign governments or international organizations with FVS accounts should submit their requests using FVS. Foreign governments or international organizations who do not have access to the Security Policy Automation Network should forward their information to the SAF/IAPD foreign visits team for a designated representative to enter the information into the FVS.

7.3.1.6. Public affairs officers approve foreign national participation in public affairs-cleared activities, subject to their visit approval process. Visit requests under the International Visits Program are not required.

7.3.1.7. DoD proponents submit visit requests to SAF/IAPD for peacetime engagement programs, including the U.S. European Command military contact program; the Latin American Cooperation Fund; CSAF-sponsored visits; and the African Cooperation Fund. DoD proponents must submit with the visit request: proposed dates of visit; facility to be visited; points of contact; purpose of visit; and the visitor's name, rank, position, organization of assignment, date of birth, citizenship, place of birth, security assurances, and identification or passport number. **(T-1)**.

7.3.1.8. DAF proponents for basic research visits by foreign nationals will submit proposals to the servicing FDO. **(T-1)**. The organization to be visited must provide information copies to additional organizations as appropriate. **(T-1)**.

7.3.1.9. U.S. defense contractors employing foreign nationals must directly arrange visits to DAF organizations in accordance with the requirements of the DoD 5220.22-M, *National Industrial Security Program Operating Manual*. **(T-0)**.

7.3.1.10. The North Atlantic Treaty Organization (NATO) security office submits visit requests in accordance with United States Security Authority for NATO Affairs Instruction 1-07, *Implementation of NATO Security Requirements*, for representatives of any NATO command, agency, the NATO International Staff, or the NATO International Military Staff including U.S. citizens assigned to NATO positions or schools. NATO points of contact without access to FVS will forward their visit request information to SAF/IAPD, wherein a designated representative will enter the information into the FVS. **(T-1)**.

7.3.1.11. Foreign students, including international military students, international civilian students, and U.S. citizens representing a foreign nation, who participate in security assistance training on invitational travel orders, are not required to submit a visit request to attend training. In accordance with Defense Security Cooperation Agency Manual 5105.38-M, "Security Assistance Management Manual," the DAF recognizes invitational travel orders issued by security cooperation officers as validation of security assurances for international military students participating in formal DAF training courses. The security cooperation officer must obtain the required security assurances from the parent government before students arrive for training. **(T-0)**. Security cooperation officers issue invitational travel orders in accordance with the requirements of AFI 16-105, *Joint Security Cooperation Education and Training*, and when the training is approved for disclosure to the foreign government. With regard to foreign students:

7.3.1.11.1. For visits to other DAF or DoD organizations that are part of the formal training program, DAF personnel responsible for administering training courses must coordinate through their servicing FDO. **(T-1)**.

7.3.1.11.2. For visits that are not part of the formal training program, students should submit a visit request through their respective embassy in Washington, D.C.

7.3.1.11.3. The International Military Student Office will provide a roster of foreign students on international travel orders to applicable security personnel for access to organizations, installations, and garrisons where training is to occur. **(T-1)**.

7.3.2. For visits including flights on U.S. military aircraft:

7.3.2.1. Foreign visits that include flights on DAF aircraft require flight-specific approval, in accordance with Department of the Air Force Instruction 11-401, *Aviation Management*, in addition to authorization for the visit.

7.3.2.2. For flying missions performed by DAF units under the sponsorship of a unified combatant commander, subordinate unified command, or other service, visit requests are not needed, unless such units disclose CMI or CUI. DAF units must coordinate flying missions with their servicing FDO to obtain disclosure guidance. **(T-1)**.

7.3.3. For visits to cleared U.S. contractor facilities:

7.3.3.1. All visits should be conducted in accordance with DoD 5220.22-M, which details the established procedures for controlling international visits to contractor facilities.

7.3.3.2. Foreign government representatives and members of international organizations should submit visit requests consistent with the International Visits Program.

7.3.3.3. Foreign government representatives and members of international organizations should arrange unclassified visits through their respective embassies using the FVS when the contractor is authorized to disclose information controlled under the ITAR or the EAR.

7.3.3.4. Visit requests are required for extended visits to contractor facilities.

7.3.3.5. Visit requests are required for all visits to contractor facilities that maintain CMI or CUI.

7.3.3.6. Visit requests are required, if mandated as part of a U.S. government contract.

7.3.3.7. For unclassified visits in which foreign nationals are not representing their governments in an official capacity, visits are arranged directly with the applicable contractor.

7.3.4. For the U.S.-Canada Joint Certification Program:

7.3.4.1. Canadian government personnel and contractors certified by the Joint Certification Office, Battle Creek, Michigan, may directly arrange visits to DAF organizations and contractor facilities that meet the conditions and procedures required under the program.

7.3.4.2. Owning organizations may release unclassified technical data after reviewing the request from the Canadian government personnel or contractors.

7.4. Coordinating Visit Requests for Foreign Representatives. FDOs will establish processes so that all offices with interests in the proposed visit have sufficient time to review and provide recommendations on the visit request. **(T-1)**.

7.5. Approving Visit Requests for Foreign Representatives. FDOs will review visit requests for foreign representatives in accordance with delegated disclosure authority prior to approval. **(T-1)**. FDOs will notify the requester and the U.S. point of contact when a visit request is approved. **(T-1)**.

7.5.1. FDOs will document disclosure guidance for each visit and provide the U.S. point of contact before the visit. **(T-1)**. The FDO will provide informational copies of the approval, as needed. **(T-1)**.

7.5.2. FDOs will provide the requester with any information needed to complete arrangements, such as the name of the U.S. point of contact, the U.S. point of contact's phone number, uniform requirements, etc. **(T-1)**.

7.5.3. FDOs will not sponsor foreign visits to U.S. contractor facilities, unless approval under [Paragraph 6.5](#) of this manual has been obtained. **(T-1)**. DAF sponsorship of foreign visits to U.S. contractor facilities may constitute an exemption to the licensing requirements of the ITAR and the EAR.

7.6. Denying Visit Requests for Foreign Representatives. For denied visit requests for foreign representatives:

7.6.1. FDOs will notify the visit requester through FVS when a visit is denied. **(T-0)**.

7.6.2. FDOs will provide the requester with justification for the denial. **(T-0)**. Organizations may deny visits for reasons including: operational, mission, or programmatic impacts; political or military considerations; lack of legal basis for approval; insufficient time to thoroughly process the visit request; or for administrative reasons. Organizations may use administrative reasons when the visit length or type is inappropriate for the visit purpose; the request is submitted more than once; the U.S. point of contact is unavailable; or other similar reasons.

7.7. Visits Hosted by Foreign Tenants on DAF Installations or Garrisons. The DAF hosts various foreign organizations on bases within the U.S. These foreign tenant organizations may host visits by U.S. personnel or foreign representatives. Foreign representative visits to foreign tenant organizations may be conducted without submitting a request through the International Visits Program. However, prior to such visits, foreign tenant organizations must coordinate with the U.S. host organization and obtain approval for base access, in accordance with local procedures. U.S. organizations developing arrangements for long-term foreign tenants must ensure that visit approval procedures are developed in concert with local DAF authorities and are included in the applicable letter of offer and acceptance, international agreement, or implementing arrangement. The DAF host organization maintains final approval authority for base access during such visits.

7.8. DAF Personnel Visiting Foreign Government or International Organization Establishments Overseas. DAF personnel will obtain approval to visit foreign establishments overseas through the Aircraft and Personnel Automated Clearance System. **(T-0)**. Before beginning foreign travel, DAF personnel will obtain disclosure approval from their servicing FDO for any discussions involving CMI or CUI that will occur during the visit. **(T-0)**. Travelers will record the designated FDO that approved disclosure of the information to be discussed in the personnel clearance request, using the office symbol. **(T-0)**.

Chapter 8

EXTENDED VISITS INVOLVING FOREIGN REPRESENTATIVES

8.1. Introduction. Foreign representatives may only be assigned to or placed in DAF organizations in accordance with the terms of a written agreement or letter of offer and acceptance (LOA) that is concluded in compliance with applicable laws and regulations. In the terms of the agreement, DAF organizations must identify administrative support, liability, obligations, and responsibilities of all involved parties. **(T-0).**

8.1.1. The LOA or agreement establishes the extended visit position. The exact language may differ as a result of agreement or LOA negotiation, but all requirements should be addressed.

8.1.2. Extended visit requests are required for personnel participating in one of the categories covered in [Paragraph 8.2](#). FDOs will not make any commitments to assign extended foreign visitors to DAF organizations unless the requirements of this chapter are met. **(T-1).**

8.1.3. For extended visits that are not defined in [Paragraph 8.2](#), proponents will forward proposals to SAF/IAPD for a policy evaluation. **(T-0).** In the proposals, proponents will include justification of the extended visit, a description of duties to be assigned, and proposed disclosure guidelines, and will be forwarded through command channels. **(T-0).**

8.1.4. Extended visit requests should be submitted by the foreign partner's embassy for the duration of the visitor's orders. If the host organization and the partner nation government agree on an extension of the visitor's orders, the partner government's embassy should submit an amended foreign visit request to cover the period of the extension in accordance with the terms of the international agreement. See [Attachment 9](#) for instructions on creating position descriptions for extended visit positions.

8.2. Categories of Extended Visits. Extended visits generally occur in the following categories:

8.2.1. Defense Personnel Exchange Programs, including the Military Personnel Exchange Program (MPEP) which includes exchange officers, the Engineer and Scientist Exchange Program (ESEP), and the Administrative and Professional Exchange Program (APEP).

8.2.2. Cooperative Project Personnel (CPP) Program.

8.2.3. Country Liaison Officer (CLO) Program.

8.2.4. The Inter-American Air Forces Academy guest instructor program and Euro-NATO Joint Jet Pilot Training program.

8.2.5. The Foreign Liaison Officer (FLO) Program.

8.3. Authorities and Guidance for Extended Visits. MPEP, ASEP, and ESEP exchanges require an international agreement that provides for the exchange of personnel between governments. CPP exchanges require a cooperative research development test and evaluation or production agreement that establishes a cooperative program and includes provisions for placing CPP. See [Attachment 8](#) for sample language that addresses administrative responsibilities for extended visit positions.

8.3.1. FLOs are established by an FMS case or a LOA that provides for the placement of personnel and defines the specific support or services to be provided. FLOs may also be established under international agreements. When support services are provided, a LOA is required for reimbursement to the DoD. FLOs are assigned through the Air Force Security Assistance and Cooperation Directorate and have a limited role in FMS cases.

8.3.2. CLOs are established by an FMS case that provides for the placement of personnel to provide administrative support for international military students from the CLO's country. CLOs are assigned through the Air Force Security Assistance Training Squadron.

8.3.3. The International Airmen Division, Directorate of Policy Programs & Strategy, Deputy Under Secretary for International Affairs provides policy guidance for MPEP positions. See AFI 16-107, *Military Personnel Exchange Program*, for guidance on MPEP.

8.3.4. The International Armaments Cooperation Division, Directorate of Policy Programs & Strategy, Deputy Under Secretary for International Affairs provides policy guidance for establishing and managing APEP and ESEP positions. See AFI 16-110, *US Air Force Participation in International Armaments Cooperation (IAC) Programs*, for guidance on APEP and ESEP. The International Armaments Cooperation Division, Directorate of Policy Programs & Strategy, Deputy Under Secretary for International Affairs also provides policy guidance for establishing and maintaining CPP positions. See Air Force Manual (AFMAN) 16-114, *Participation in International Armaments Cooperation (IAC) Programs*, for guidance on CPP. International focal points may be designated at MAJCOM, field command, or subordinate levels to provide advice and assistance for implementing International Armaments Cooperation policies.

8.3.5. Prior to receiving contracted services, foreign nationals are expected to coordinate with the servicing FDO.

8.4. Establishing Extended Visit Positions.

8.4.1. DAF proponents seeking positions that require extended visits will coordinate with the appropriate command OPR to verify that an agreement exists to authorize the assignment. **(T-1)**. Extended visit positions cannot be established without an appropriate LOA or agreement in place. Proponents should advise the servicing FDO of forthcoming initiatives that will result in the creation of extended visit positions. Proponents should also include the servicing FDO in planning for assignments. The end date of the extended visit authorization will not exceed the end date of the FMS case, international agreement, or program agreement. For activities that occur outside of DAF or service level headquarters, servicing FDOs advise SAF/IAPD of approved extended visit position. Servicing FDOs must identify the type of position, the basis for approval of the position, and the location of the extended visit position. **(T-1)**.

8.4.1. **(EGLINAFB)** Organizational POCs will submit requests to establish a Foreign Exchange Officer or Foreign Liaison Officer position to 96 TW/IPF (FDO) for review and coordination.

8.4.2. Identifying the visitor's assigned responsibilities and duties is critical to plan an extended visit. Position descriptions are required for any program involving an extended visit. Position descriptions ensure that assigned duties are consistent with the authorizing agreement for extended visitors and also ensure that responsibilities assigned to the extended visitor are clearly understood. Reference [Attachment 9](#) for a sample position description.

8.4.2.1. Include position descriptions in the staff packages that request extended visit positions under ESEP, CPP, and MPEP programs.

8.4.2.2. DAF officials will ensure ESEP, CPP, and MPEP participants will not perform liaison functions between the DAF and their nation's military service. (T-1). DAF officials will ensure FLOs do not act in an official capacity for the DAF. (T-1).

8.5. Dual Assignment as a Cooperative Project Personnel and a Foreign Liaison Officer. In some cases, and in accordance with the terms of the authorizing agreement, an extended visitor may perform part-time duties as a FLO and part-time duties as a CPP. SAF/IA approves the arrangements of dual-assigned visitors. Forward requests for approvals of dual-assigned visitors to SAF/IAPD through FDO channels.

8.5.1. Proposed arrangements ensure that dual assignments will not be detrimental to the cooperative program involved and ensure that responsibility and funding for the FLO functions are maintained separately. This is required because FLO and CPP positions rely on different legal authorities.

8.5.2. Dual assignments are not permitted for ESEP, MPEP, or APEP positions.

8.6. Coordinating Extended Visit Requests. FDOs are notified of proposed assignments to extended visit positions via the Security Policy Automation Network or by the DAF supervisor of a foreign exchange officer. FDOs establish processes for all offices with interest in the proposed assignment review and make recommendations regarding the request.

8.6.1. The FDO, DAF contact officer, and others, as needed, will develop a security plan that documents access controls to information and facilities within the organization and installation or garrison. (T-1). See [Attachment 10](#) for a sample security plan.

8.6.2. The FDO and DAF contact officer will determine other locations that the assigned visitor may visit during their assignment to carry out responsibilities and duties under the approved position description. (T-1). The FDO and contact officer will periodically review the initial determination. (T-1).

8.6.2.1. Recurring visits for APEP, ESEP, MPEP, and CPP may be directly arranged between DAF organizations. SAF/IAPD supports visits directly arranged with other services and other DoD agencies for MPEP and CPP. DAF contact officers must comply with the policies and regulations of the service or agency to be visited. (T-1). DAF contact officers will coordinate visits with their servicing FDOs. (T-1). DAF contact officers must ensure disclosure guidance is in place before commencing the visit. (T-0). FDOs will use SPAN procedures to coordinate these visits. (T-0).

8.6.2.2. DAF host units will authorize temporary duty assignment orders for foreign exchange officers traveling to alternate locations on behalf of the DAF. (T-1). The DDL reflects the clearance level and authorization to work in the capacity assigned.

8.6.2.3. Requesting governments should use SPAN to request recurring visits to various locations for FLOs and CLOs.

8.7. Approving Extended Visit Requests. FDOs shall not approve extended visit requests until verifying that an appropriate agreement or LOA exists that authorizes the extended position. (T-0).

8.7.1. FDOs will approve the release of CMI and CUI in accordance with delegated disclosure authority to support the assignment. **(T-1)**.

8.7.2. FDOs will document disclosure guidance for each visit. **(T-1)**. This guidance is provided to the DAF contact officer for each visit and is also provided to information addressees, as needed.

8.7.3. FDOs will brief DAF contact officers on their responsibilities related to visitors assigned on an extended basis. **(T-1)**.

8.7.4. FDOs will maintain a file for each extended visit made to organizations they support. **(T-1)**. Files include, at minimum, a copy of the extended visit request (if the FDO does not have SPAN access); verification of the legal basis for the visit; the security plan; and coordination and approval records for MPEP and CPP visits to other locations. FDOs will notify the requester when a visit is approved. **(T-1)**. FDOs will also provide the requester with the name and telephone number of the visit point of contact and the terms of the visit approval. **(T-1)**.

8.8. Security Requirements for Extended Visits.

8.8.1. Access to CMI and CUI depends on the security clearance granted by the visitor's government, need-to-know, and disclosure guidance issued by the servicing FDO.

8.8.2. DAF will not permit exchange personnel to have personal custody of CMI or CUI. **(T-1)**. Refer to the applicable exchange officer DDL for additional guidance.

8.8.3. Foreign Liaison Officers may have custody of CMI, as stipulated in the authorizing agreement that establishes their position, and subject to the following conditions:

8.8.3.1. FLOs may assume custody of documentary information when authorized, in writing, by their government, provided that U.S. security personnel exercise oversight over the storage container. This oversight is similar to that executed by U.S. security personnel over U.S. storage containers.

8.8.3.2. FLOs may act as couriers only when they are authorized, in writing, by their government to assume responsibility as an agent of their government. The FLO's government provides all necessary courier credentials.

8.9. Extended Visitor Access to DAF Facilities, Installations, and Garrisons.

8.9.1. DAF personnel will not approve unescorted access for foreign representatives to DAF restricted or controlled areas, or other facilities where access to CMI or CUI may occur, unless all of the conditions in the next four paragraphs have been met **(T-1)**.

8.9.1.1. The foreign representative's government extends commensurate reciprocal privileges to DoD personnel.

8.9.1.2. The foreign representative is sponsored by their government or international organization through a formal visit request and the need for frequent access is justified.

8.9.1.3. Security measures exist to limit access to only CMI and CUI authorized for disclosure.

8.9.1.4. A badge or pass issued to the foreign representative clearly identifies them as such. Such identification is valid only for a specific facility during normal duty hours. DAF contact officers will make specific arrangements for access during non-duty hours on a case-by-case basis with the FDO and all offices having a functional interest in the extended duty hours. **(T-1)**. The badge or pass will be displayed on the outer clothing and clearly visible.

8.9.2. Base access is a security issue and is not the responsibility of FDOs. For base access, each base should follow DoDM 5200.08V3_AFMAN 31-101V3, *Installation Perimeter Access Control (FOUO)*, and local security forces protocols to determine proper base access procedures.

Chapter 9

DAF PROCUREMENT ACTIVITIES INVOLVING FOREIGN INDUSTRY

9.1. Introduction. U.S. acquisition reform established a hierarchy of potential alternatives to be evaluated before commitment to a new acquisition program. The first alternative is to access the use or modification of an existing commercial system or a previously developed U.S. military or allied nation system that would alleviate the necessity for a weapons development program. Since U.S. defense procurements may include foreign sources, foreign disclosure and technology transfer requirements are addressed prior to contract award.

9.2. Reviewing Planned Procurements.

9.2.1. DAF contracting authorities announce planned procurements on System for Awards Management (SAM) website at www.beta.sam.gov. Air Force Federal Acquisition Regulation Supplement, Subpart 5327.90, *Foreign Disclosure* provides foreign disclosure procedure and guidance starting points. Contracting authorities coordinate invitations to bid, requests for proposals, pre-solicitation, pre-bidders, pre-proposal, and pre-award meetings, etc., with their servicing FDO prior to announcing procurement activities so that restrictions can be identified to foreign bidders.

9.2.1.1. If given the opportunity to do so, FDOs review procurements prior to the SAM announcement and identify necessary restrictions on foreign participation.

9.2.1.2. When it is not possible to review all procurements prior to the SAM announcement, DAF contracting officers must ensure that announcements include notification that restrictions regarding foreign bidders may be placed on the contract. **(T-1)**. Foreign bidders should indicate to the contracting officer their interest in the procurement prior to submitting a proposal. Once foreign interest is identified, FDOs must review the procurement announcement in a timely manner so that foreign bidders can submit proposals to meet contracting office submission deadlines. **(T-0)**.

9.2.1.3. Prime contractors are responsible for obtaining authorization to disclose CMI and CUI to foreign sub-contractors, pursuant to the International Trafficking in Arms Regulation and Export Administration Regulations.

9.2.2. The Defense Counterintelligence and Security Agency is assigned functional responsibility for foreign ownership, control or influence, in accordance with DoDD 5105.42, *Defense Security Service*, and the National Industrial Security Program Operating Manual. FDOs must maintain communication with DAF government contracting activities who support contracts when a company under foreign ownership, control or influence mitigation is awarded a contract with a foreign disclosure nexus. **(T-1)**. DAF government contracting activities must maintain communication with Defense Counterintelligence and Security Agency on all foreign ownership, control or influence matters in accordance with DoDM 5220.22V2 and DoDM 5220.22 V2_AFMAN 16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. **(T-1)**.

9.3. Appeals Regarding Decisions to Exclude Foreign Contractors. FDOs will forward requests by foreign contractors to appeal denials through FDO channels to SAF/IAPD. **(T-1)**.

Chapter 10

SECURITY REQUIREMENTS

10.1. Introduction. This chapter provides guidance for reporting compromises of or unauthorized access to both U.S. and foreign CMI and CUI. Personnel must understand these requirements to ensure that DAF responsibilities are properly executed in accordance with DoDM 5200.01V3, *DoD Information Security Program: Protection of Classified Information*, DoDI 5200.48, and the respective general security of military information agreements, as applicable. **(T-0).** A general security of military information agreement is a binding international agreement establishing agreed upon security requirements to protect sensitive information and forms a basis for military information exchange between two countries.

10.2. Reporting and Processing Unauthorized Access to Classified Military Information. Notifications of known or suspected compromises of U.S. or foreign government classified information should be made in accordance with AFI 16-1404 for DoD civilians, military members, and onsite contractors. Notifications of known or suspected compromises should be made in accordance with the National Industrial Security Program Operating Manual for offsite DoD contractors. The Security, Special Program Oversight and Information Protection Office will notify SAF/IAPD of any reports of compromises or probable compromises of NATO classified information, foreign government classified information, or U.S. classified information to or by foreign representatives.

10.3. Reporting and Processing Unauthorized Access to Controlled Unclassified Information. DAF personnel must report known or suspected unauthorized access to U.S. CUI be made in accordance with AFI 16-1404 for DoD civilians, military members, and onsite contractors. Notifications of known or suspected access to export-controlled articles, services, or technical data should be made in accordance with the National Industrial Security Program Operating Manual for cleared offsite DoD contractors.

KELLI L. SEYBOLT,
Deputy Under Secretary of the Air Force
International Affairs

(EGLINAFB)

JEFFREY T. GERAGHTY
Brigadier General, USAF
Commander, 96th Test Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 13526, *Classified National Security Information*, 29 December 2009

Federal Acquisition Regulation, Subpart 7.5, *Inherently Governmental Functions*, current edition

8USC Section 1101, *Aliens and Nationality*

18USC, Section 1905, *Disclosure of Confidential Information Generally*

15Code of Federal Regulations Subchapter C, *Export Administration Regulations*, current edition

22Code of Federal Regulations Section 120.10, *Technical Data*, current edition

22USC, Chapter 39, *Arms Export Control*

22USC, Chapter 32, *Foreign Assistance*

22USC Section 2778, *Control of Arms Exports and Imports*

42USC Chapter 23, *Development and Control of Atomic Energy*

50USC, Chapter 58, *Export Control Reform*

JP1, *Doctrine for the Armed Forces of the United States*, 25 March 2013

JP1-0, *Joint Personnel Support*, 1 December 2020

JP2-01, *Joint and National Intelligence Support to Military Operations*, 5 July 2017

DoDD 5105.42, *Defense Security Service*, 3 August 2010

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 June 1992

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, 22 June 2005

DoDI S-5105.63, *Implementation of DoD Cover and Cover Support Activities (U)*, 20 June 2013

DoDI 2040.02, *International Transfers of Technology, Articles, and Services*, 27 March 2014

DoDI, 5200.48, *Controlled Unclassified Information (CUI)*, 6 March 2020

DoDI 5230.24, *Distribution Statements on Technical Documents*, August 23, 2012

DoDM 5200.01V2, *DoD Information Security Program: Marking of Information*, 24 February 2012

DoDM 5200.01V3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, 28 February 2006

DoDM 5200.08V3_AFMAN 31-101V3, *Installation Perimeter Access Control (FOUO)*, 27 February 2020

DoDM 5220.22 V2_AFMAN 16-1406 V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 08 May 2020

National Disclosure Policy (NDP-1), *National Policy and Procedures for the Disclosure of*

Classified Military Information to Foreign Governments and International Organizations, 14 February 2017

HAFMD 1-16, *Deputy Under Secretary of the Air Force, International Affairs*, 14 January 2015

HAFMD 1-4, *Chief of Staff of the Air force*, 7 March 2012

DAFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*, 17 October 2019

AFI 16-105, *Joint Security Cooperation Education and Training*, 3 January 2011

AFI 16-107, *Military Personnel Exchange Program*, 29 August 2018

AFI 16-110, *US Air Force Participation in International Armaments Cooperation, (IAC) Programs*, 18 September 2018

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 6 February 2020

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

AFI 35-101, *Public Affairs Operations*, 20 November 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 38-101, *Manpower and Organization*, 29 August 2019

AFI 90-201, *The Air Force Inspection System*, 20 November 2018

Department of the Air Force Instruction 33-360, *Publications and Forms Management*, 1 December 2015

AFMAN 16-114, *Participation in International Armaments Cooperation (IAC) Programs*, 23 October 2018

Department of the Air Force Manual 11-401, *Aviation Management*, 27 October 2020

Air Force Federal Acquisition Regulation Supplement, Subpart 5327.90, *Foreign Disclosure*, current edition

Intelligence Community Policy Guidance 710.1, *Application of Dissemination Control: Originator Control*, 25 July 2012

United States Security Authority for North Atlantic Treaty Organization Affairs Instruction 1-07, *Implementation of NATO Requirements*, 5 April 2007

Defense Security Cooperation University, "Security Cooperation Management" Green Book, available at dscu.mil

Defense Security Cooperation Agency Manual 5105.38-M, "Security Assistance Management Manual," available at samm.dsca.mil

Adopted Forms

(Added-EGLINAFB) AFMC Form 193, *Foreign Travel Disclosure Review and Foreign Clearance Guide Worksheet*

DD Form 441, DoD Security Agreement

Air Force Form 349, *Receipt for Documents Released to Accredited Representatives of Foreign Nations*

Air Force Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

APEP—Administrative and Professional Exchange Program

CLO—Country Liaison Officer (AF and DoS term)

CMI—Classified Military Information

CPP—Cooperative Project Personnel

CSAF—Chief of Staff of the Air Force

CUI—Controlled Unclassified Information

DAF—Department of the Air Force

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

DCS—Direct Commercial Sales

DDL—Delegation of Disclosure Authority Letter

DDTC—Directorate of Defense Trade Controls

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DRU—Direct Reporting Unit

EAR—Export Administration Regulations

ESEP—Engineer and Scientist Exchange Program

FDO—Foreign Disclosure Officer

FDR—Foreign Disclosure Representative

FLO—Foreign Liaison Officer

FMS—Foreign Military Sales

FOA—Field Operating Agency/Agencies

FOUO—For Official Use Only

FVS—Foreign Visit System

HAFMD—Headquarters Air Force Mission Directive

IAC—International Armaments Cooperation

ITAR—International Traffic in Arms Regulation

LOA—Letter of Acceptance

MAJCOM—Major Command

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MPEP—Military Personnel Exchange Program

NATO—North Atlantic Treaty Organization

NDP-1—National Disclosure Policy

NDPC—National Disclosure Policy Committee

NOFORN—Not Releasable to Foreign Nationals

OPR—Office of Primary Responsibility

SAF—Secretary of the Air Force (organization)

SAF/IA—International Affairs

SAF/IAPD—Foreign Disclosure and Technology Transfer Division

SAF/IAPW—Weapons Division

SAM—System for Awards Management

SCO—Security Cooperation Office/Officer

SPAN—Security Policy Automation Network

U.S.—United States

USSAN—United States Security Authority for North Atlantic Treaty Organization Affairs

Terms

Area of Responsibility—The geographical area associated with a combatant command within which a geographic combatant commander has authority to plan and conduct operations. (JP 1, *Doctrine for the Armed Forces of the United States*)

Baselines—Weapons baselines are foundational CSAF-approved DAF positions on the export of weapons, weapons systems, related technologies, and information.

Classified Information—Official information that has been determined to require, in the interests of national security, protections against unauthorized disclosure and which has been so designated.

Classified Military Information (CMI)—Information originated by or for DoD or its agencies or that is under their jurisdiction or control and requires protection in the interests of national security. Such information is designated “TOP SECRET,” “SECRET,” and “CONFIDENTIAL,” as described in Executive Order 13526, *Classified National Security Information* (DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International*

Organizations). Eight categories of CMI (see [Attachment 2](#)) are subject to national disclosure policy control.

Certification—Formal recognition by a DoD component of a working relationship with a representative of a foreign government (e.g., a foreign liaison officer) for specified purposes and on a recurring basis over an agreed period of time. DAF certification of foreign nationals is established by approval of an extended visit request.

Combatant Command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff.

Combined Military Information—Military information that, by agreement, is shared by the United States and another government or international organization, regardless of which party to the agreement produces the information. (Combined military information may result or originate from specific projects which the United States and another government agree to conduct so that the different phases of the project are undertaken separately; one government will assume sole project responsibility on behalf of both; or the best results of independent endeavors will be adopted.)

Contact Officer—A DoD 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 DoD component or subordinate organization. In the case of MPEPs, the host supervisor may be the contact officer.

Contractor—Any industrial, educational, commercial, or other entity which has executed a contract or a DD Form 441, *DoD Security Agreement*, with a DoD activity.

Controlled Unclassified Information (CUI)—*Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify. (DoDI 5200.48)*

Cooperative Program—A program for research, development, test, evaluation, and/or production that is not implemented under the Security Assistance Program.

Cooperative Program Personnel (CPP)—Foreign government personnel, assigned to a multinational program office that is hosted by a DoD component pursuant to the terms of a cooperative program international agreement, who report to and take direction from a DoD-appointed program manager (or program manager equivalent) for the purpose of carrying out a multinational project or program.

Country Liaison Officer (CLO)—The CLO is established through an FMS case that provides for the placement of CLO personnel to assist with administrative details for international military students from the CLO's country. He/she is an officer or non-commissioned officer of a foreign military establishment selected by his or her government and attached to a MILDEP or DoD agency for the primary purpose of helping administer International Military Student from his or her home country. For administrative purposes, the CLO is considered in a student status. In State Department terms, the CLO is the Community Liaison Officer, similar to a Morale, Welfare and Recreation officer in the military.

Defense Article—Defense article means any item or technical data including that recorded or stored in any physical form, models, mock-ups or other items that reveal technical data (See explanation of term) directly related to items designated in the United States Munitions List.

Defense Service—1) The furnishing of assistance (including training) to foreign persons, whether in the U.S. or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; or 2) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice (in accordance with ITAR).

Defense Personnel Exchange Program—A program under which DoD military and civilian personnel and military and civilian personnel of the defense ministries and/or military services of foreign governments, pursuant to the terms of an international agreement, occupy positions with and perform functions for a host organization to promote greater understanding, standardization, and interoperability. The Defense Personnel Exchange Program consists of APEP, DIPEP, ESEP and MPEP programs.

Defense Technology Security Administration—The Defense Technology Security Administration, under the authority, direction, and control of the Deputy Undersecretary of Defense (Technology Security Policy and Counterproliferation), serves as the focal point within DoD for administering the DoD Technology Security Program. The Defense Technology Security Administration's mission is to develop and implement policies on international transfers of defense-related articles, services, and technologies to ensure that such transfers are consistent with U.S. national security interests.

Delegation of Disclosure Authority Letter (DDL)—A letter issued by the Office of the Deputy Under Secretary of the Air Force, International Affairs, Foreign Disclosure and Technology Transfer Division explaining classification levels, categories, scope, and limitations of information under DAF jurisdiction or control that designated disclosure authorities may approve for disclosure to specific foreign governments. DDLs are issued when there are requirements to disclose information in support of continuing programs. DDLs are comprised of a formal delegation letter that includes a basic delegation and country or system specific delegations.

Designated Disclosure Authority—An official, at subordinate component level, designated by the Head of a DoD component or the component's principal disclosure authority to control disclosures of CMI by his or her organization.

Disclosure—the permanent or temporary transfer of classified or controlled unclassified information to an authorized representative of a foreign government or international organization and/or the act of permitting access to classified or controlled unclassified information to an authorized representative of a foreign government or international organization. There are three disclosure methods: oral (verbal disclosure), visual (disclosure by sight) and documentary (disclosure of tangible/recorded information or equipment).

Foreign Disclosure Officer (FDO)—A U.S. government official designated in writing whose primary responsibilities are to authorize disclosure of CMI or CUI and manage and implement a disclosure program for their command or organization. Only FDOs trained by SAF/IAPD or Headquarters MAJCOM Command FDOs Training Course (certified by SAF/IAPD) may authorize disclosures of CMI and CUI.

Foreign Interest—Any foreign government, agency of a foreign government, or representative of a foreign government or international organization; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its possessions and trust territories; and any person who is not a citizen or national of the United States.

Foreign Liaison Officer (FLO)—Military or civilian officials of a foreign defense establishment who are authorized by their government or an international organization, and certified by a DoD component, to act as an official representative of that government or organization in dealing with the DoD components. (DoDD 5230.20) There are two types of FLOs:

a. Security Assistance—A foreign government representative who is assigned to a DoD component or contractor facility pursuant to a requirement that is described in a foreign military sales letter of offer and acceptance.

b. Operational—A foreign government representative who is assigned to a DoD component pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education.

Foreign National—A person who is not a citizen or national of the United States unless that person has been lawfully admitted for permanent residence in the United States under the *Immigration and Naturalization Act*. (8 USC, Section 1101(a) (20)). Any person other than a United States citizen, United States permanent or temporary legal resident alien, or person in United States custody. (JP 1-0, *Joint Personnel Support*)

Foreign Ownership, Control, or Influence—A U.S. company is considered under foreign ownership, control or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Foreign Representative—Any representative of a foreign interest or foreign national.

Foreign Visit System (FVS)—A SPAN sub-system supporting staffing and databases for processing requests for visits by foreign nationals to DoD activities and defense contractors.

Government-to-Government Channels—The principle that classified and controlled unclassified information and materiel will be transferred by government officials through official channels, e.g., military postal channels, Defense Courier Service, etc.). The information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.

General Security of Military Information Agreement—“The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the U.S. The intent of a foreign government to protect U.S. CMI is established in part by the negotiation of a general security of military information agreement or other similar international agreement.” (Defense Security Cooperation University “Security Cooperation Management” Green Book). “If CMI is to be released in support of an FMS sale, and there is no general security of information agreement or general security of military information agreement, a program specific security agreement developed and approved by the Defense Technology Security Administration containing the security requirements must be concluded prior to discussion of CMI with the purchasing government.” (Defense Security Cooperation Agency Manual 5105.38-M)

International Organization—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. (DoDD 5230.11)

International Visits Program—A program established to process visits by and assignments of authorized representatives to DoD components and DoD contractor facilities. This program is designed to ensure that CMI and CUI disclosed to authorized foreign representatives has been properly authorized for disclosure to their governments, to ensure the requesting foreign government provides security assurance when classified information is involved in the visit or assignment, and to facilitate administrative arrangements (e.g., date, time, and place) for the visit or assignment.

Joint Atomic Information Exchange Group—The Joint Atomic Information Exchange Group is organized under the Defense Nuclear Agency and reviews and makes determinations regarding disclosure of U.S. atomic information.

Joint Information—Military information over which two or more DoD components, or two or more federal departments or agencies, exercise control, jurisdiction, or security awareness. (DoDD 5230.11)

License—A document bearing the word "license" which is issued by the director, Directorate of Defense Trade Controls, United States State Department, or his authorized designee. This document permits the export or in-transit shipment of a specific defense article, defense service, or technical data.

Memorandum of Agreement (MOA)—An agreement concluded with one or more foreign governments including their agencies, instrumentalities, or political subdivisions, or with an international organization that is signed or agreed to by authorized personnel of a DoD component, or by representatives of the DOS or any other department or agency of the U.S. government and signifies the intention of the signatories to be bound in international law. (AFI 16-110)

Memorandum of Understanding (MOU)—MOUs are interpreted similarly to an MOA, for the purposes of Armaments Cooperation. (AFI 16-110)

Military Personnel Exchange Program (MPEP)—This program involves the assignment of military personnel to authorized positions within the Military Departments.

National Disclosure Policy Committee—The central authority formulating, promulgating administering, and monitoring the National Disclosure Policy.

National Disclosure Policy—This policy promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definitions of terms, release arrangements, and other guidance required by U.S. departments and agencies having occasion to release classified U.S. military information to foreign governments and international organizations. In addition, it establishes and provides for the management of an interagency mechanism and procedures which are required for the effective implementation of the policy.

National Intelligence—All intelligence, regardless of the source from which derived, and including that which is gathered within or outside the United States, that pertains to more than one agency, and involves (1) threats to the United States, its people, property, or interests, (2) the development, proliferation, or use of weapons of mass destruction, or (3) any other matter bearing on U.S. national or homeland security. (JP 2-01, *Joint and National Intelligence Support to Military Operations*)

Not Releasable to Foreign Nationals (NOFORN)—“The dissemination marking “NOFORN” is an intelligence control marking used to identify intelligence which an originator has determined meets the criteria of [DoDM) 5200.01V2] and which may not be provided in any form to foreign governments (including coalition partners), international organizations, foreign nationals, or immigrant aliens without the originator’s approval.” (DoDM 5200.01, Volume 2, Enclosure 4)

Originator—The command by whose authority a message is sent, which includes the responsibility for the functions of the drafter and the releasing officer.

Parent Government/Service—The government/service of a foreign representative assigned to the United States DAF.

Release—Commonly used synonym for the term "disclosure." (See explanation of term.)

Restricted Data/Formerly Restricted Data—Restricted Data/Formerly Restricted Data is U.S. atomic information that is controlled under 42 USC, Chapter 23, *Development and Control of Atomic Energy*. The Joint Atomic Information Exchange Group organized under the Defense Nuclear Agency, reviews and makes determinations as to the disclosure of U.S. atomic information when it meets the applicable criteria under existing statutes and for the purpose of furthering approved cooperative agreements.

Security Cooperation Office/Officer (SCO)—Those DoD organizations permanently located in a foreign country and assigned responsibilities for carrying out of security cooperation management functions under 22 USC Chapter 32, *Foreign Assistance*, regardless of the actual name given to such DoD component. SCOs include military assistance advisory groups, military missions and groups, offices of defense and military cooperation, liaison groups, and defense attaché; personnel designated to perform security cooperation functions. The term "SCO" does not include units, formations, or other ad hoc organizations that conduct security cooperation activities

such a mobile training teams, mobile education teams, or operational units conducting security cooperation activities. The generic term SCO replaces the former term Security Assistance Office. Security cooperation officers are individuals designated, in writing, by the SCO Chief to oversee and maintain the custody of each Security Cooperation Information Portal token within the SCO.

Security Policy Automation Network (SPAN)—A wide area computer network operated by the Office of the Under Secretary of Defense (Policy) consisting of a DoD- wide SECRET-high classified network that supports communications and coordination among DoD activities on foreign disclosure, export control and foreign visits. The system also supports an unclassified segment between DoD and foreign embassies.

Special Access Program—A program activity which has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the Special Access Program is identified by a security classification guide.

Technical Data (defined at 22 Code of Federal Regulations Section 120.10, *Technical Data*)—Information whose export is controlled by the Department of State in accordance with the U.S. Munitions List. This information is (1) required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles; (includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation); (2) can be classified or unclassified and related to defense articles and defense services; (3) is covered by an invention secrecy order; or (4) is software directly related to defense articles. All printed and electronic technical data should be marked with an appropriate Distribution Statement and an export control warning statement as detailed in DoDI 5230.24, *Distribution Statements on Technical Documents*, Enclosure 4.

Topline—The process for obtaining CSAF, CSO, or SAF/IA approval of an adjustment to a DAF baseline. Toplines may be in the form of a permanent or temporary modification.

Visit Authorization—A request approved by an FDO that permits a visit by an authorized representative. FDOs authorize visits after an evaluation of a request from a foreign government or international organization that identifies the visitor as its official representative, verifies personal information, verifies the visitor's security clearance, and provides security assurances that CMI and CUI provided to the visitor will be protected. There are three types of authorizations:

a. One-Time—Permits contact by foreign nationals with a United States DAF organization or contractor facility for a single, short-term occasion (normally less than 30 days) for a specified purpose.

b. Recurring—Permits intermittent visits (not to exceed a year) by a foreign national to a United States DAF organization or contractor facility over a specified period of time in accordance with a government-approved license, contract or agreement, or other program. Recurring visits are approved when the information to be disclosed has been defined and approved for disclosure in advance by the U.S. government.

c. Extended—Permits a single visit by a foreign national for an extended period of time, normally up to one year but can be extended to cover the entire duration of a MPEP, FLO, Inter-American Air Forces Academy guest instructor, or Euro-NATO Joint Jet Pilot Training assignment. Extended visit authorizations are used when a foreign national is required to be in continuous contact with a United States DAF organization or a contractor facility. Extended visits are used to assign foreign personnel as FLOs, CPPs, and ESEPs.

Attachment 2

NATIONAL DISCLOSURE POLICY (NDP-1) FUNCTIONAL CATEGORIES OF INFORMATION

A2.1. Category 1, Organization, Training, and Employment of Military Forces. Military information of a general nature necessary to the organization of military, paramilitary, or irregular forces to include those tactics, techniques, and tactical doctrine (including military intelligence and counterintelligence doctrine and techniques) necessary to train and employ those forces. This category does not include specific technical data and training needed to operate and maintain individual items of military materiel and munitions.

A2.2. Category 2, Military Materiel and Munitions. All military materiel, arms and munitions procured and controlled by the U.S. government for the equipping, operation, maintenance and support of its military forces or the military, paramilitary, or irregular forces of its allies. Items developed by U.S. private interests as a result of U.S. government contracts or derived from technology paid for by the U.S. government are included within this category. It also includes U.S. Munitions List items which may be proposed for sale abroad by the U.S. Private interests under the International Traffic in Arms Regulations or items specifically covered by other U.S. government-prescribed export control regulations falling within this definition. (Items under development fall under Category 3.) This category also comprises information to include technical data and training necessary to operate, maintain, or support specific military materiel, arms, or munitions. It does not include information necessary to produce, coproduce, or in any other way manufacture the item.

A2.3. Category 3, Applied Research and Development Information and Materiel. Classified military information resulting from the extension of fundamental theories, designs, and data from a purely theoretical or experimental investigation into possible military applications to include research, the construction and testing of prototypes, and such design changes affecting qualitative performance as may be required during the service life of an item. This also includes engineering data, general operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when materiel has completed operational suitability testing or has, for all practical purposes, been adopted for military use or production. It includes tactics, techniques, and tactical doctrine pertaining to specific equipment not yet in production or not yet approved for adoption by U.S. forces. It includes military information, materiel, or munitions under development by U.S. private interests as a result of U.S. government contracts or derived from technology paid for by the U.S. government.

A2.4. Category 4, Production Information. Designs or drawings of chemical and mathematical equations, specifications, models, manufacturing techniques, software source codes, and related information (excluding information under Category 2 and 3) necessary to manufacture or substantially upgrade military materiel and munitions.

A2.5. Category 5, Combined Military Operations, Planning, and Readiness. That information necessary to plan, assure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined operations and exercises. This includes information regarding installations, garrisons, and facilities located within the territory under jurisdiction of, or of direct concern to, the recipient foreign government or international organization. This category is limited to that information on installations, garrisons,

and facilities as well as readiness, planning, and operational information which is necessary to further specific multilateral or bilateral plans and agreements for common defense purposes between the United States and the recipient. It does not include strategic planning and guidance or North American Defense Information.

A2.6. Category 6, United States Order of Battle. Information pertaining to U.S. forces located within territory which is under the jurisdiction of a recipient government or is otherwise of direct concern to a foreign government or an international organization. In general, authorization is limited to U.S. order of battle in the recipient countries or in adjacent geographical areas.

A2.7. Category 7, North American Defense. North American Defense Information is that which concerns plans, programs, projects, operations, and certain specific technical data pertaining to equipment directly related to North American defense, especially when it is originated by or under the mission and control of NORAD.

A2.8. Category 8, Military Intelligence. Military intelligence comprises information of a military character pertaining to foreign nations and areas.

Attachment 3

DELEGATION OF DISCLOSURE AUTHORITY LETTER (DDL) EXAMPLE

Figure A3.1. DDL Example. FDOs must have SAF/IAPD approval for any significant departure from this template. (T-1).

Country Delegation # (Provided by SAF/IAPD)	DDL Title _____
1. (U) <u>Participating Nation</u>: Name(s) of the country or countries involved in the DDL. 2. (U) <u>Classification</u>: Highest classification level of information to be released during the program. If more than one category is involved, indicate the highest classification for each category, if appropriate. NOTE: If multiple nations are involved or for exchange officer DDLs, the first paragraph will identify participating nations, with this paragraph and subsequent paragraphs renumbered accordingly. 3. (U) <u>Disclosure Methods</u>: Either "Oral, visual, and documentary" or any combination of the three methods. 4. (U) <u>Category (Categories) Permitted</u>: Specify disclosure category or categories (1 through 8), as specified in DAFMAN 16-201. 5. (U) <u>Scope</u>: Describe the purpose of the disclosure, to which country (countries) disclosure is authorized, which MAJCOM(s) is/are authorized to disclose the information or materiel, and the source of the program (e.g., letter of offer and acceptance (LOA), memorandum of understanding (MOU) or memorandum of agreement (MOA), National Disclosure Policy Committee (NDPC) record of action (RA), etc.). The purpose of the disclosure must define the intent of the program (e.g., end-item sale, cooperative development, co-production, etc.). 6. (U) <u>Authorized to Disclose</u>: Describe the information or materiel that can be disclosed to support the program. This section, and the "Not Authorized to Disclose" paragraph, cannot address every possible situation, particularly for major programs. Therefore, it is particularly important that the previous paragraphs clearly and adequately define the delegated authority so the FDO can interpret the DDL in situations specifically addressed in this and the following paragraphs. 7. (U) <u>NOT Authorized to Disclose</u>: Describe information or materiel that cannot be disclosed under the program. This paragraph and the preceding paragraph should clearly define the limits of delegated authority rather than listing everything that may or may not be disclosed. 8. (U) <u>Additional Guidance and Procedures</u>: Identifies program-unique requirements and additional offices which need to coordinate, etc. Also, identifies where requests that fall outside the scope and authority of the DDL should be submitted.	

9. (U) Further Delegation: "Not authorized" or "(Identify the MAJCOM)" may further delegate authority to disclose information to FDOs in subordinate elements as required to insure effective implementation of this delegation. Authority to disclose classified information may be further delegated only by designated disclosure officials who have been trained by SAF/IAPD. Further delegation of disclosure authority to other than designated disclosure officials must be approved by SAF/IAPD. All further delegations will be in writing and copies provided to SAF/IAPD."

Attachment 4**DISSEMINATING DDL INFORMATIONAL COPIES****Figure A4.1.**

(Your Organizational Letterhead)	Date of Memo
MEMORANDUM FOR (Identify Office Receiving DDL)	
FROM: (Identify FDO Disseminating DDL)	
SUBJECT: Information Copy of Delegation of Disclosure Authority Letter (DDL)	
1. This copy of (identify specific DDL by name) is transmitted only for the information purposes of the recipient. It is being provided (state purpose for which the DDL copy is being transmitted). This copy is subject to the following conditions: a. This DDL may not be copied in whole or in part. b. This DDL may not be incorporated into other documents. c. This transmittal memo must remain attached to the DDL.	
2. Questions regarding guidance contained in the DDL or the above conditions may be directed to (identify foreign disclosure office point of contact).	
(FDO SIGNATURE BLOCK)	
Attachment: (Identify Specific DDL)	

Attachment 5**SUBMITTING FOREIGN DISCLOSURE REQUESTS TO SAF/IAPD**

A5.1. When submitting requests to SAF/IAPD for disclosure determination, the requesting organization must address the information in this attachment in the submission. **(T-1)**. Failure to address each question below may result in the request being returned without action, with a determination pending responses to the required information listed below. Submit the completed submission to the SAF/IAPD workflow email.

A5.2. Describe the foreign disclosure request in a detailed and concise manner, answering the following:

A5.2.1. Purpose for specific information sought (e.g., Third Party Transfer, FMS Case, request for data or information, briefing clearance, conference attendance, visits, etc.).

A5.2.2. Requested completion date.

A5.2.3. What defense article, service or technical data is being proposed for disclosure (Be specific: model, make, version, etc.).

A5.2.4. Highest level of classification of release sought for this defense article, service or technical data.

A5.2.5. Originator/owner for the defense article, service or technical data (AF, other service, commercial, international partner, etc.).

A5.2.6. What does this foreign disclosure release support? For example, what is its relation to the DAF/DoD/U.S. government building partnership capacity initiatives (e.g. the purpose/importance of the disclosure, such as FMS, loans, leases, MOUs, cooperative development, acquisition, combined operations, exercises, etc.)?

A5.2.7. Proposed end-use or end-user for this article.

A5.2.8. Was this an FMS case, DCS case, etc. What is its original acquisition value (This information is necessary for Congressional reporting.), and the FMS case number, if applicable.

A5.2.9. What are the DAF equities associated with the defense article, service, or technical data? If there are other service/agency equities, list what and whom you were/are dealing with, at the other service/agency.

A5.2.10. Any other political/military factor(s) that would further support your recommendation to disclose/deny/defer (Be specific.).

A5.2.11. Precedent for this case/previous related disclosure requests/record(s) of action.

Attachment 6

FORMAT FOR AUTHORIZING DISCLOSURE OF CMI

A6.1. The following template is provided for use when drafting memoranda authorizing disclosure of CMI information. FDOs must have SAF/IAPD approval for any significant departure from this template. **(T-1).**

Figure A6.1. Format for Authorizing Disclosure of CMI.

(Your organizational letterhead)	Date of Memo
MEMORANDUM FOR (Identify Requesting Office)	
FROM: (Identify FDO Authorizing Disclosure)	
SUBJECT: (Subject of Disclosure Request)	
1. (Office/individual authorized to disclose the specific item of information) is authorized to disclose a(n) (classification of the item of information authorized for disclosure) (identify document media, i.e., briefing, report, videotape, etc.) titled (identify the specific item of information to be disclosed) on a(n) (oral, visual or documentary basis) to representatives of the (Government of the intended recipient country or international organization). The information is to be disclosed pursuant to (identify specific purpose for disclosure) and subject to the following conditions. a. The front page of the (identify document and/or electronic media, i.e., briefing, report, videotape, etc.) will contain the following statement: "This information is furnished on condition that it will not be released to another nation without specific authority of the Department of the Air Force of the United States, that it will be used for military purposes only, that individual or corporate rights originating in the information, whether patented or not, will be respected, that the recipient will report promptly to the United States any known or suspected compromise, and that the information will be provided substantially the same degree of security afforded it by the Department of Defense of the United States. Also, regardless of any other markings on the document, it will not be downgraded or declassified without the written approval of the originating U.S. agency." b. The beginning statement for electronic media containing CMI or CUI is as follows. "This information is furnished on the condition that it will be given substantially the same degree of security protection given to it by the United States and will not be released to another nation without United States Department of the Air Force authorization."	

c. Transfer of classified information and material will be accomplished only through official government-to-government channels. U.S. government responsibilities are included in the following statement.

“The U.S. government sponsor is responsible to ensure that U.S. participants (government or contractor) involved in technical discussion of U.S. export-controlled or classified information during briefings, meetings, conferences, or events are provided advanced notification of the approved scope and limitations of this disclosure decision.”

d. Discussions and documentary release beyond the scope of the foreign disclosure release are covered in the following statement.

“Discussions and documentary release beyond the contents of this release authorization will require a separate disclosure review.”

e. “FDO presentations must conform to AFI 16-1404, *Air Force Information Security Program*, 29 May 2015.”

f. (Identify any other conditions that must be met prior to disclosure).

g. A signed AF Form 349, *Receipt for Documents Released to Accredited Representatives of Foreign Nations*, must be completed, signed by the recipient and returned to (Identify the FDO who authorized the disclosure).

2. Questions regarding this disclosure authorization should be directed to (identify the POC who can answer questions regarding the approval.)

(Signature Block of Authorizing FDO)

Attachment 7

FORMAT FOR AUTHORIZING DISCLOSURE OF CUI

A7.1. The following template is provided for use when drafting memoranda authorizing disclosure of CUI. FDOs must have SAF/IAPD approval for any significant departure from this template. **(T-1)**.

Figure A7.1. Format for Authorizing Disclosure of CUI.

(Your organizational letterhead)	Date of Memo
MEMORANDUM FOR (Identify Requesting Office)	
FROM: (Identify FDO Authorizing Disclosure)	
SUBJECT: (Subject of Disclosure Request)	
1. (Office/individual authorized to disclose the specific item of information) is authorized to disclose an Unclassified (identify document media, e.g., briefing, report, videotape, etc.) titled (identify the specific item of information to be disclosed) on a(n) (oral, visual, or documentary basis) to representatives of the (Government of the intended recipient country or international organization). The information is to be disclosed pursuant to (identify specific purpose for disclosure) and subject to the following conditions. a. (Identify any other conditions that must be met prior to disclosure and include the following.) b. Include the following statement at the beginning of electronic media containing CMI or CUI: “This information is furnished on the condition that it will be given substantially the same degree of security protection given to it by the United States and will not be released to another nation without United States Department of the Air Force authorization.” c. Include the following statement, covering U.S. government responsibilities. “The U.S. government sponsor is responsible to ensure that U.S. participants (government or contractor) involved in technical discussions of U.S. export-controlled or classified information during briefings, meetings, conferences, or events, are provided advanced notification of the approved scope and limitations of this disclosure decision.”	

d. The front page of (identify document and/or electronic media, e.g., briefing, report, videotape, etc.) will contain the following statement:

“This information is furnished on condition that it will not be released to another nation without specific authority of the Department of the Air Force of the United States, that it will be used for military purposes only, that individual or corporate rights originating in the information, whether patented or not, will be respected, that the recipient will report promptly to the United States any known or suspected compromise, and that the information will be provided substantially the same degree of security afforded it by the Department of Defense of the United States. Also, regardless of any other markings on the document, it will not be downgraded or declassified without the written approval of the originating U.S. agency.”

e. Include the following statement, covering digital metadata and documentary release.

“To reduce the risk associated with latent metadata capture in digital products, documentary release is limited to paper copy only. When mission requirements dictate and are acknowledged by the responsible U.S. government authority, release of digital products is permitted in read-only .pdf or .tif format.”

f. Include the following, covering controlled unclassified information.

“Prepare the briefing by adding the following as a header and footer to the title page and each subsequent page containing CUI, “Controlled Unclassified.” Portion mark all controlled unclassified paragraphs, bullets, sub-bullets and notes pages “CUI” and all CUI graphic depictions, pictures, or charts “Controlled Unclassified” where applicable. Presentations must conform to the security classification marking requirements stipulated in AFI 16-1404.”

g. Included the following statement, covering the scope of the foreign disclosure release.

“Discussions and documentary release beyond the contents of this release authorization will require a separate disclosure review.”

2. Questions regarding this disclosure authorization should be directed to (identify the POC who can answer questions regarding the approval.

(Signature of Authorizing FDO)

Attachment 8**SAMPLE LANGUAGE TO ADDRESS ADMINISTRATIVE RESPONSIBILITIES FOR EXTENDED VISIT POSITIONS**

A8.1. The purpose of this attachment is to provide FDOs sample language used in the DoD International Agreements Generator to identify administrative support, liability, obligations, and responsibilities for Cooperative Program Personnel. Similar language is used to address support requirements for MPEP, APEP, and ESEP positions. FDOs and U.S. contact officers must review signed agreements for the positions they manage to verify specific requirements for each position. **(T-1).** FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1).**

Figure A8.1. Sample Language to Address Administrative Responsibilities for Extended Visit Positions.**1. Purpose and Scope**

- a. This Annex [or Article] establishes the terms and conditions for [identify type of program under which the foreign national is to be assigned] assigned for work in accordance with Article III [Scope of Work] of this MOU/MOA. [Assigned foreign nationals] must be able to perform all responsibilities assigned to them under this MOU/MOA. Commencement of assignments shall be subject to the requirements that may be imposed by the Host Party or its government regarding acceptance of assigned foreign nationals, such as, but not limited to, visas and visit request documentation. The Host Party and Parent Party shall determine the length of tour for the positions at the time of initial assignment.
- b. [Foreign nationals] shall be assigned to work on a specific [name of MOU/MOA activity, project, effort, etc.] and shall report to a supervisor to be identified by the Host Party. [Foreign nationals] shall have a position description mutually determined by the Parent Party and Host Party. [Foreign nationals] shall not act as liaison officers for their Parent Party.
- c. [Foreign nationals] shall not be assigned to command or other positions that would require them to exercise responsibilities that are reserved by law or regulation to an officer or employee of the Host Party's government.

2. Security

- a. The Host Party shall establish the level of security clearance required, if any, to permit [foreign nationals] to have access to classified information and facilities. Access to classified information and facilities in which classified information is used shall be limited by the scope of the relevant [name of MOU/MOA activity, project, effort, etc.].
- b. The Parent Party shall file visit requests through prescribed channels in compliance with the Host Party's procedures. As part of the visit request procedures, each Party shall cause security assurances to be filed, through the [identify the Parent Party's Government embassy and U.S. location] in the case of [insert country name] personnel, and through the U.S. Embassy in

[identify location] in the case of United States personnel, specifying the security clearances for the [foreign nationals] being assigned.

c. The host and parent party shall use their best efforts to ensure that [foreign nationals] assigned to a Host Party's facility to conduct a [name of MOU/MOA activity, project, effort, etc.] are aware of the requirements of the [title of MOU/MOA]. On arrival, [foreign nationals] and their dependents shall be informed by the Host Party's representative about applicable laws, orders, regulations, and customs and the need to comply with them. Prior to commencing assigned duties, [foreign nationals] shall, if required by the Host Party's government laws, regulations, policies or procedures, sign a certification concerning the conditions and responsibilities of [foreign nationals assigned to United States DAF organizations].

d. [Foreign nationals] shall at all times be required to comply with the security and export control laws, regulations, and procedures of the Host Party's government. Any violation of security procedures by [foreign nationals] during their assignment shall be reported to the Parent Party for appropriate action. [Foreign nationals] committing significant violations of security laws, regulations, or procedures during their assignments shall be withdrawn from the project with a view toward appropriate administrative or disciplinary action by their Parent Party.

e. All Classified information made available to [foreign nationals] shall be considered as Classified information furnished to the Parent Party and shall be subject to all provisions and safeguards provided for in Article XII* [Security].

f. [Foreign nationals] shall not have personal custody of classified information or controlled unclassified information unless approved by the Host Party and as authorized by their Parent Party. They shall be granted access to such information in accordance with article IX [Controlled Unclassified Information], Article XII* [Security], and the applicable project security instruction during normal duty hours and when access is necessary to perform work for the [name of MOU/MOA activity, project, effort, etc.].

g. [Foreign nationals] assigned to a Host Party's facility to conduct a [name of MOU/MOA activity, project, effort, etc.] shall not serve as a conduit between the Host Party and Parent Party for requests and/or transmission of classified information and material or controlled unclassified information outside the scope of their assignment, unless specifically authorized by the Parent Party.

3. Technical and Administrative Matters

a. Subject to applicable multilateral and bilateral treaties, agreements, and arrangements of the governments of the Host Party and Parent Party, [foreign nationals] and their authorized dependents shall be accorded:

(1). Exemption from any Host Party's government tax upon income received from the Parent Party.

(2). Exemption from any Host Party's government customs and import duties or similar charges levied on items entering the country for their official or personal use, including their baggage, household effects, and private motor vehicles.

b. On arrival [foreign nationals] and their dependents shall be provided briefings arranged by the Host Party's representative regarding (subject to applicable multilateral and bilateral agreements) entitlements, privileges, and obligations such as:

(1). Any medical and dental care that may be provided to [foreign nationals] and their dependents at local medical facilities, subject to the requirements of applicable laws and regulations, including reimbursement when required.

(2). Purchasing and patronage privileges at military commissaries, exchanges, theaters, and clubs for [foreign nationals] and their dependents, subject to the requirements of applicable laws and regulations.

(3). The provision, if available, by Host Party, of housing and messing facilities for [foreign nationals] and their dependents on the same basis and priority as for its own personnel. [Foreign nationals] shall pay messing and housing charges to the same extent as Host Party personnel. At locations where Host Party does not provide facilities for its own personnel, the Parent Party shall make suitable arrangements for [foreign nationals].

(4). Responsibility of [foreign nationals] and their accompanying dependents to obtain motor vehicle liability insurance coverage in accordance with the laws and regulations applicable in the area where they are residing. In case of claims involving the use of private motor vehicles by [foreign nationals], the recourse shall be against such insurance.

c. The Host Party shall, in consultation with the [foreign nationals], establish standard operating procedures for [foreign nationals] in the following areas:

(1). Working hours, including holiday schedules.

(2) Leave authorization, consistent to the extent possible with the military and civilian personnel regulations and practices of the Host Party and Parent Party.

(3). Dress regulations, consistent to the extent possible with the military and civilian personnel regulations and practices of the Host Party and Parent Party.

(4). Performance evaluations, recognizing that such evaluations shall be rendered in accordance with the Parent Party's military or civilian personnel regulations and practices.

d. [Foreign nationals] committing an offense under the laws of the government of the Host Party or Parent Party may be withdrawn from this project with a view toward further administrative or disciplinary action by the Parent Party. Disciplinary action, however, shall not be taken by the Host Party against [foreign nationals], nor shall [foreign nationals] exercise disciplinary powers over the Host Party's personnel. In accordance with Host Party's government laws and regulations, the Host Party shall assist the Parent Party in carrying out investigations of offenses involving [foreign nationals].

e. During their assignment, [foreign nationals] shall not be placed in the following duty status or environments unless mutually decided by the Host Party and Parent Party:

(1). Areas of political sensitivity where their presence may jeopardize the interests of either the Host Party or Parent Party, or where, in the normal course of their duty, they may become involved in activities which may embarrass either Party.

(2). Deployments in non-direct hostility situations, such as UN peacekeeping or multi-national operations, or third countries.

(3). Duty assignments in which direct hostilities are likely. Should a Host Party's facility become involved in hostilities unexpectedly, [foreign nationals] assigned to that facility shall not be involved in the hostilities. Any such [foreign national] approved by the Host Party and Parent Party for involvement in hostilities shall be given specific guidance as to the conditions under which the assignment shall be carried out by the appropriate authorities of the Host Party and Parent Party.

Attachment 9

INSTRUCTIONS FOR CREATING POSITION DESCRIPTIONS FOR EXTENDED VISIT POSITIONS

A9.1. The information below serves as a template to be used when creating position descriptions for foreign nationals assigned as Engineer and Scientist Exchange Program (ESEP) positions, as foreign liaison officers, and as cooperative program Personnel (CPP) within U.S. DAF organizations. (Position descriptions supporting Defense Personnel Exchange Program positions should be developed in accordance with AFI 16-107. FDOs must have SAF/IAPD approval for any significant departure from this template will require SAF/IAPD approval. (T-1).

Figure A9.1. Instructions for Creating Position Descriptions for Extended Visit Positions.

1. Position Location: Identify the organizational address of the organization where the foreign representative will perform his/her duties.

2. Position Title: Identify the title that describes the position that the foreign representative will perform duties as.

3. Description of Duties, Skills and Responsibilities: This section identifies the types of activities that the individual will be expected to perform as well as how that activity will be used. This development process may require several revisions to ensure the duties are sufficiently described. This description is important for three reasons. First, it will be used as the foundation upon which the delegation of disclosure authority letter (DDL) will be built or to verify that an existing DDL will support the position. Second, it ensures that both DAF and the foreign government agree to the duties to be performed by the foreign representative. Third, it helps the contact officer educate other DAF personnel working with the foreign representative understand the specific assigned duties of the foreign representative.

The following examples are provided to demonstrate the type of detail that the creator of the position description needs to provide in order to help facilitate the establishment of a long-term visitor position within the organization. They are grouped into unsatisfactory and satisfactory examples of descriptions of duties:

Unsatisfactory - Records and reports test results.

Satisfactory - Knowledge of the terminology used with a variety of diagnostic and treatment procedures provided general medical patients to record and report medical information such as x-ray and test results.

Unsatisfactory - Knowledge of engineering concepts to perform military research.

Satisfactory - Knowledge of materials science to research, develop and apply static and dynamic material properties measurement tests to energetic materials and simulants.

Unsatisfactory - Individual will use standard laboratory techniques.

Satisfactory - Individual will adapt and apply standard laboratory techniques for the assessment of material properties. Test techniques to be used will include Split Hopkinson

Pressure Bar Tests, Tensile Tests, and Fracture Toughness Tests for both high explosives and simulants.

Unsatisfactory - Individual will review and evaluate engineering designs.

Satisfactory- Individual will review engineering drawings for the proposed demonstrator using knowledge of mechanical engineering principles and evaluate the proposed design against XYZ program requirements.

Unsatisfactory - Specific duties will include, but not be limited to, the collection of samples, chemical analysis, data reduction and groundwater treatment process evaluation. (The phrase but not limited to indicates there are other duties, if so they should be identified.)

Satisfactory - Develop concept of operations and packaging concept for Tactical and Special Mission ground stations. Include deployment requirements, physical and functional layouts, data link requirements and procedure development issues.

4. Qualifications Required for Position: Qualifications are training, education, or other accomplishments that prepare an individual to carry out specific work or responsibilities, for example, the ability to use good English, oral and written skills, and certain types of computer software. Unique qualifications may also be desired by the organization. When qualifications are desired, identify the type of qualification and whether a specific amount of time performing the activity is required to be considered qualified. For example, 3 years performing duties as a research engineer.

5. U.S. Contact Officer: This is the name, organizational address and telephone number of the DAF official designated in writing to oversee and control all contacts, requests for information, consultations, access, and other activities of the foreign national who will be assigned to or placed in the DAF organization. Previously, this U.S. person was referred to as the "supervisor" for all extended visitors including those assigned under formal exchange programs. The term "contact officer" is now being used to be consistent with DoD terminology. In all cases of Defense Personnel Exchange Positions, the U.S. host supervisor may be the contact officer (within DAF this has traditionally been the rule).

6. Security Clearance Level Required: Confidential, Secret or Top Secret (identify one). Information will not be released to the participant based on the required security clearance. Only designated FDOs using the appropriate DDL are authorized to approve releases of classified or controlled unclassified military information to the participant. This is the level of security clearance required for access to U.S. classified military information necessary to perform assigned duties and responsibilities. The decision regarding what U.S. classified military information will be available to the foreign representative will be documented in the delegation of disclosure authority letter (DDL). Once the position has been established, the foreign government will be required to provide a security assurance to DAF that it has granted its representative a security clearance commensurate with the access required. By submitting the extended visit request, the foreign government provides the security assurance and identifies the level of clearance it has granted its participant. The bold statement above is a required statement in the position description.

Attachment 10**SECURITY PLAN SAMPLE FORMAT**

A10.1. The purpose of this sample format is to assist U.S. contact officers in documenting physical controls necessary to ensure that extended visitors' access to information and sensitive work areas is consistent with the disclosure guidance supporting the visitor's placement. All U.S. individuals coming into contact with the foreign national must be made aware of the contents of this plan as well as the disclosure guidance pertaining to the extended visitor's placement. **(T-1)**. The U.S. contact officer, foreign disclosure officer, and local information security program manager must approve the extended visitor's security plan. **(T-1)**. FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1)**.

Figure A10.1. Security Plan Sample Format.

1. Extended Visitor: Identify the individual's name, rank, and country.
2. Assigned Duty Area: Identify the physical location of the individual's work area to include physical address, building, and room number. Identify the extended visitor's normal work hours. Also, identify any other local organizations that the extended visitor will be required to visit during their placement.
3. U.S. Contact Officer: Identify the name, organizational address, and telephone number of the DAF official designated in writing to oversee and control all contacts, requests for information, consultations, access, and other activities of the extended visitor.
4. Access Controls: A general requirement is that all extended visitors identify themselves as members of their parent service in all communications. This requirement ensures that U.S. personnel communicating with the extended visitor are aware that he is an international officer. The extended visitor will be informed to identify himself as a member of his parent service in all written, electronic, and telephonic communications. The following items must be addressed separately. It may be necessary to identify other controls depending upon the activities taking place at the organization. To identify if other controls are necessary, review activities of U.S. personnel who have similar responsibilities.
 - a. Computer Access: The supporting foreign FDO and systems accreditation authorities must be included in the approval process. Document the approved computer access with any conditions that apply.
 - b. Other Equipment Use: Identify the equipment and the location that the extended visitor is authorized to use. Are there any requirements which must be met before the equipment can be used (e.g., use logs, etc.)? If so, identify them.

c. Physical Access: Identify whether the extended individual will have escorted or unescorted access to the work area or any other areas. For unescorted access, identify that the extended visitor has been issued a badge or pass that clearly identifies him as a foreign national, the badge is valid for specific facilities during normal duty hours, and the organization has received a security assurance from the individual's government verifying that he meets all clearance requirements for unescorted access to the facility (facilities). Identify for what official purposes unescorted access is required on a frequent basis. Identify how the unescorted access will be prevented outside normal duty hours.

d. Information Access: Identify the actions U.S. personnel will be responsible for taking to ensure that classified and controlled unclassified information in their work areas or common work areas will be controlled during the placement of the extended visitor. Also, ensure that guidance for U.S. personnel conducting classified discussions in the office is included.

e. Organization Visitors: Identify how the organization will ensure that visitors are informed about the existence of the extended visitor and the disclosure and security requirements that are in place regarding the visitor.

f. Extended Visitor Visits:

(1) Identify how the organization will ensure that extended visitor contacts outside of the organization are informed of the disclosure and security requirements regarding the visitor.

(2) Identify that the extended visitor will be required to submit a visit request through his/her embassy channels for visits outside his/her location of assignment.

g. Emergency Procedures: Identify the actions that will be taken should the extended visitor be found unescorted outside the areas approved for unescorted entry or have access to information not approved for release. This information should include the name, location and telephone numbers of any individuals who should be contacted.

h. Points of Contact: Identify all points of contact appropriate for this placement. As a minimum, identify the FDO, unit security manager, the installation or garrison information security program manager, facility entry control points, others as appropriate for the organization.

Attachment 11

**SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES FOR
DEFENSE PERSONNEL EXCHANGE PROGRAM PERSONNEL**

A11.1. The following is provided for use as a template for drafting certification of conditions and responsibilities letters for Defense Personnel Exchange Program personnel. FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1).**

Figure A11.1. Sample Certification of Conditions and Responsibilities for Defense Personnel Exchange Program Personnel.

I understand and acknowledge that I have been accepted for assignment to [insert name and location of organization to which assigned] pursuant to an agreement between the United States Department of the Air Force and the Air Force of [insert country name]. In connection with this assignment, I further understand, acknowledge, and certify that I will comply with the following conditions and responsibilities:

1. The purpose of this assignment is to gain knowledge of the organization and management of United States Department of the Air Force [cite area of assignment] defense activities. There shall be no access to information except as required to perform the duties described in the position description (PD) of the position to which I am assigned, as determined by my designated United States Department of the Air Force supervisor.
2. I shall perform only functions that are properly assigned to me as described in the PD for my assignment, as set out in the Annexes to this Arrangement, and shall not act in any other capacity on behalf of my government or my parent service.
3. All information to which I may have access during this assignment shall be treated as information provided to me in confidence and shall not be further released by me to any other person, firm, organization or government, including my parent government, without the prior written authorization of the United States Department of the Air Force.
4. When dealing with individuals outside my immediate office of assignment on official matters, I shall inform such individuals that I am a foreign exchange person.
5. I have been briefed on, understand, and shall comply with all applicable security regulations of the United States Department of the Air Force and Host Organization.
6. I shall immediately report to my supervisor any attempts by unauthorized personnel to obtain classified, restricted, proprietary, or controlled unclassified information to which I may have access as a result of this assignment.

(Printed/Typed Name)

(Signature)

(Rank/Title)

(Date)

Attachment 12

**COMMITMENT REGARDING INVENTIONS MADE AND TECHNICAL
INFORMATION DEVELOPED BY VISITING SCIENTISTS AND ENGINEERS**

A12.1. The following serves as the template for use when drafting the commitment regarding inventions made and technical information developed by visiting scientists and engineer's letter. FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1)**.

**Figure A12.1. Commitment Regarding Inventions Made and Technical Information
Developed by Visiting Scientists and Engineers.**

In consideration for being selected to participate in the United States Department of the Air Force (*insert country name*) Personnel Exchange Program, I hereby grant to the United States Department of the Air Force a worldwide, non-transferable, irrevocable, non-exclusive, royalty-free license to make, use, or sell inventions, whether patentable or not, and unlimited use and reproduction rights for technical information developed by me during the period of and as a result of my participation in this program.

Additionally, to secure the rights granted above, I hereby grant to the United States Department of the Air Force the right to prosecute or to have prosecuted patent applications on the above-mentioned inventions in any country for which my parent service or I choose not to prosecute a patent application.

(Signature of Exchange Personnel)

(Date)

Attachment 13

**SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES FOR
COOPERATIVE PROJECT PERSONNEL (CPP)**

A13.1. The following serves as the template for use when drafting the certification of conditions and responsibilities letter for cooperative program personnel (CPP). FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1)**.

Figure A13.1. Sample Certification of Conditions and Responsibilities for Cooperative Project Personnel (CPP).

I understand and acknowledge that I have been accepted for assignment to (insert name and location of project to which assigned) pursuant to [identify agreement which provides for the cooperative program]. Capitalized terms in this certification have the meanings defined in the MOU/MOA. In connection with this assignment, I further understand, acknowledge, and certify that I shall comply with the following conditions and responsibilities:

1. The purpose of the assignment is to provide my expertise to the project [or Program]. There shall be no access to project information except as required to perform my assigned duties or as otherwise authorized in accordance with the MOU/MOA.

2. All [identify agreement which provides for the cooperative program] project information to which I may have access during this assignment shall be treated as information provided to my government in confidence and shall not be further released or disclosed by me, except as authorized by the MOU/MOA.

3. I have been briefed on, understand, and shall comply with all applicable laws and regulations pertaining to classified information and material and controlled unclassified information as well as the requirements of [identify applicable MOU/MOA Articles; e.g., Article IX (Disclosure and Use of Project Information), Article X (Visits to Establishments), Article XI (Controlled Unclassified Information), Article XII (Security)], and the Project Security Instruction and Classification Guide.

4. When dealing with individuals outside of my immediate office of assignment on official matters, I shall properly identify myself.

5. I shall immediately report to my designated supervisor all unauthorized attempts to obtain classified information and material or controlled unclassified information to which I may have access as a result of this assignment.

6. [Include the information in Attachment 12, Commitment Regarding Inventions Made and Technical Information Developed by Visiting Scientists and Engineers, verbatim.]

(Printed/Typed Name)

(Signature)

(Rank/Title)

(Date)

Attachment 14

SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES FOR FOREIGN LIAISON OFFICERS (FLO)

A14.1. The following serves as the template for use when drafting the certification of conditions and responsibilities letter for foreign liaison officers (FLO). FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1).**

Figure A14.1. Sample Certification of Conditions and Responsibilities for Foreign Liaison Officers (FLO).

I understand and acknowledge that I have been accepted for assignment to (insert name and location of Project Office to which assigned) pursuant to [identify LOA including a short case description which provides for the liaison activity]. In connection with this assignment, I further understand, acknowledge, and certify that I shall comply with the following conditions and responsibilities:

1. The purpose of the assignment is to provide my expertise to the [identify FMS program(s) for which the individual will be a liaison officer]. There shall be no access to U.S. government information except as required to perform my liaison duties.
2. All [identify LOA that provides for the liaison activity] information to which I may have access during this assignment shall be treated as information provided to my government in confidence and shall not be further released or disclosed by me, except as authorized by the U.S. government.
3. I have been briefed on, understand, and shall comply with all applicable laws and regulations pertaining to classified information and material and controlled unclassified information as well as the requirements of [identify any applicable host organization security instructions].
4. When dealing with individuals outside of my immediate office of assignment on official matters, I shall properly identify myself as a foreign liaison officer in all modes of written and verbal communication, to include memoranda, electronic mail address and signature blocks, and telephonically.
5. I shall immediately report to my designated supervisor all unauthorized attempts to obtain classified information and material or controlled unclassified information to which I may have access as a result of this assignment.

(Printed/Typed Name)

(Signature)

(Rank/Title)

(Date)

Attachment 15

SAMPLE ITAR EXEMPTION CERTIFICATION REQUEST LETTER

A15.1. The following serves as the template for use when drafting ITAR Exemption request letters for submission to SAF/IAPD. FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1).**

Figure A15.1. Sample ITAR Exemption Certification Request Letter.

(Your organizational letterhead)	Date of Memo
MEMORANDUM FOR Field FDO Office Symbol MAJCOM FDO Office Symbol SAF/IAPD Attn: Chief, Foreign Disclosure & Technology Transfer 1080 Air Force Pentagon Washington, DC 20330-1080	
FROM: (Your office) (Your address) (Supporting Office Location) 12345-6789	
SUBJECT: Request for Certification of ITAR Exemption or Extension for (contractor name)	
1. (Subject Program Office) has requested an ITAR Exemption under 125.4(b) (1) and/or 126.4 for (CONTRACTOR) to support (FMS Case XX-Q-XXX or contract ###). The exemption will enable (CONTRACTOR) to provide or continue providing technical data and defense services to the Government of XXX in support of FMS or contract. (Then state the benefit to the U.S. in allowing the contractor to provide the information). Request this extension be approved from (insert dates requested) or until TAA is approved and granted. 2. (CONTRACTOR) supports the (Program Office), as the Chief Engineer for the Program contract. As the Chief Engineer, (CONTRACTOR) supports Field Level and provides oversight responsibility on behalf of the U.S. government at various meetings which include assigned supporting and operational (Country/Foreign National) personnel. (Country/Foreign National) provides (insert responsibilities and justification). These exemptions apply to (CONTRACTOR) technical staff that directly supports the Program Office at (SUPPORTING OFFICE LOCATION). (CONTRACTOR) has certified their compliance with and shall remain eligible for these exemptions pursuant to ITAR 120.1, as well as other ITAR conditions applicable to the use of exemptions. 3. Justification for this request is as follows: (CONTRACTOR) submitted a Technical Assistance Agreement TAA to the Department of State – Directorate of Defense Trade Controls DDTC. (CONTRACTOR) was assigned a DDTC Case#: (insert contractor license info and date requested). (CONTRACTOR) shall immediately acquire signatures of (Foreign Government) as soon as the approved TAA is received from the DDTC. Denial of this request	

would significantly affect the U.S. government's oversight responsibility for critical technical assistance in support of our nation's air, missile, and space warning systems (provide rationale for urgency of request).

4. All proposed disclosures of technical data or assistance to (Country/Foreign National) personnel shall be authorized by field foreign disclosure office or MAJCOM foreign disclosure office, in accordance with the applicable delegation of disclosure authority Letters DDL (insert applicable DDL number and/or policy and date of document). U.S. government personnel, who have been trained as escorts and are familiar with the DDLs, and limitations of this exemption, shall be in attendance at all meetings whenever (Country/Foreign National) are present. No defense articles software/hardware will be shipped under provisions of the exemptions to Country Y.

5. My POC for this request is Ms. Jane Doe, Title (YOUR OFFICE) Phone 000-000-0000 DSN 000-0000.

Requesting official's signature block
(Must be an O-6 or GS-15)

Attachment 16**SAMPLE ITAR EXEMPTION CERTIFICATION CHECKLIST**

A16.1. The purpose of this checklist is to assist FDOs at SAF/IAPD, MAJCOM, and field levels to ensure that ITAR exemption certification requests contain the appropriate details required to complete certification. This checklist captures lessons learned from processing previous ITAR exemption certifications. FDOs must have SAF/IAPD approval for any significant departure from this sample. **(T-1)**.

A16.2. The information requested in the questions below is required for each ITAR exemption certification request submitted to SAF/IAPD for processing:

Figure A16.1. Sample ITAR Exemption Certification Checklist.

1. Identify whether the certification requested is to support exports by U.S. contractors only. (The answer must be “yes” to proceed with the ITAR exemption). **(T-1)**.
2. Identify the expertise provided by the contractor to DAF (as related to the DAF requirement). **(T-1)**.
3. Identify the relationship between DAF and the U.S. contractor (provide contract number if one exists). **(T-1)**.
4. Identify the services provided to the DAF under the contract. **(T-1)**.
5. Identify the export license application number, if the contractor has applied for one, to support exports under the contract. If this information is unknown, or if the contractor has not submitted a license application, please indicate. NOTE: The following statement will be included on all ITAR Exemption Certifications: “SAF/IAPD is granting this ITAR Exemption Certificate on the understanding that the requestor must submit a Technical Assistance Agreement (TAA) to the Department of State's Directorate of Defense Trade Controls (DDTC) to ensure that they have the legal authority to export defense services and/or technical data for further activities as described herein.” **(T-1)**.
6. Specifically identify (by title, number) the relationship between the DAF and foreign government end use (e.g., the LOA or international agreement under which the exports will be made). **(T-1)**.
7. Specifically identify (by full/accurate company or personal name, as applicable) any foreign contractors to whom exports are anticipated. **(T-1)**.
8. Specifically identify the defense articles, services, and technical data proposed for export; include a parts list for any/all hardware. **(T-1)**.
9. Identify the DAF organization that will transfer data regarding documentary disclosures, if requested. **(T-1)**.

10. Include contact information for the company's export control officer. **(T-1)**.
11. Identify the classification of the proposed export. **(T-1)**.
12. Provide the dates relevant to the export (e.g., the specific length of time desired for certification). **(T-1)**.

Attachment 17

FOREIGN DISCLOSURE EXCEPTION TO NATIONAL DISCLOSURE POLICY
PROCESS

Figure A17.1. Foreign Disclosure Exception to National Disclosure Policy Process.

