

CHAPTER 11

CONTRACTOR OPERATIONS ABROAD

A. INTRODUCTION

This Chapter sets forth requirements governing contractor operations abroad, including security clearances for U.S. contractor employees assigned outside the United States and their access to classified information. Although this Chapter applies primarily to contractors, U.S. Government employees overseas can also be involved, primarily in the role of receiving, storing, and maintaining custody and control of classified information for U.S. contractor personnel, or approving contractor requests for assistance.

B. ACCESS, STORAGE, CUSTODY, CONTROL AND TRANSMISSION OF CLASSIFIED INFORMATION

1. **Access.** Contractor employees assigned outside the United States may have access to classified information and, therefore possess a security clearance, only in connection with performance on a specified U.S. Government classified contract or a specified foreign government or North Atlantic Treaty Organization (NATO) classified contract, including responses to foreign government and NATO requests for proposal.
 - a. The National Industrial Security Program Operating Manual (NISPOM) (*reference y*) prohibits the assignment of an employee who is a foreign national (including those who are protected individuals) outside the United States on programs that will involve access to classified information. Such an assignment negates the basis on which a Limited Access Authorization (LAA) may have been provided to the employee.
 - b. Consultants, and other persons who are hired to provide similar services, will not be assigned outside the United States with responsibilities that require access to classified information. Such assignments also would negate any clearance held by the consultant.
 - c. For the purpose of this section, "assignment" means a presence in a foreign country under other than a one-time or recurring visit authorization as defined in Chapter 7.

2. **Storage, Custody, and Control.**

a. The storage, custody and control of classified information by U.S. government and U.S. contractor employees abroad are the responsibility of the U.S. Government. Therefore, the storage of classified information by employees at any location abroad that is not under U.S. Government control is prohibited. The storage may be at a U.S. military installation, a U.S. Embassy or Consulate, or other location occupied by a U.S. Government organization that is authorized to store classified information.

b. Contractor employees may be furnished an approved security container to store classified material temporarily at a contracting Department of Defense (DoD) Component's overseas location (e.g., military base) when the material is required for a specific government contract. The decision to permit a contractor to temporarily store classified information abroad must be approved in writing by the senior security official at the DoD Component contracting organization and by the U.S. Government host organization. The contracting organization is responsible for ensuring U.S. Government security requirements are enforced at its overseas location.

c. Contractor employees may be permitted to remove classified information temporarily from a U.S. Government controlled facility abroad when necessary for the performance of a DoD Component contract or pursuant to an approved export authorization. The responsible security official at the U.S. Government facility must verify the contractor has an export authorization or other written U.S. Government approval to have the material; verify the need for the material to be removed from the facility; and brief the employee on handling procedures. In such cases, the contractor employee will sign a receipt for the material and return the material to government custody for storage during non-working hours.

d. Contractor employees will not store classified information at overseas divisions or at subsidiaries of U.S. companies incorporated or located in a foreign country. These divisions or subsidiaries, if cleared under the procedures of the foreign government, may have access to U.S. classified information that has been transferred through government-to-government channels to the applicable foreign government pursuant to an approved export authorization or other written U.S. Government authorization. Access to this classified information at such locations by a U.S. contractor employee assigned abroad by the parent company in support of a foreign government contract or subcontract is governed by the laws and regulations of the country in which the division or subsidiary is registered or incorporated. The division or subsidiary that obtained the information from the foreign government, therefore, will provide the necessary access.

3. **Transmission.** The transmission of classified material to a cleared contractor employee located outside the United States must be through government channels. If the material is to be used for other than U.S. Government purposes, an export license is required and a copy of the authorization must accompany the material. The material must be addressed to a U.S. Government organization (e.g., an embassy or consulate). The U.S. Government organization abroad is responsible for custody and control of the material as described in Subsection B.2., above.

C. SECURITY BRIEFINGS

Contractor employees who are to be assigned outside the United States must be briefed on the security requirements of their assignment, including the handling, disclosure, and storage of classified information and the other requirements of this chapter. If access to North Atlantic Treaty Organization (NATO) information is involved, a NATO briefing is also required (see Chapter 10). The employee is required to sign a certificate as described below. The certificate must be witnessed by the Facility Security Office (FSO) or a designee.

1. The certificate will attest to the following:

- a. The employee has received a security briefing on and understands the requirements of his or her responsibilities for the control, disclosure, and storage of classified information, as well as the nature and extent of the classified information to which the employee requires access and the nature and scope of the threat.
- b. The employee will comply with the prescribed security requirements.
- c. The classified information to which the employee has been granted access will be used only for the purpose for which it is provided.
- d. The employee understands his or her security clearance may be suspended or revoked for violation of security regulations or improper use of classified information.
- e. The employee understands he or she may be subject to action under the espionage laws of the United States or the host nation with respect to the classified information to which access is granted.
- f. The employee also understands upon termination of the purpose for which he or she has been granted access, the employee's responsibilities for safeguarding the classified information continue unabated until the security classification is removed by appropriate government authority.

2. Each employee also will be given an annual refresher briefing. A certificate similar to that described in subsection 1, above, must be executed annually and retained as long as the employee is assigned outside the United States. The briefing may be modified as necessary to reflect any change in the nature and extent of the classified information to which the employee requires access, and the scope and nature of the threat to which the individual may be exposed.

3. Refresher briefings may be accomplished on the temporary return of the employee to the United States, by a security representative of the contractor stationed outside the United States or during visits. A briefing certificate must be executed. When any of the foregoing are not

practical, the briefing and execution of the certificate may be accomplished by a written briefing and execution of the certificate by mail.

D. REPORT OF ASSIGNMENT OUTSIDE THE UNITED STATES

1. Contractors must promptly report cleared employees assigned to a location outside the United States for a period expected to exceed 90 consecutive days to the Defense Industrial Security Clearance Office (DISCO). The report must contain the following information: full name, date and place of birth, social security number and level of clearance;

a. Name address and telephone number and the DISCO overseas code (if known) of the location to which the employee will be assigned. State whether the location is under U.S. Government or foreign government control, and provide the name, title, and telephone number of the U.S. government or foreign government security official at the location;

b. Justification for access to any U.S. or foreign government classified information, to include identification of the contract, license, or agreement under which access is necessary. If access to classified information will not be required outside the United States, provide written justification for retaining the personnel clearance. If the continuation of a security clearance cannot be justified, the DISCO will terminate the clearance;

c. A brief description of access required, including the highest level required; and

d. A certification that the required security briefings have been accomplished and the date accomplished.

2. Subsequent to the assignment of a cleared employee outside the United States, the contractor must provide to the responsible Defense Security Service (DSS) office:

a. Justification, based on a specified contract, license, agreement or other Government approved arrangement, for the employee's continuing need for a security clearance three years from the date of initial assignment and every three years thereafter;

b. Notification of any change in the location and mailing address of the affected employee;

c. Notification of any change of assignment or purpose for access, to include any change to the information in subparagraphs 1.a. through e., above; and

d. Notification of termination of the employee's assignment outside the United States.

3. Contractors will ensure the standard practice procedures (SPP), when required, or a supplement to an existing SPP, is prepared to cover security procedures for their employees assigned outside the United States. The SPP or supplement will identify the location where each

cleared employee is assigned, a description of the duties and contract work involved, the name and telephone number of the responsible on-site security official and all relevant security practices and procedures to be adhered to by the employee. A copy of the SPP must be maintained at the U.S. parent facility. A copy of the SPP prepared to cover security procedures for employees assigned outside the United States will be maintained at the U. S. parent facility and a copy provided to the applicable DSS office.

4. Effective March 31, 2005, DSS closed the last of its overseas offices and ended the on-site industrial security oversight support that it was providing U.S. Government activities around the world. Although DSS will no longer be visiting overseas locations, the local Industrial Security (IS) Representative responsible for oversight of cleared U.S. facilities dispatching cleared employees overseas will be available to provide advice and assistance to contractor organizations and government activities. DoD components overseas will continue to be responsible for providing the day-to-day oversight and management of contractors collocated with and supporting government customers.