CHAPTER 7

VISITS AND PERSONNEL EXCHANGES

A. INTRODUCTION

1. The U.S. Government and most foreign governments have established specific requirements and procedures to control visits and assignments of foreign nationals to their government organizations and cleared contractor facilities. In order to control visits by foreign nationals to Department of Defense (DoD) facilities and cleared contractor facilities, DoD has established the International Visits Program (IVP), the Foreign Liaison Officer (FLO) Program, the Defense Personnel Exchange Program (DPEP) and the Cooperative Program Personnel (CPP) Program. This chapter describes the policy and procedures for those programs and requirements for international visits by DoD personnel. The visit request process is used to approve visits by foreign nationals to DoD organizations and cleared defense contractor facilities and to assign foreign nationals to DoD organizations under the FLO, DPEP, and CPP programs. In this context it covers the types of international visits and the process for requesting and approving the visits.

2. The visit request process serves several important purposes. The primary purpose is that it provides a means for consideration of proposed export or disclosure decisions related to the visit. In this connection, it is the means for the requesting government to provide security assurances on the visitors, and on their firms, if appropriate, and authorize the visitor to receive Classified Military Information (CMI) on its behalf. It also serves to facilitate administrative arrangements associated with the visit.

B. POLICY

1. When a visit authorization is required, the request must contain the information described in Appendix P. Failure to provide the required information in the appropriate format may result in the request being denied. The government-to-government principle applies to access to classified and controlled unclassified information during visits. Therefore, visits by foreign nationals, including foreign contractors, to DoD and defense contractor facilities that will involve U.S. or foreign government classified or controlled unclassified information must be requested through government channels and the requesting government must provide a security assurance on the visitors.

2. Classified information is not to be disclosed to a foreign visitor (including liaison officers and exchange personnel) unless the appropriate principal or designated disclosure authority has authorized the disclosure and has received a security assurance from the foreign visitor's

government. Classified documents may not be released to liaison officers or other foreign visitors unless the terms of certification or visit authorization specifically state the individual may assume custody on behalf of the foreign government and the visitor has the necessary courier documentation (see Chapter 6 and Subsections I.1. and M.4, below). A receipt must be obtained for all classified information provided to a foreign representative, regardless of its classification level. (Note - Foreign governments may waive this requirement for their RESTRICTED information.)

3. DoD Components and defense contractors must establish procedures to monitor international visits or assignments of foreign nationals to their facilities to ensure the disclosure of and access to export controlled articles and related information are limited to those approved by an export authorization or exemption or, in the case of DoD components, a delegation of disclosure authority.

4. DoD visit authorizations are not to be used by defense contractors to employ or otherwise acquire the services of foreign nationals that require access to classified or other export controlled information or to support the assignment of foreign nationals to contractor facilities under a commercial contract (e.g., quality control personnel). An export license is required for such situations.

5. A contact officer will be appointed to control the activities of all foreign nationals assigned to DoD Components as exchange officers, liaison officers, or other on-site or long term visit or assignment. Contractors must adopt similar procedures, using a Technology Control Plan (see section P. below).

6. The Defense Intelligence Agency (DIA) administers requests for visits by foreign nationals to the Office of the Secretary of Defense, the Joint Staff, and the DoD Agencies, and their contractors. These DoD Components must ensure they obtain disclosure authorization from the appropriate DoD Principal (PDA) or Designated Disclosure Authority (DDA) prior to notifying DIA of the acceptance of a visit by foreign nationals.

C. TYPES OF VISITS

DoD policy identifies three types of visits:

1. **One-Time Visits**. A visit for a single short-term occasion (normally less than 30 days) for a specified purpose.

2. **Extended Visits**. A single visit for an extended period of time, normally up to one year. (Note: Many governments only have two categories of visits, one-time and recurring, and refer to an extended visit as a one-time, long-term visit.) Extended visits usually support one of the following situations:

a. A government contract or joint program (e.g., joint venture, representative to a joint or multinational program);

b. Participation in an exchange program under the Defense Personnel Exchange Program (DPEP);

c. Training, except for those individuals on invitational travel orders; or

d. Liaison officers to a DoD component.

3. **Recurring Visits**. Intermittent, recurring visits over a specified period of time, normally up to one year in duration. These visits usually are in support of a government approved agreement, contract or license when the information to be released has been defined and approved for release by the applicable government disclosure authority. By agreement of the governments, the term of authorization may be for the duration of the agreement, contract, or license subject to annual review and validation.

4. **Emergency Visits**. 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 and ensure that the complete name, grade, or position, address and telephone number of the person and a knowledgeable foreign government point of contact are provided in the visit request, along with the identification of the contract, agreement or program and the justification for submission of the emergency visit request.

D. INTERNATIONAL VISITS PROGRAM

1. The Department of Defense established the International Visits Program (IVP) (see DoD Directive 5230.20) *(reference ff)* to control and facilitate visits by foreign individuals to the DoD Components and cleared defense contractors. It also covers visits by DoD personnel and U.S. cleared defense contractors to foreign countries.

2. The Foreign Visit System (FVS) is the automated system for processing requests for visits by foreign nationals to DoD Components and cleared defense contractor facilities that are received from foreign governments. FVS permits the participating government, through its embassy, to create visit requests in an established format on a personal computer (PC) and submit them via a dial-up connection to the FVS communications processor in the Pentagon. The requests are then sent to the FVS central processor which distributes them to one of four Defense Visit Offices (DVO) located in Army, Navy, Air Force and DIA (See Appendix F). The DVOs provide a

staffing scheme that identifies the appropriate DoD and commercial facilities with which the request is to be staffed. Upon completion of staffing, the DVO renders a decision that is returned to the submitting embassy or organization over the same electronic path used for submission of the request. The FVS has halved the processing time for routine requests and has eliminated the need to handle over two million pieces of paper each year. Foreign embassies that are 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 a manual that contains instructions for submission of visit requests under the FVS including assignments under the FLO, DPEP, and CPP Programs.

E. FOREIGN 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. Amendments to visit requests are not authorized except to change dates or names of visitors. If other information is to be changed, a new visit request must be submitted. Emergency visit requests and 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 visit. 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. 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 courier orders and identification. 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 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.

F. HOSTED VISITS TO DOD FACILITIES

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 if the DoD official who extends the invitation notifies the DVO which will 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. Designated disclosure officials also must authorize the release of the appropriate information prior to the invitation being extended.

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

1. All visits involving a NATO Command or Agency or the NATO International Staff, including U.S. citizens (military and civilian) assigned to NATO, that involve access to NATO information or U.S. classified information will be processed in the FVS under the International Visits Program in compliance with the National Industrial Security Program Operating Manual (NISPOM) *(reference y)* and DoD Directive 5230.20 (reference ff).

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

H. VISITS FOR FOREIGN PARTICIPATION IN CLASSIFIED MEETINGS AUTHORIZED BY THE DEPARTMENT OF DEFENSE

1. Department of Defense policy on the conduct of classified conferences, seminars and other similar gatherings (hereafter referred to as meetings) is contained in DoD 5200.1-R (*reference j*) . Foreign attendance at meetings that may lead to contract opportunities for foreign contractors should be considered during the planning for the meetings. Department of Defense policy and procedures concerning meetings in which classified information will be disclosed are summarized below. DoD 5200.1-R must be consulted for other requirements.

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

(1) 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 Offices of the Secretary of Defense (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 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 be sent to the invitees by the DoD Component that authorizes the conduct of the meeting. The invitation should be sent through the applicable foreign embassy(ies) in the United States 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 *(reference dd)*. 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.

I. LIAISON OFFICERS

1. Liaison officers are representatives of the sponsoring government. They are not to be used as a member of the DoD Component's work force. They may, however, participate in the activities of the organization to which assigned when the assignment is in support of a joint program agreement. Such participation must be described in the pertinent certification or agreement, as applicable, and the related DDL. They may have access only to information, classified or unclassified, that has been authorized for release to their government as described in the DDL. Liaison officers 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. Liaison officers who are 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.

2. Liaison officers will be certified to the DoD components in compliance with DoD Directive 5230.20 (*reference ff*) certification procedures. If a liaison officer is to be physically located at a DoD facility, the terms of the assignment will be set forth in an international agreement that is in compliance with DoD Directive 5530.3 *(reference cc)*. Security Assistance Liaison Officers (i.e., those assigned pursuant to an FMS case) may be assigned under the terms of an agreement or a LOA, which must contain the same terms as an agreement.

3. The DoD will not certify liaison officers 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 International Traffic in Arms Regulations (ITAR) *(reference c)* and comply with the NISPOM.

J. 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. All such exchange programs constitute the Defense Personnel Exchange Program (DPEP). These programs are authorized by law; and the law requires the Secretary of Defense to submit an annual report to Congress on the status of foreign exchange officer assignments to DoD organizations.

2. Personnel exchange programs are established by an international agreement negotiated pursuant to DoD Directive 5530.3 (*reference cc*). Exchange personnel are assigned to positions within and perform functions for the organization to which they are assigned. They do not represent their government, as is the case with liaison officers. However, they are still foreign nationals. This fact must be taken into consideration when considering the establishment of exchange officer positions. The below listed limitations apply to personnel exchange programs and the personnel assigned to exchange positions. Exceptions to these limitations will not be authorized.

a. Procedures must be developed to preclude their inadvertent or unauthorized access to CMI and Controlled Unclassified Information (CUI) that has not been authorized for release to their government.

b. Exchange positions will not be used for training or as a substitute for, or in combination with, the functions of a Foreign Liaison Officer.

c. Participants will not be used as a conduit for exchanging technical data or other controlled information between governments. Other agreements are designed for this purpose.

d. Participants will not be assigned to positions giving them access to information not authorized for release to their government or to areas (e.g., libraries, restricted areas) where they might gain access to such information..

e. Participants will not be assigned to DoD contractor facilities.

f. Participants will not be given any security responsibilities (e.g., escort duties, document custodian, security checks, etc.).

g. Participants will 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.

h. Participants will not have access to restricted areas or to the following types of information:

(1) RESTRICTED DATA (RD) or FORMERLY RESTRICTED DATA (FRD);

(2) Information systems security information unless there is a current agreement with the participant's government that permits access;

(3) CMI or CUI provided by another government, unless access is approved in advance, in writing, by the originating government;

(4) Compartmented information, unless authorized by a current agreement with the participant’s government;

(5) Information bearing a special handling notice restricting access, except when authorized in advance by the originator; and

(6) Any U.S. CMI not previously authorized for release to the participant's government by the responsible designated disclosure authority of the originating Component or Agency.

2. Each DPEP position requires a position description and a DDL or equivalent document that provides disclosure guidance. 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 and National Disclosure Policy approves the DDL for 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 categories listed in enclosure 5 of DoD Directive 5230.20 (*reference ff*).

3. 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.

4. DPEP participants must sign a certificate of conditions and responsibilities similar to that contained in enclosure 6 of DoD Directive 5230.20 (*reference ff*) 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 the Department of Defense on inventions and rights in property. U.S. persons participating in this program in a foreign country may also be required to sign these certificates.

K. COOPERATIVE PROGRAM REPRESENTATIVES

Such foreign personnel may be assigned to a program office located in the United States as a representative of their government. An international agreement is required. The program agreement is not sufficient. The agreement for the assignment of the foreign personnel to a DoD organization must contain provisions similar to those in a liaison officer of DPEP agreements. The provision may be placed in an Annex to the international agreement.

L. CONTROL OF ACCESS TO DEFENSE FACILITIES BY FOREIGN NATIONALS

Foreign nationals, including exchange personnel, attaches and liaison officers may not have uncontrolled access to DoD 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.

M. VISITS BY FOREIGN NATIONALS TO CLEARED DEFENSE CONTRACTOR FACILITIES

DoD visit authorizations are not necessary for foreign national visits to DoD contractor facilities, provided they involve access only to unclassified information, and the information has been authorized for export in compliance with the International Traffic in Arms Regulations (ITAR) (*reference c*) or the Export Administration Regulations (EAR) (*reference e*), or it is in the public domain; a pertinent government contract does not require a government approved visit authorization; and provided the visit will have no impact on DoD activities or responsibilities at the facility. It is the contractor's responsibility to ensure an export authorization is obtained, if applicable. Requests for visits to defense contractor facilities by foreign nationals involving the disclosure of or access to classified information *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 subsections 1 through 3, below, the DoD Component may approve or deny the request, or decline to render a decision. However, if classified information 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.

1. **Visit Approvals**. Visit requests approved by DoD constitute an exemption to the export licensing provisions of part 125.5 of the ITAR when the technical data authorized for disclosure is fully described. If the technical data is not fully described, the contractor to be visited must obtain an export license. DoD approved visits are not to be used to avoid the export licensing requirements for commercial programs. Therefore, 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., program involving a U.S. Government agency and the intended recipient foreign government such as government 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, and 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.

2. **Visit Denials**. 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.

3. **Visit Non-Sponsorship**. 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, and, if classified information is involved, has been notified by the DoD Component that the requesting foreign government has provided the required security assurances on the proposed visitors. 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.

4. **Access by Foreign Visitors to Classified Information**. Contractors are to establish procedures to ensure foreign visitors are not afforded access to classified information 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.

5. **Visitor Records**. Records shall be maintained for all visits involving classified information. The records shall clearly identify foreign national visitors. Pursuant to the ITAR, the visit authorization constitutes an export authorization and therefore the records are to be maintained for five years in compliance with Part 122.5 of the ITAR.

6. **Visits to Subsidiaries**. A visit request 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 concurs.

N. EXTENDED VISITS TO CLEARED CONTRACTOR FACILITIES

Extended visits by foreign nationals to U.S. contractor facilities require written permission from the DoD component having jurisdiction over the information involved. A license or letter application must justify the requirements for the extended visit and include a Technology Control Plan (TCP) in accordance with the NISPOM. As described in subsection L. above, a visit request will be necessary only when the visit is in support of a DoD program or it is

necessary to pass the security assurances. Access to classified information by such personnel is to be in compliance with the NISPOM.

O. FOREIGN NATIONAL EMPLOYEES OF DOD CONTRACTORS

Foreign nationals may not be hired for positions requiring access to classified information except under unique circumstances described in 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. The license should contain access limitations. The foreign national employee must also possess a Limited Access Authorization (LAA) at the appropriate level, issued in compliance with DoD 5200.2-R *(reference jjj)* 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.

P. TECHNOLOGY CONTROL PLAN (TCP)

1. **Background.**

a. The requirements for the Technology Control Plan (TCP) are set forth in Sections 10-509 and 2-310 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 measures to control access to classified information and programs by foreign national employees and visitors 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 Defense Security Service (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 2-310 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 that 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 Export Administration Regulation. 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 classified and controlled unclassified information 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. Even though foreign nationals who are "protected individuals" may be given access to unclassified export controlled information pursuant to the International Traffic in Arms Regulations (ITAR) (reference c) and Export Administration Regulations (EAR) (reference u), the TCP must still address such persons since they are not eligible for access to classified information (except in limited circumstances pursuant to a Limited Access Authorization (LAA) which has been approved pursuant to DoD 5200.2-R and the NISPOM). In such cases, access under the LAA 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 that are 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.

c. It is not necessary to prepare a TCP for each foreign national visitor or employee. 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 that are to be addressed in a TCP, and DSS determines that 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 so that 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 also will facilitate 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 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 their receipt and understanding of the requirements.

Q. VISITS BY U.S. PERSONS TRAVELING 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 Chapter 9, subsection B.6, 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 and 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 personnel are governed by DoD Directive 4500.54 *(reference pp)* and the Foreign Clearance Guide, DoD Directive 4500.54-G *(reference kkk)*.

a. 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 OUSD(P), before plans or arrangements are communicated abroad.

b. DoD personnel not covered by subparagraph 1.a., above, must obtain a "theater clearance" from the Combatant Command Commander, if required (see subparagraph 1.c., below) and a "country clearance" from the U.S. Embassy. The Foreign Clearance Guide (formerly the U.S. Air Force Clearance Guide) describes the procedures for obtaining these clearances. Requests for clearances must include the information outlined in the General Information Booklet of the Foreign Clearance Guide 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. 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 Foreign Clearance Guide concerning personnel clearances and host-government visitor security requirements. If the Foreign Clearance Guide is not clear in this respect, contact the

applicable U.S. Defense Attaché Office or Office of Defense Cooperation 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 (*reference dd*) 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 5200.1-R *(reference j)*. 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 Foreign Clearance Guide.

2. **Contractor Personnel**. Contractors must follow the procedures in Chapter 9, Subsection B.6, and its 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, unless the disclosure of the information is covered by an exemption to the ITAR.

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

b. **Request Format**. Visit requests must contain all of the information specified in Chapter 9, Subsection B.6., and its 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 that such coordination has occurred.

c. **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 its visit procedures.