CHAPTER 7

INTERNATIONAL VISITS AND ASSIGNMENTS

A. INTRODUCTION.

1. The Department of Defense (DoD) and DoD cleared contractor facilities host thousands of foreign national visitors on an annual basis. Hundreds of these visitors are foreign government representatives assigned to DoD facilities in different capacities. In some cases, cleared DoD contractor facilities also have foreign government representatives assigned, and they hire foreign national employees. These visitors, assignees, and employees present a significant risk of unauthorized disclosures or compromises of DoD classified military information (CMI) and controlled unclassified information (CUI), as well as other export controlled technical data, unless prescribed access controls are appropriately applied. As a consequence, DoD has established specific requirements and procedures to control visits and assignments of foreign nationals to DoD facilities and cleared contractor facilities.

2. The DoD has codified the requirements and procedures for visits and assignments of foreign nationals in the International Visits Program (IVP). The IVP documents the process for considering requests by foreign governments and international organizations for visits and assignments. Within the IVP there are three subspecialty programs. The first is the Foreign Liaison Officer (FLO) Program, which documents the policy and procedures governing visits and assignments of FLOs. The second is the Defense Personnel Exchange Program (DPEP), which documents the policy and procedures for the assignment of exchange officers under the DPEP. And finally, the Cooperative Program Personnel (CPP) Program, which documents the policies and procedures for the assignment of foreign government representatives in support of cooperative arms agreements. Foreign nationals visiting or assigned under the foregoing programs are representing or are sponsored by a foreign government or international organization and are “official visitors”. The requests for visits and assignments are processed in the Foreign Visits System (FVS). Only official visitors may have access to classified information and CUI.

3. Hundreds of DoD personnel visit abroad on an annual basis, conducting official business for the Department. Procedures also have been established to control these visits and disclosures of DoD official information during the visits.

4. This chapter describes the policy and procedures for visits and assignments of foreign nationals to DoD components and cleared contractor facilities. These procedures are contained in DoD Directive 5230.20 *(reference gg).* The requirements for international visits by DoD personnel are contained in DoD Directive 4500.54 (*reference pp*) and DoD 4500.54-G *(reference kkk).*

5. Foreign national visitors who are not sponsored by a foreign government or international organization are “unofficial visitors”. Their access to DoD facilities is governed by DoD Instruction 5200.08 *(reference bbbb).* Access to information at DoD facilities by “unofficial visitors” is limited to that which is in the public domain.

B. POLICY.

1. The decision to grant access to CMI and CUI during visits and assignments of foreign nationals is to be consistent with the national security and foreign policy interests of the United States (U.S.) and the government-to-government principle. Therefore, foreign nationals shall have access to such information only if they represent or are officially sponsored by their government or an international organization, i.e. an “official visit.” To assure adherence to this requirement, the sponsoring government or international organization shall provide a security assurance, in the form of a visit request, on all visitors requiring access to CMI and CUI. Only foreign nationals in an official visit status may be assigned to DoD Component organizations.

2. The IVP process and the FVS shall not be used as the authority for training foreign nationals; training must be authorized by statute and implementing DoD policy.

3. Requests for official visits to the United States shall be submitted through the sponsoring government’s embassy in Washington, DC, or by the sponsoring international organization, using the FVS and IVP procedures. Visits to DoD Components outside the United States shall be in compliance with procedures established by the Chairman of the Joint Chiefs of Staff for the Combatant Commands and by the Military Departments for their subordinate organizations. These procedures must be commensurate with the requirements of DoD Directive 5230.20.

4. A Request for Visit (RFV) to a DoD contractor facility that is approved by a DoD Component may constitute an exemption to the license requirements of the International Traffic in Arms Regulations (ITAR) *(reference c)* for a DoD contractor. However, only when the visit is in support of a government program. Additionally, the RFV and/or DoD visit authorization for such a program must identify the exporter, the specific technical data to be disclosed, the end user, and the end use. DoD officials shall not approve visits to a contractor facility for a commercial program; the contractor must obtain an export authorization for exports during a visit related to a commercial program.

5. RFVs shall be approved by the responsible DoD Component Principal Disclosure Authority (PDA), Designated Disclosure Authority (DDA), or Defense Visit Office (DVO) in compliance with DoD Component procedures which implement DoD Directive 5230.20. The DoD Component official is responsible for ensuring the appropriate type of RFV is requested by the foreign government or international organization and the requirements of DoD Directive 5230.20 are satisfied.

6. Foreign nationals shall have access during their visit to only that CMI authorized under the National Disclosure Policy (NDP)-1 *(reference s)* for disclosure to their government or international organization. This is in compliance with the government-to-government principle,

7. Information to be disclosed to foreign nationals by DoD personnel during the visit shall be reviewed and approved for disclosure prior to the visit in accordance with DoD Directive 5230.11 (*reference ee*), DoD Directive 5230.25 (*reference l*), and/or DoD Regulations 5400.7-R *(reference h)*. All DoD contractors shall ensure an export authorization has been approved or an export exemption applies in accordance with the ITAR or the Export Administration Regulations (EAR) (*reference e*). Subject to compliance with paragraphs 5 and 6, above, and this paragraph, information to be disclosed to the visitor shall have further limitations placed on it. Limitations include information for which the visitor has a need-to-know, consistent with the terms of the approved visit authorization and related Delegation of Disclosure Authority Letter (DDL) or, in the case of contractor facilities, an export authorization.

8. A visit by persons, who are Representatives of a Foreign Interest (RFI), which involves access to CMI, CUI, or other official information not authorized for public release, shall be handled as a foreign visit pursuant to DoD Directive 5230.20. RFIs include U.S. citizens employed by foreign governments, foreign companies and international organizations. (In this context, a foreign owned company located and incorporated to do business in the U.S. is a "U.S. Person", not a foreign interest.)

9. The terms and conditions for assigning foreign nationals to a DoD Component shall be established in a legally binding international agreement, an annex to such agreement, or a master agreement. Currently policy provides an exception for Security Assistance Liaison Officers from countries having a General Security Agreement with the U.S., if the requirements contained in an agreement are incorporated in the pertinent LOA. These agreements are coordinated and negotiated in compliance with DoD Directive 5530.3 *(reference dd).*

10. In accordance with section 1082 of Public Law 104-201 *(reference cccc)*, the assignment of visitors as foreign exchange personnel under the DPEP requires the negotiation of an international agreement. The international agreement provides for the reciprocal assignment of personnel of equal qualifications, training and skills. The law also stipulates that no personnel exchanged pursuant to an agreement may take or be required to take an oath of allegiance to the host country or to hold a position in an official capacity. This law also may not be used to train foreign exchange officers.

11. Requests for coordination and approval of DPEP agreements and CPP agreements shall include a position description and a DDL. Requests for FLO agreements shall include a DDL. A visitor shall not serve concurrently as a DPEP assignee and a FLO. A CPP assignee may serve concurrently as a FLO.

12. Prior to assigning a FLO or CPP to a DoD contractor facility, the DoD Components shall coordinate with the contractor facility and the Director, Defense Security Service (DSS), to establish written responsibility for security oversight of the FLO and CPP activities.

13. A Contact Officer knowledgeable in the policies and procedures contained in DoD Directive 5230.20 shall be designated to monitor the activities of foreign nationals assigned to the DoD Components or DoD contractor facilities.

14. The occurrence of visits by foreign nationals to the DoD Components, except visits at activities or events that are open to the general public, shall be documented using the FVS Confirmation Module (CM) or other procedures approved pursuant to DoD Directive 5230.20, as described in section G, below. DoD contractors shall maintain records of foreign national visitors as required by the ITAR.

15. Physical access controls and procedural controls shall be employed to ensure foreign national visitors and assignees do not have access to locations where they may gain unauthorized or inadvertent access to information that has not been properly authorized for disclosure to their government or international organization. When unescorted access to DoD work areas is permitted, it shall be the during normal duty hours for the DoD employees at the location.

16. Information to be disclosed to unofficial visitors and to visitors during events that are open to the public shall be approved for release into the public domain pursuant to DoD Directive 5230.09 *(reference uu).*

17. The following visits need not be processed through the FVS, provided they are recorded in compliance with paragraph 14 above, and provided the security controls and procedures of DoD Directive 5230.20 and implementing documentation are enforced:

a. Visits by foreign nationals on Invitational Travel Orders (ITOs) for International Military Students (IMS) (DD Form 2285) pursuant to DoD 5105.38-M *(reference d)* or section 168(c) of Title 10.

b. Unclassified visits under the United States- Canada Joint Certification Program by Canadian government officials and by Canadian defense contractors who are certified at the United States-Canada Joint Certification Office at the Defense Logistics Agency, Battle Creek Michigan.

c. Visits by foreign nationals participating in the Department of State's (DoS) Bureau of Educational and Cultural Affairs tours and other similar DoS initiatives. Such visits shall be handled as public visits.

d. Visits conducted at DoD contractor facilities involving access only to unclassified information, provided such information is authorized for export pursuant to the ITAR or EAR, and provided:

(1) The visit is in support of a commercial program, and

(2) The information to be disclosed does not reveal technical data related to a classified defense program; or

(3) A contract or export authorization proviso does not require a visit request.

e. Visits to DoD Components and DoD contractor facilities by foreign nationals who are employees of other DoD contractor facilities. Such visits will be processed in accordance with the National Industrial Security Program Operating Manual (NISPOM) *(reference (z)).*

18. Visits by DoD personnel resulting in assignments in other countries shall be in compliance with DoD Directive 4500.54, DoD 4500.54-G, and DoD Directive 5230.20. When the DoD Components assign personnel to other countries, they shall ensure a DoD organization is designated to provide administrative support for and disciplinary authority over the DoD personnel.

C. INTERNATIONAL VISITS PROGRAM.

1. When a visit authorization is required, the RFV authorization must contain the information described in this Handbook at Appendix P, International Visits Procedures, and be submitted by the sponsoring government or international organization over the FVS using IVP procedures. The RFV is to be addressed to the DVO of the DoD Component to be visited. Each Military Department has a DVO, which processes RVAs for their subordinate organizations and contractor facilities. The Defense Intelligence Agency (DIA) DVO processes RVAs for the Office of the Secretary of Defense (OSD), the Office of the Joint Chiefs of Staff, and the Defense Agencies, and their contractors. However, the DDA of the visited DoD Component is responsible for the disclosure decision, not the DIA. The addresses of the DVOs are listed at Appendix F. Failure to provide the required information in the appropriate format may result in the request being denied or returned without action.

2. The FVS permits the participating government, through its embassy, to create visit requests in an established format on a personal computer and submit them via electronic connection to the FVS communications processor. The requests are then sent to the FVS central processor which distributes them to the applicable DVOs. The DVOs provide a staffing scheme identifying the appropriate DoD and commercial facilities with which the request is to be staffed. Upon completion of staffing, the DVO renders a decision and returns to the submitting embassy or organization over the same electronic path used for submission of the request. Foreign embassies or international organizations not participating in the FVS must submit two typed copies of their requests directly to the applicable DVO who enters and processes the request in the FVS.

3. DIA provides foreign embassies instructions for submission of visit requests under the FVS including assignments under the FLO, DPEP, and CPP Programs. These instructions provide information on obtaining documentary information.

D. TYPES OF VISITS.

The DoD policy identifies three types of international visit authorizations:

1. One-Time Visit. This shall be used to document a single, short term visit to a DoD Component or DoD contractor facility, when the visitor is not to be assigned to the DoD Component installation or DoD contractor facility. It is used for visitors when there is no known requirement for subsequent visits to the DoD Component or contractor in the foreseeable future, and the conditions for a recurring visit authorization or extended visit authorization do not apply. Upon approval of the request, visitors may arrange visit details directly with the installation or facility to be visited.

2. Extended Visit. This shall be used to certify national representatives and other FLOs who are stationed at their embassies and are authorized to conduct business with the DoD Components, operating from their embassies. It also shall be used to document the assignment of each foreign national to a DoD Component or DoD contractor facility. For the DoD Components, the assignment shall be under the terms of an international agreement. This authorization may be valid for the duration of the certification. Extended visit authorizations usually support assignments of foreign nationals to a DoD facility under one of the following situations:

   a. The CPP if required by a cooperative program agreement;

   b. Foreign exchange officers under the DPEP; or

   c. Foreign liaison officers to a DoD component under the FLO Program.

3. Recurring Visits. This shall be used to document intermittent, recurring visits to DoD Components or DoD contractor facilities. It is to be used in support of government approved and documented programs, agreements, export authorizations, and contracts when the foreign disclosure decision or export authorization has been approved. The authorization is established by identifying each government organization and contractor facility to be involved in a program and, for each organization or facility, preparing a list of the organizations' and facilities' personnel who will be involved in the program, along with their level of security clearance. Each such "facility list" with the listed personnel shall be verified by each participating government, who also shall provide the security assurance for its organizations' and facilities' personnel. The lists are exchanged, and any person on a list may visit another facility, subject to the requirements agreed upon by the participating governments, without having to submit additional RFVs. The authorization may be valid for the duration of the program or contract, subject to annual review and revalidation. The lists of visiting personnel and organizations or facilities to be visited shall be reviewed and updated annually to verify the continued involvement of personnel, organizations, and facilities on the lists.

E. HOSTED VISITS TO DOD FACILITIES.

A hosted visit may be used by DoD officials in those circumstances when an RFV for a recurring visit authorization is not appropriate. It permits DoD officials to issue an invitation to foreign nationals to visit a DoD Component or to participate in a gathering at the invitation of the DoD Component. This invitation must be in support of authorized programs or projects when there will be a need for non-programmed, recurring meetings, often hosted by each of the governments participating in the program on a rotational basis. Visits to DoD facilities by foreign nationals at the invitation of DoD officials do not normally require the submission of a complete visit request by the visitors. This applies if the DoD official who extends the invitation notifies the supporting DVO, who will in turn make security arrangements with the appropriate embassy. However, the DVO must nevertheless obtain a security assurance on the visitors. A visit request may be used for this purpose. The DDA also must authorize the disclosure of the information prior to the invitation being extended.

F. VISITS IN EMERGENCY SITUATIONS.

Although not a separate type of visit, most countries allow for "emergency" visits when unforeseen situations occur which do not permit the use of standard visit request procedures (usually with less than the normal processing time). To qualify as an Emergency Visit, the visit must relate to a specific government approved contract, international agreement or announced request for proposal, and failure to make the visit reasonably could be expected to seriously jeopardize performance on the contract or program, or loss of contract opportunity. Requests for emergency visits will be controlled and will be approved for a single, one-time visit only. The requester should coordinate the emergency visit in advance with the person to be visited. The request must contain the complete name, grade, or position, address and telephone number of the person and a knowledgeable foreign government point of contact. Additionally, the request must identify the contract, agreement or program, and the justification for the emergency visit request.

G. FOREIGN VISITS SYSTEM-CONFIRMATION MODULE.

The DoD Component hosting a visit by foreign nationals shall document the actual occurrence of the visit using the FVS-CM or other Component unique system already in place. The system used must be capable of recording and reporting the required information. If any DoD Component uses an automated system not integrated with the FVS-CM, then that system shall be integrated with the DoD Cornerstone System. DoD contractors shall be required to maintain records of the visits as required by ITAR, and make those records available to the DSS, if so requested. The report shall verify the date(s) of the visit, locations visited (to include approved deviations from the locations specified in the initial RFV), identification of foreign nationals who participated in the visit. It should include the identification of foreign nationals not on the

approved visit authorization who attempted to accompany the visitors, any attempts by visitors to seek information beyond that which was approved by the visit authorization, and any attempts to visit locations beyond those that were approved.

H. PROCEDURES FOR FOREIGN NATIONAL VISITS TO DOD FACILITIES.

1. Requests for One-time or Recurring Visits to DoD facilities normally must be received by the appropriate DVO at least 21 work days (30 calendar days) in advance of the date of the proposed visit. Requests to establish new liaison programs under an extended visit authorization require 90 calendar days advance notice, while those for filling currently established liaison positions require 45 calendar days for processing. A security assurance is required with the RFV for foreign national visitors and assignees. Amendments to visit requests are not authorized except to change dates to a later date or change the names of visitors. If other information is to be changed, a new visit request must be submitted. Requests for emergency visits and approved visit authorizations cannot be amended.

2. Upon approval of a visit, the appropriate DoD DVO will identify a Contact Officer at the activity to be visited who will be responsible for the visitor. The foreign embassy may work directly with the Contact Officer to complete administrative arrangements for the visit. The foreign embassy should notify the contact officer at least 72 hours (not counting weekends and holidays) prior to the expected date and time of arrival of the visitor so necessary arrangements (e.g., access and escort) can be completed.

3. Unless specifically stated in the visit authorization, visitors are not authorized to request documentary information directly from the host activity. Requests for documentary information must be submitted through the visitor's Embassy. It normally is the visitor’s military attaché office in Washington that is responsible for ensuring all visitors are aware of this restriction. When a visitor is designated in the visit request as a government courier by his or her government, the visitor must have appropriate government issued courier orders and identification, and the necessary documentation required by carrier and port security authorities and Customs. The specific material to be transported by the courier must be identified in the visit request. The material must be inventoried, packaged and addressed in compliance with DoD Regulation 5200.1-R *(reference j)*, and the courier shall sign for the sealed package.

4. All visitors must have in their possession personal identification containing a picture and an identification number, date of birth, and nationality. They also must know the applicable visit authorization number.

I. VISITS BY REPRESENTATIVES OF NORTH ATLANTIC TREATY ORGANIZATION (NATO) AND REPRESENTATIVES OF OTHER INTERNATIONAL ORGANIZATIONS.

1. All visits involving access to NATO information or U.S. classified information by a NATO Command or Agency or the NATO International Staff, including U.S. citizens (military and civilian) assigned to a NATO position will be processed in the FVS under the IVP in compliance with DoD Directive 5230.20 and the NISPOM.

2. Care must be exercised when dealing with U.S. citizens assigned to an international organization. When representing an international organization they are RFIs and authorized to receive only U.S. and foreign government information authorized for disclosure to the particular international organization they represent.

J. VISITS BY FOREIGN NATIONALS TO CLEARED CONTRACTOR FACILITIES.

1. The DoD visit authorizations are not necessary under the circumstances described in section B.17, above. If an export authorization is required, it is the contractor's responsibility to ensure it is obtained. Requests for visits to defense contractor facilities by foreign nationals involving the disclosure of or access to CMI or unclassified information related to a classified program, and plant visits covered by the ITAR exemption on plant visits, as described below, will be processed through the sponsoring foreign government (normally the visitor's embassy) to the controlling DoD Component DVO for approval. As described in subparagraphs a. through c., below, the DoD Component may approve or deny the request, or decline to render a decision. However, if CMI is to be disclosed, a visit request must be submitted even though the contractor has a valid export authorization. In this case, the visit request is the means used by the sponsoring government to pass the security assurance on the visitors.

a. Approved. The DoD Components will approve foreign visits to contractor facilities only when the proposed visit is in support of an actual or potential government program (e.g., a program involving a U.S. government agency and the intended recipient foreign government such as FMS sales or an international agreement). When the DoD Component approves a visit, the notification of approval will contain instructions on the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations. The approval will be transmitted to the contractor to be visited. Final acceptance of the visit will be subject to the concurrence of the contractor. Contractors must comply with the instructions provided by the DoD Component. The contractor must notify the DoD component when a visit is not desired.

b. Denied. If the DoD Component does not approve the disclosure of the information related to the proposed visit, it will deny the request. The requesting government and the

contractor to be visited will be advised of the reason for the denial. The contractor may accept the visitor(s); however, only information in the public domain may be disclosed and no commitments are to be made concerning the subject on which disclosure authorization was denied.

c. Non-Sponsored. The DoD Component will decline to render a decision on a visit request that is not in support of a government program (i.e., DoD is not a party to the transaction). A declination notice, indicating the visit is not government approved (i.e., non-sponsored), will be furnished to the requesting government with an information copy to the contractor to be visited. A copy of the visit request will accompany the declination notice. A declination notice does not preclude the visit, provided the contractor has, or obtains, an export authorization for the information involved. If CMI is involved, the DoD Component must notify the contractor they have received the required security assurances on the visitors from the requesting foreign government. The normal visit request procedure is used to obtain this assurance, even though the contractor has a license authorizing the disclosure of specified information. It is the responsibility of the contractor to consult applicable export regulations to determine licensing requirements regarding the disclosure of export controlled information during such visits by foreign nationals.

2. Controlling Access by Foreign National Visitors to Classified Information and CUI. Contractors must establish procedures to ensure foreign visitors are not afforded access to CMI, CUI, and other export controlled technical data except as authorized by an export license, approved visit request, or other exemption to the licensing requirements. Contractors will not encourage a foreign visitor to seek a higher level of access than authorized by the DoD Component. The fact that a foreign visitor may possess a personnel security clearance at a particular level does not entitle the visitor to receive U.S. classified information at that level. Foreign visitors are not to be given custody of classified material except when they are acting as an official courier of their government and the DSS authorizes transfer.

3. Visitor Records. Records shall be maintained for all foreign national visits involving access to export controlled information in compliance with the ITAR, normally at least five years. The records for visits involving access to CMI and CUI must clearly identify the foreign national visitors and the information divulged.

4. Visits to Subsidiaries. A visit authorization for a visit to a parent facility also may be used for visits to other divisions or subsidiaries of the same company provided disclosures are for the same purpose; the information to be disclosed does not exceed the parameters of the approved visit request; and the controlling DoD Component DVO concurs.

K. CONTROL OF ACCESS BY FOREIGN NATIONALS.

Foreign nationals, including foreign exchange personnel, FLOs and CPP assignees may not have uncontrolled access to DoD facilities and cleared contractor facilities. They may, however, have unescorted access when all of the following conditions are met:

1. The foreign national's government extends commensurate reciprocal privileges to DoD employees;

2. The foreign national is sponsored by his or her government; the need for frequent access is justified, and the requisite security assurance is provided;

3. Security measures are in place to control access to information and sensitive areas within the DoD facility;

4. Access is required for official purposes on a frequent basis (i.e., more than once a week);

5. A badge or pass is issued identifying the bearer as a foreign national and is valid for a specific facility during normal duty hours;

6. The badge or pass is displayed on the outer clothing so it is clearly visible; and

7. The request for issuance of the badge or pass is in writing and describes how the above requirements will be met.

L. ACCESS TO CLASSIFIED INFORMATION BY FOREIGN NATIONAL EMPLOYEES OF DOD CONTRACTORS.

Foreign nationals may not be hired for positions requiring access to classified information except under unique circumstances in support of a user agency contract, as described in DoD Regulation 5200.2-R *(reference jjj)* and the NISPOM. Access to export-controlled technical data, including classified information, by foreign national employees of U.S. contractors is predicated on an export license being obtained by the employing contractor (see also section M., below). The license must contain access limitations. The foreign national employee must also possess a Limited Access Authorization (LAA) at the appropriate level, issued in compliance with DoD Regulation 5200.2-R and the NISPOM, before classified information may be disclosed to the employee. The LAA must be consistent with the terms of the license. Visits by foreign national employees of defense contractors to DoD Components or to other DoD contractor facilities do not require the submission of a visit request through FVS channels. The visit request is to be processed following the procedures for industry visits described in Chapter 6 of the NISPOM. The employing contractor is responsible for providing a copy of the license or the LAA to the designated disclosure official or security office, as appropriate, at the facility to be visited, prior to the visit.

M. TECHNOLOGY CONTROL PLAN.

1. Background.

a. The requirements for the Technology Control Plan (TCP) are set forth in Sections 10-509 and 2-307 of the NISPOM and Part 126.13 of the ITAR. The original purpose for the TCP was to require cleared contractor facilities to develop specific access and physical control procedures to control access to classified information and programs by foreign national employees and visitors assigned to the facility similar to the procedures required for DoD Components in DoD Directive 5230.20. This requirement is described in Section 10-509 of the NISPOM. In an attempt to remind cleared contractors of the requirement to expedite decisions on export license applications related to the hiring of foreign nationals and long-term plant visits by foreign nationals, the requirement specified in the NISPOM was included in Part 126.13 of the ITAR. With respect to this requirement for the TCP, the DSS may grant an exception regarding the preparation of a specific "TCP" if the facility has in place other security documentation (such as a Standard Practices Procedures (SPP) document) that adequately covers the specific components of a TCP.

b. Section 2-307 of the NISPOM requires a TCP in all situations when facilities are cleared under certain Foreign Ownership, Control or Influence (FOCI) arrangements. In such cases, it is presumed there is a significant risk of unauthorized or inadvertent access by foreign nationals because of the FOCI circumstances. Therefore, a specific TCP is mandatory even though the facility may have in place a SPP or other similar security document that implements the NISPOM. When a SPP or other security document adequately covers controls for classified information and programs, the TCP may be limited to unclassified export controlled information, including that related to dual-use terms controlled by the EAR. However, the documents should cross-reference each other.

2. Preparation Guidance.

a. The purpose of a TCP is to describe specific procedures covering how access to CMI, CUI, and other official DoD information not authorized for export or disclosure will be controlled in circumstances when foreign nationals are located at security cleared contractor facilities as visitors or employees, or there is a FOCI situation. The TCP must cover the requirements of export control laws and regulations, the NISPOM, classified contracts and, in the case of a FOCI situation, the provisions of the facility clearance arrangement. Foreign Nationals who are "protected individuals" and aliens lawfully admitted to the United States for permanent residence may be given access to unclassified export controlled information pursuant to the ITAR and EAR. However, the TCP must still address such persons since they are not eligible for access to classified information (except in limited circumstances pursuant to a LAA which has been approved pursuant to DoD Regulation 5200.2-R and the NISPOM. Additionally, their access to CUI or other export controlled information may be restricted by law, executive order, or contract. In the case of an LAA, access will be

restricted to specified classified information and limited to a specified government program or project; therefore, access to other information must be controlled.

b. It is not necessary or desirable to repeat the requirements stated in the NISPOM or the export control regulations except where necessary to emphasize a particular requirement. The facility security and export control officials must be thoroughly familiar with the specific security and export control requirements, and it is they, in the first instance, who are responsible for monitoring enforcement. However, they should not be designated to oversee the daily activities of the foreign national; that responsibility should be assigned to a supervisor in the location where the foreign national is employed or assigned.

c. It is not necessary to prepare a TCP for each foreign national visitor or employee, unless there are differences in authorized access to areas and/or information. Access authorizations and restrictions for individual situations can be prepared and appended to a single, generic TCP or SPP.

d. Even if a facility's internal security procedures documentation (e.g., SPP) might fully cover the requirements addressed in a TCP, and DSS determines a separate TCP is not necessary, it would be preferable that the TCP requirements be included in a separate annex to the SPP or other document. In this manner, the guidance can be removed, merged with guidelines on information access authorizations and restrictions, and provided to the foreign national visitor or employee and coworkers. This facilitates compliance with the ITAR provision dealing with the submission of a copy of the TCP with requests for licenses for foreign national visitors and employees by cleared companies.

e. The TCP should, at a minimum, identify the key facility management officials responsible for export control and security (e.g., the empowered official, the facility security officer, the official on a board of directors designated to monitor contacts with the parent company in a FOCI situation) procedures within the facility. This facility official is responsible for overseeing the activities of the foreign national(s), identifying programs or contracts and related information to which access is permitted, controlling electronic office equipment (e.g. computers, reproduction, telefaxes, secure telephones), adopting a means to identify the person as a foreign national, and putting in place physical access controls.

f. The TCP guidance and the information access authorizations and restrictions must be provided to each foreign national visitor or employee, as well as coworkers, and they must acknowledge the receipt and understanding of the requirements.

N. VISITS BY DOD AND CONTRACTOR EMPLOYEES ABROAD

Many foreign governments require the submission of a visit request for all visits to a government facility, even though classified information may not be involved, and for visits to cleared contractor facilities involving the disclosure or possible disclosure of classified information. They also require the requests be received by a specified number of days in advance of the visit.

See this Handbook's Chapter 9, subsection C.7, and its associated Appendix for lead-times for NATO countries. For many countries, the U.S. visit requests must be translated into the language of the host country. Therefore, the prescribed format must be followed. Sufficient time should be allowed when submitting visit requests to permit not only security clearance verification and processing by the host government, but also for translation of the request by U.S. in-country personnel.

1. DoD Personnel. Official temporary duty (TDY) and other visits by DoD personnel are governed by DoD Directive 4500.54 and the Foreign Clearance Guide (FCG), DoD 4500.54-G.

a. The DoD civilian officials appointed by the President, by and with the advice and consent of the Senate, members of the Joint Chiefs of Staff, and the Vice Chairman of the Joint Chiefs of Staff, must clear their overseas travel plans with the Executive Secretary of the Department of Defense, through the Office of the Under Secretary of Defense (Policy) (OUSD(P)), before plans or arrangements are communicated abroad.

b. The DoD personnel not covered by subparagraph 1.a., above, must obtain a "theater clearance" from the Combatant Command Commander, if required (see subsection 1.c., below) and a "country clearance" from the U.S. Embassy. The FCG describes the procedures for obtaining these clearances. Requests for clearances must include the information outlined in the General Information Booklet of the FCG and in the individual country sections.

c. A theater clearance is always required if the visit is to a U.S. military facility. A theater clearance also may be required to visit a particular country or when the subject of the visit is of direct interest to the Combatant Command Commander, such as force protection requirements for United States citizens in the Command's area of responsibility. A country clearance and host-government approval is required (for classified and unclassified visits) if the visit is to a host-government organization or to a contractor facility where classified information might be discussed. In such case, the prescribed country clearance message also serves as the visit request, and the message subject should so specify (i.e., subject: Request for Country Clearance/Visit Authorization). Special care must be given to the requirements of the FCG concerning personnel clearances and host-government visitor security requirements. If the FCG is not clear in this respect, contact the applicable U.S. Defense Attaché Office (DAO) or Office of Defense Cooperation (ODC) for additional information on host-government requirements.

d. When travel of DoD persons will involve the disclosure or presentation of CMI, the request for travel orders will contain a statement that the appropriate disclosure authorization has been approved in compliance with DoD Directives 5230.11 and C-5230.23 *(reference r)*. If the travelers must carry classified material, the request for travel orders also must state that they are aware of and will comply with the requirements to protect CMI as described in DoD Regulation 5200.1-R. There also must be a certification that export controlled information has been approved for release. If the traveler is expected to have access to foreign government classified information, additional certification may be required by the FCG.

2. Contractor Personnel. Contractors must follow the procedures in Chapter 9, subsection C.7, and it's associated Appendix for proposed visits to foreign government organizations and foreign contractor facilities. An export authorization must be obtained if export controlled technical data is to be disclosed or if information to be divulged is related to a classified U.S. government program. An export authorization is not required if the disclosure of the information is covered by an exemption to the ITAR.

a. Routing. The visit request is forwarded to the Defense Industrial Security Clearance Office (DISCO) which will verify clearances and add the security assurance. They will then forward the visit request to the in-country U.S. Government office designated to coordinate the visit with appropriate foreign government officials, normally the ODC.

b. Request Format. Visit requests must contain all of the information specified in Chapter 9, subsection C.7., and it's associated Appendix. Incomplete visit requests and those not adequately justified place an additional burden on the DISCO and U.S. in-country staffs, who must translate each request and make the arrangements. Incomplete requests may be returned without further action. If the visit is initiated at the invitation of an official of the foreign government or the contractor to be visited, the request must contain the full name, grade and/or position, organization, address, and telephone number of the person who extended the invitation. The invitation may not be valid, however, if the host for the visit has not coordinated the visit in advance with appropriate government authorities who are required to approve the visit. It is the visitor's responsibility to ensure such coordination has occurred.

c. The DoD Component Programs. When contractor employees are to visit foreign government facilities or foreign contractors on government orders in support of a DoD Component contract or program, a visit request is also required. The visit request and certification of clearances may be processed by the DoD Component following IVP procedures.

O. ASSIGNMENTS OF FOREIGN NATIONALS

1. International Agreement. Assignments of foreign nationals to a DoD Component facility require the negotiation of an international agreement pursuant to DoD Directive 5530.3, except as noted in section B.4. The agreement establishes the terms of the assignment and the responsibilities and liabilities of the governments and the assignees. The extended visit authorization is used to assign each person to a position and obtain the necessary biographical data and security assurance on the assignee.

2. General Limitations on Assignments. All foreign nationals assigned to a DoD Component or a DoD contractor facility shall be subject to the limitations described below. DPEP assignments are subject to additional limitations described in section Q below.

a. They may have access only to CMI and CUI that is authorized for disclosure to their government or organization. Access shall be further limited to the specific information necessary to perform the duties associated with the position to which they are assigned, subject to a favorable foreign disclosure decision respecting their government or international organization.

b. They shall not have permanent custody of CMI or CUI. They may be permitted use of a storage container to secure CMI or CUI that is approved for their use. However, security officials of the DoD Component or contractor facility shall retain overall control of the container and its contents.

c. They shall not have unsupervised access to libraries, operations centers or other areas where CMI or CUI is stored or used. These areas include catalogues and reference lists containing references to classified documents, unless all information available within the spaces or documents is approved for disclosure to their government or international organization or access controls are established to preclude unauthorized access.

d. They shall not remove CMI or CUI from the premises except when acting as a courier for their government or organization, upon a written request from their government or organization. They shall not act as a courier of classified information for the DoD Component.

e. They shall wear their uniform if they are military personnel, or, if civilian, appropriate civilian attire.

f. They shall wear, in clear view, a distinctive building or installation badge that clearly identifies them as foreign nationals. Their access to DoD work areas is during established DoD duty hours for the installation or if they are accompanied by DoD personnel after duty hours.

g. Other identification (including organizational code, title, signature block, office nameplate, business cards, name tags, or email address) used by or issued to foreign nationals shall clearly identify the person's status as a foreign national. In order to avoid misunderstandings about their status, abbreviations will not used for this purpose.

h. If there are areas of an installation or facility that are normally access-restricted, foreign nationals may also be issued a vehicle pass that clearly identifies their vehicle as belonging to a foreign national.

3. General Limitations on Access. Assignees shall not have access to:

a. Information to which access is prohibited by law.

b. RESTRICTED DATA and FORMERLY RESTRICTED DATA as defined in the Atomic Energy Act of 1954 (*Reference f*).

c. Naval Nuclear propulsion information, except pursuant to an agreement negotiated pursuant to Reference (f) above.

d. Security vulnerabilities pertaining to DoD Automated Information Systems.

e. Communications security (COMSEC) and signals intelligence (SIGINT) information, unless authorized by a separate government-to-government agreement.

f. Classified Information or CUI provided by another government or international organization or by another DoD or U. S. Government department or agency, unless access is approved in writing by the originating government, international organization, or department or agency.

g. National intelligence and sensitive compartmented information, unless specifically authorized by a separate government-to-government Agreement.

h. Information bearing a special handling notice that restricts access, except when authorized by the originator.

i. Any CMI and CUI or other official U.S. Government unclassified information that would not be authorized for disclosure to the foreign national's government or international organization.

j. Classified and unclassified operational tactics, techniques, and procedures which are unique to U.S. military forces, and related training, unless approved by the responsible DoD Component.

k. Proprietary information the rights to which are owned by private firms or citizens (e.g., patents, copyrights, trade secrets) without the owner's consent, unless access is permitted by legislation and then only pursuant to the legislation.

P. FOREIGN LIAISON OFFICERS.

1. Foreign Liaison Officers who conduct business with DoD represent the sponsoring government for the purpose of exchanging information on programs of mutual interest. They are not to be used as a member of the DoD Component's work force. The purpose of the FLOs' assignment must be described in the pertinent certification and the related DDL. They may have access only to information, classified or unclassified, authorized for release to their government as described in the DDL. FLOs may assume custody of documentary information for transfer to their government only when they are authorized in writing by their government to serve as a courier and they have the necessary courier orders and the necessary documentation required by carrier and port security authorities and Immigration and Customs authorities. FLOs physically located at a DoD facility may have temporary on-site custody of classified information when necessary to participate in joint or combined activities. They will sign a receipt for all

documentary classified information. They are subject to all of the restrictions described in section O, above.

2. FLOs will be certified to the DoD Components in compliance with DoD Directive 5230.20 certification procedures. If a FLO is to be physically located at a DoD facility, the terms of the assignment will be set forth in an international agreement.

3. The DoD will not certify FLOs for assignment to U.S. defense contractor facilities unless prior arrangement for security oversight has been coordinated with the contractor and DSS and security responsibility has been agreed upon. U.S. defense contractors must obtain an export license for such assignments under the provisions of the ITAR and comply with the NISPOM.

Q. DEFENSE PERSONNEL EXCHANGE PROGRAM

1. The exchange of personnel between the U.S. Military Services and counterpart services of friendly foreign governments has been occurring under various agreements since World War II. Typically each party provides, on a reciprocal basis, assignments to established manpower positions within its force structure for military personnel of the other party. Similar agreements have been negotiated for the reciprocal exchange of defense establishment civilians such as intelligence analysts, scientists and engineers, medical personnel, and administrative and planning specialists. These exchange programs constitute the DPEP. DPEPs are authorized by P.L. 104-210, Section 1082.

2. Pursuant to the law, a DPEP is established by an international agreement negotiated pursuant to DoD Directive 5530.3. Exchange personnel are assigned to positions within and perform functions for the organization to which they are assigned. However, they are not DoD employees; they are representatives of a foreign government. For this reason, the law places strict limitations on the use of such personnel, and Congress insisted that the Department adopt other controls. Thus, they cannot be fully integrated into DoD operations. The signing of a Statement of Understanding or any form of non-disclosure statement does not mitigate this restriction. These facts must be taken into consideration when considering the establishment of DPEP positions. The below listed restrictions apply to the DPEP and the personnel assigned to the positions.

a. Legal Restrictions.

(1) The establishment of a DPEP arrangement with another government requires the negotiation of an international agreement which provides for the exchange of personnel of essentially the same qualifications, training, and skills.

(2) Foreign exchange personnel shall not be assigned to positions requiring them to act in an official capacity for DoD.

(3) The DPEP shall not be used to train foreign exchange personnel.

b. Policy Restrictions.

(1) They shall not be assigned to command or other positions requiring them to exercise responsibilities reserved by law or regulation to an official of the U. S. Government.

(2) They shall not be used as an intermediary to facilitate requests and exchanges of technical data or other controlled information between the governments. This is the responsibility of FLOs.

(3) They shall not act in the dual capacity as a DPEP participant and as a FLO for their government.

(4) They shall not be assigned to positions or to locations that could result in their gaining access to CMI, CUI or other official information not authorized for disclosure to their government.

(5) Procedures must be developed to preclude their inadvertent or unauthorized access to CMI and CUI not authorized for release to their government.

(6) They shall not be assigned to DoD contractor facilities.

(7) They shall not be given any security responsibilities (e.g., escort duties, document custodian, security checks, etc.).

(8) They shall not have permanent custody of CMI or CUI. They may have supervised access to materials authorized for disclosure during normal duty hours at the place of assignment. They may not have unsupervised access to libraries or document catalogs unless the information therein is releasable to the public.

(9) They shall not have access to restricted areas where they might gain unauthorized access to the information types of information described in section O, above.

3. Each DPEP position requires a position description and a DDL. The host activity supervisor of the prospective participant, in coordination with Component disclosure officials, prepares the DDL based on the position description. The position description and DDL must accompany the request to establish a DPEP position. The Office of the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (DUSD (TSP&NDP) approves the DDL for the OSD, the Office of the Joint Chiefs of Staff and Defense Agency positions. A Principal or Designated Disclosure Authority of each Military Department approves departmental requests. The DDL must cover the information elements listed in DoD Directive 5230.20.

4. A contact officer or other person designated to supervise the DPEP participant is responsible for:

a. Ensuring the participant understands the duties he or she is to perform in the assigned position;

b. Ensuring the participant only has access to CMI and CUI necessary to fulfill the duties of the position as described in the DDL, or as otherwise authorized in writing by the originator;

c. Ensuring coworkers are knowledgeable about the limitations on access to information by the exchange participant and their responsibilities in dealing with the individual; and

d. Informing the participant of his or her rights, responsibilities and obligations.

5. DPEP assignees must sign a statement of Understanding of Conditions and Responsibilities similar to that contained in DoD Directive 5230.20 before being assigned to the host DoD Component. If the assignment will involve access to technical data, the participant must also sign a certification governing the rights of the individual and DoD on inventions and rights in property. The DoD persons participating in this program in a foreign country may also be required to sign these certificates.

R. COOPERATIVE PROGRAM PERSONNEL

Foreign nationals participating in a Cooperative Arms Program may be assigned to a program office located in the United States as a representative of their government. An international agreement is required to establish the cooperative program. The program agreement alone is not sufficient to establish the terms and conditions of a CPP assignment. The agreement for the assignment of the foreign government personnel to a DoD organization must contain provisions similar to those in a FLO or DPEP agreement. The provisions may be placed in an Annex to the program cooperative agreement or in a separate agreement.

S. VISITS BY FOREIGN NATIONALS AT CLASSIFIED MEETINGS AUTHORIZED BY THE DEPARTMENT OF DEFENSE

1. The DoD policy on the conduct of classified conferences, seminars and other similar gatherings (hereafter referred to as meetings) is contained in DoD Regulation 5200.1-R. Foreign attendance at meetings that may lead to contract opportunities for contractors from countries with which DoD has signed reciprocal procurement arrangements should be considered during the planning for the meetings. The DoD policy and procedures concerning meetings in which classified information will be disclosed are summarized below. DoD Regulation 5200.1-R must be consulted for other requirements.

a. The number of classified meetings must be limited and those that are authorized must be for a lawful and authorized DoD purpose. They will be authorized only when the Head of the DoD Component authorizing the meeting, or designee, determines the following in writing:

(1) The conduct of the classified meeting serves a specified U.S. government purpose;

(2) The use of other prescribed channels for dissemination of classified information does not accomplish the purpose;

(3) The location selected for the meeting is under the security control of a U.S. government agency or a U.S. contractor having an appropriate facility security clearance;

(4) Adequate security procedures have been developed and can be implemented.

b. The conduct of a classified meeting must be authorized by the Head of a DoD Component that has principal interest (normally classification jurisdiction) in the subject matter of the meeting. Responsibility for authorizing meetings involving foreign participation will be delegated only as follows:

(1) To a person serving in a position at or above the level of Deputy Assistant Secretary or equivalent for the OSD;

(2) The senior security official in the Military Departments;

(3) The Director of the Joint Staff, Office of the Joint Chiefs of Staff; or

(4) The Directors of Defense Agencies.

c. The Heads of DoD Components, or their designees, may authorize the organization of and administrative support to classified meetings by non-government organizations, provided the meeting is in support of a lawful and authorized government purpose. However, the authorizing official must retain full responsibility for all security aspects of the classified meeting to include decisions on foreign attendance and classified information to be presented.

d. Classified presentations must be segregated from unclassified presentations to the maximum extent practicable to allow for appropriate foreign attendance and security control.

2. Announcements of classified meetings must be unclassified and must be limited to a general description of topics expected to be presented and administrative instructions for requesting invitations or participation.

3. If foreign nationals are to be invited to a classified meeting, invitations will be approved in advance and sent to the invitees by the DoD Component authorizing the conduct of the meeting. The invitation should be sent through the applicable foreign embassy(ies) in the U.S. or the applicable U.S. Embassy(ies) overseas. The invitation must require each foreign government provide identification of its representatives and security assurances in accordance with prescribed visit request procedures.

4. Classified information to be presented at the meeting must be authorized for disclosure in advance by a Principal or Designated Disclosure Authority of the DoD Component having classification jurisdiction over the information involved. Each U.S. government and U.S. contractor employee must provide a written assurance that their presentation has been cleared for foreign disclosure in compliance with DoD Directive 5230.11. The written assurance will be provided to the DoD Component representative designated to manage the security aspects of the meeting(s). This requirement may be satisfied for U.S. contractors by a valid export license.

5. Classified presentations will be delivered orally and/or visually. Classified documents are not to be distributed and classified note-taking and electronic recordings normally will not be permitted by attendees. Exceptions to the latter policy may be granted for special purposes provided arrangements are made for securing the material after hours and subsequent transmission to the participants through government channels. The transfer of classified documentation to foreign participants is to be in accordance with Chapter 6, of this Handbook.