Chapter 15 - Special Access

1501 Special Access Programs

Special access programs have been established to impose access controls beyond those normally required for access to information classified as Confidential, Secret, or Top Secret. Under this definition, any classified program requiring additional access controls could be considered a special access program. Such programs may require special clearances, special investigative requirements, special briefings, and/or lists of persons who require access to special programs due to job or organizational requirements. This chapter describes certain special access programs and covers the investigative processing requirements and procedures associated with the granting of access for those programs.

1502 Special Access Program Policies

A. Requisite security investigations must be favorably completed before an individual may be granted access to information covered under one of these programs. General guidance showing the minimum type of security investigation to be conducted for the special access programs covered in this chapter is provided in Appendix E, Obtaining Access to Classified Information, paragraph C, Special Access. Department of Commerce employees who require information on obtaining authorization for access to any other special access program not covered in this chapter or elsewhere in the Security Manual should contact the Office of Security.

B. Immediate supervisors or managers must notify their servicing security officer immediately upon discovery of any information, which indicates that an individual's current involvement in a special access program may not be in the national interest.

C. When access to one of the special access programs is no longer needed, the immediate supervisor or manager must initiate immediate action to administratively withdraw the clearance. In most cases, a termination statement signed by the individual is required. Supervisors or program managers should contact their servicing security officer or the Office of Security for guidance.

D. Employees in special access programs that require a Top Secret security clearance must undergo an SSBI-PR or UDI (depending upon the program) every five years to maintain program eligibility.

E. A special access clearance usually requires a prerequisite departmental security clearance; however, a departmental security clearance will not be issued just for purpose of granting special clearance access.

Rather, a justified "need-to-know" for access to classified information in the Department must be demonstrated prior to requesting or being granted access to a special access program.

F. Access to one of the special access programs may be terminated for administrative reasons unrelated to an adverse security determination. An administrative termination of special access does not prejudice a person's eligibility for future access to a special program. On the other hand, revocation of special access program participation will be administered under the provisions of Chapter 14, Suspension, Revocation, and Denial of Access to National Security Information.

1503 Special Access Program Interagency Agreement

Special access programs may require an interagency Memorandum of Understanding (MOU) establishing the procedures and conditions under which an agency shall provide special access information to the Department. This agreement obligates the Department to maintain effective security control of special access information. Special access programs cannot be established within the Department of Commerce without prior approval.

1504 Sensitive Compartmented Information

Particular categories of classified intelligence information require special security access, special handling, and special storage facilities not covered by procedures for Confidential, Secret, and Top Secret information. Special markings are prescribed in directives, regulations, and instructions relating to Sensitive Compartmented Information (SCI). Agencies within the Intelligence Community have responsibility for maintaining the security control of classified foreign intelligence materials furnished to governmental organizations that are not part of the Intelligence Community, such as the Department of Commerce. These intelligence materials should not be confused with Foreign Government Information (FGI), which is described in Chapter 27.

1505 SCI Program Management

The Department's SCI program is sponsored by the Central Intelligence Agency (CIA) pursuant to a MOU between the Department and the member agencies of the Intelligence Community. The CIA maintains cognizance over the security aspects of departmental approvals for access to, and receipt, handling, storage, and destruction of, foreign intelligence information. Under the MOU, the Department must comply with the directives and regulations which govern access to SCI such as the Director of Central Intelligence Directive (DCID) 1/14. Specific instructions for applying for access to SCI are prescribed in Appendix E, Obtaining Access to Classified Information, paragraph E.2, Access to Classified and Other Programs, and DCID 1/14,

Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information. Within the Department, the Office of Executive Support and the Office of Security have responsibility for administering the SCI program in the various operating units.

1506 Request for Special Access to SCI

A. Requests for access to Sensitive Compartmented Information should be submitted with appropriate justification through the Office of Executive Support to the Office of Security. Such requests shall be submitted prior to the initiation of a background investigation. The Office of Security shall ensure that personnel requiring access to SCI have been afforded appropriate investigations and granted the appropriate security clearance. The CIA will adjudicate the background investigations departmental personnel requesting access to SCI. The Office of Security or designated agency officials in the SCI program will conduct SCI indoctrination of departmental personnel.

B. The requirements for access to Sensitive Compartmented Information include a Top Secret clearance granted by the Department of Commerce, a favorable SSBI completed or updated within the most recent five-year period, specific justification for the special access clearance, and concurrence by the Department's Office of Executive Support. When conditions warrant, additional in-depth investigation shall be conducted on the spouse of the individual and/or on members of the immediate family (or on other persons to whom the individual is bound by either affection or obligation) to the extent necessary to permit an informed determination that the security standards are met. The individual, through his or her servicing security officer, will be notified by the Office of Security prior to the five-year anniversary of the SSBI in order to initiate an SSBI-PR. Special briefings and debriefings are required.

C. An individual denied clearance based on investigation for SCI access may appeal the decision within 45 days of notification of the denial. Procedures for appeal are shown in DCID 1/14. The security contact or servicing security officer should contact the Office of Security for assistance.

D. An SCI Nondisclosure Agreement, Standard Form 4414, will be signed by the employee after receiving an SCI indoctrination. When the need for access is no longer required, an employee will be given a security debriefing and be asked to sign a debriefing acknowledgment. The security debriefing will be required also for separation, transfer, change in duties, suspension, or revocation of access. A copy of the signed Nondisclosure Agreement will be retained in the employee's personnel security file while the original document is forwarded to the CIA.

1507 SCI Security Education

The Office of Security shall administer a continuing security education program for all departmental personnel authorized access to Sensitive Compartmented Information. Under the program, employees with SCI access, shall be reminded of their obligation to properly handle and safeguard SCI materials and of the potential consequences to the U.S. Government of any compromise or unauthorized use of such information. This reminder shall be given to the employee at least annually through an SCI refresher briefing or through another form of instruction.

1508 Travel of Employees with SCI Access

Departmental employees who have been granted access to Sensitive Compartmented Information shall comply with special security requirements established to safeguard such information. The safeguarding requirements for SCI access shall be observed at all times, especially during travel. Each SCI-cleared employee in the Department who has official or unofficial travel to any country must contact the Office of Security to arrange for a defensive security briefing prior to such travel. The Office of Security shall determine the briefing requirement for each specific country visited (see DCID 1/20).

1509 Accreditation of SCI Facilities

SCI material can be maintained only in facilities approved by the CIA for its receipt, storage, and handling. To request establishment and accreditation of a SCI Facility (SCIF), forward a request through the Director, Office of Executive Support to the Office of Security. The request must include the SCI level of accreditation desired, complete address, point of contact, justification, and a description of any automated equipment that will be housed in the area. The Office of Security will then arrange a physical security survey. Recommendations for any security upgrades will be provided to the requester. After implementing the recommendations, a follow-up inspection will be conducted prior to final accreditation. A final accreditation shall be provided in writing to the head of an operating unit and the servicing security officer. The file copy will be maintained in the Office of Security.

1510 North Atlantic Treaty Organization Security Clearance

The **North Atlantic Treaty Organization (NATO**) security clearance is governed by the United States Authority for NATO Affairs (USSAN). Access to NATO classified information requires an equivalent level U.S. security clearance and a special NATO briefing. The request package is the same as that for the equivalent U.S. security clearance except that the Form CD-79 is annotated as described in Appendix E, as

relating to access to NATO classified information. The request package is forwarded through the security contact or the servicing security officer directly to the Office of Security, which will arrange for the appropriate NATO briefing. Prior to being granted access to NATO classified information, the employee must sign a NATO briefing acknowledgment form. A debriefing acknowledgment form is required when the access is terminated. Refer to Chapter 26, Safeguarding North Atlantic Treaty Organization Information, and Chapter 27, Foreign Government Information.

1511 Department of Energy "Q" and "L" Security Clearances

The security clearances labeled **"Q"** and **"L"** are part of the Department of Energy's program for protection of information as required by the Atomic Energy Act of 1954 (10 CFR Part 95.31 and 42 U.S.C. § 2014 and §2162). A **"Q"** clearance is equivalent to a Top Secret clearance, while an **"L"** clearance is equivalent to a Secret clearance. The clearances may be granted only by the Department of Energy based on an individual's need for access to the information and favorable adjudication of the clearance request. The package for requesting a **"Q"** clearance is described in Appendix E, paragraph E.2, Access to Classified and Other Programs. The security contact should contact the Office of Security for information on preparing a request package for those requiring an **"L"** clearance. The request packages should be sent directly through the security contact or servicing security officer to the Office of Security.

1512 Cryptographic Clearance

A. Certain U.S. classified communications security **(COMSEC)** information requires special access restrictions. The Department administers the COMSEC clearance process. Security contacts requiring COMSEC access should contact the Office of Security headquarters. COMSEC information is specified as:

1. Top Secret and Secret, CRYPTO designated, key, and authenticators; and

2. Classified cryptographic media which embody, describe, or implement a classified cryptographic logic, such as full maintenance manuals, cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic computer software.

B. An individual may be granted access to COMSEC information based on the following requirements.

1. Maintains U.S. citizenship.

2. Remains employed by the U.S. Government, or represents the U.S. Government, or serves as a Government contractor, or is employed by a contractor.

3. Requires access to perform official duties for, or on behalf of, the Department of Commerce;

4. Possesses a Department of Commerce security clearance appropriate to the classification level of the COMSEC information to be accessed;

5. Receives a security briefing appropriate to the COMSEC information to be accessed;

6. Acknowledges the granting of access by signing a Cryptographic Access Certificate; and

7. Consents to the administration of a periodic counterintelligence-scope polygraph examination. The polygraph examination will encompass questions concerning espionage, sabotage, and unauthorized giving or selling of classified information to, or unauthorized contacts with, representatives of foreign governments or agencies. The Office of Security will arrange the polygraph examination.

C. The requirements listed above apply to all individuals whose primary assignment allows continuous, long-term access to COMSEC information in large quantities or with highly sensitive applications. Accordingly, these requirements apply specifically to the following personnel.

1. COMSEC custodians or alternates.

2. Producers or developers of cryptographic key or logic.

3. Personnel assigned to the major supply points where cryptographic keying materials are generated or stored.

4. Couriers in the Defense Courier Service.

5. Personnel assigned to secure telecommunications facilities located in fixed ground facilities or on board ships.

6. Specialists who prepare, authenticate, or decode valid or exercise nuclear control orders.

7. Anyone else who has access to classified cryptographic media.