Department of Homeland Security
Management Directives System
MD Number: 11043
Issue Date: 09/17/2004

SENSITIVE COMPARTMENTED INFORMATION PROGRAM MANAGEMENT

I. Purpose

This directive establishes Department of Homeland Security (DHS or Department) policy for the management of Sensitive Compartmented Information (SCI) programs.

II. Scope

This directive applies to all DHS organizational elements with access to information designated Sensitive Compartmented Information.

III. Authorities

A. The Homeland Security Act of 2002, P. L. 107-296.

B. The National Security Act of 1947, 50 U.S.C. 401.

C. Executive Order 12333 “United States Intelligence Activities.”

D. Executive Order 12829, “National Industrial Security Program.”

E. Executive Order 12958, as amended, “Classified National Security Information.”

F. Executive Order 12968, “Access to Classified Information.”

G. Executive Order 13284, “Establishment of the Department of Homeland Security.”

H. Director of Central Intelligence Directive (DCID) 6/1, “Security Policy for Sensitive Compartmented Information and Security Policy Manual.”

I. DCID 6/3, “Protecting Sensitive Compartmented Information Within Information Systems.”

J. DCID 6/4, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information.”

K. DCID 6/7, “Intelligence Disclosure Policy.”

L. DCID 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities.”

M. Department of Homeland Security Delegation Number 8000.1, “Delegation to Chief, Office of Security of Determination Authority and Cognizant Security Authority.”

N. Designation of Chief Security Officer as Senior Agency Official, March 3, 2004.

IV. Definitions

A. ***Accreditation*** is the formal approval of a specific place, referred to as a Sensitive Compartmented Information Facility (SCIF), that meets prescribed physical, technical, and personnel security standards.

B. ***Cognizant Security Authority (CSA)*** is the individual designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management with respect to protection of intelligence sources and methods under SOIC responsibility. The CSA for DHS is the Chief Security Officer.

C. ***Contractor Special Security Officer (CSSO)*** administers the receipt, control, and accountability of SCI materials and the SCI security functions for contractor facilities.

D. ***Information System Security Manager (ISSM)***: The security official responsible for the IS security program for a specific Directorate, Office, or contractor facility.

E. ***Information System Security Officer (ISSO)***: The security official, either government or contractor, responsible for the security posture of a specific Information System.

F. ***Intelligence Community*** includes United States Government agencies and organizations and activities identified in the National Security Act of 1947.

G. ***National Foreign Intelligence Board*** is chaired by the Director of Central Intelligence and is comprised of Intelligence Community members and distinguished civilians appointed by the President.

H. ***Need- to-know*** is a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function. Such person shall possess an appropriate security clearance and access approvals in accordance with Executive Orders 12958, as amended, and 12968, as well as DCID 6/4.

I. ***Senior Agency Official*** is the official designated by the agency head under section 5.4(d) of E.O. 12958, as amended, who directs and administers the agency's program under which information is classified, safeguarded, and declassified. The Senior Agency Official for DHS is the Chief Security Officer.

J. ***Senior Official of the Intelligence Community (SOIC)*** is the head of an organization within the Intelligence Community, as defined by the National Security Act of 1947. Within DHS there are five SOICs: The Secretary, the Deputy Secretary, the Under Secretary for Information Analysis and Infrastructure Protection, the Assistant Secretary for Information Analysis, and the Assistant Commandant for Intelligence for the United States Coast Guard.

K. ***Sensitive Compartmented Information (SCI)*** is classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling within formal access control systems established by the Director Central Intelligence (DCI). SCI is also referred to as "codeword" information. The sensitivity of this information requires that it be protected in a much more controlled environment than other classified information. Therefore, the DCI has established special policies and procedures for the protection of SCI. These policies and procedures are promulgated through Director of Central Intelligence Directives (DCIDs).

L. ***SCI Facility (SCIF)*** is an accredited area, room, group of rooms, buildings, or installation where SCI may be used, stored, discussed and/or processed.

M. ***Security Clearance*** is a formal authorization for an employee with a specific need-to-know to have access to information that is classified as Confidential, Secret, or Top Secret in the interest of national security or the defense of the United States.

N. ***Special Security Officer (SSO)*** works under the direction of the Chief, Special Security Programs Division and administers the receipt, control and accountability of SCI. The SSO oversees SCI security functions and reporting requirements for subordinate SCIFs.

O. ***Special Security Representative (SSR)*** works under the direction of the supporting SSO, and is responsible for the day-to-day management and implementation of SCI security and administrative instructions for a separate, subordinate DHS SCIF.

P. ***Technical Surveillance Countermeasures*** are techniques and measures used to detect and nullify a wide variety of technologies used to obtain unauthorized access to classified national security information, restricted data, and/or unclassified sensitive information.

Q. ***Telecommunications and Automated Information Systems (TAIS)*** is defined as any telecommunications or computer related equipment, or interconnected system or subsystems of equipment, that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice or data (digital or analog), including software, firmware, and hardware.

R. ***TEMPEST*** is an information protection program to preclude inadvertent disclosure of national security information through poor design or installation practices.

V. Responsibilities

A. The Chief Security Officer (CSO) is responsible for administering the Department's SCI program, less that portion under the authority of the Commandant, United States Coast Guard. (See Paragraph V.C below.) The CSO concurrently acts as the Cognizant Security Authority (CSA) for the Department. The CSO shall:

1. Establish a Special Security Programs Division (SSPD) within the Office of Security, with responsibility for administering a Departmental security program that protects SCI information and facilities, in accordance with applicable DCIDs. The office will operate under the authority of the CSA.

2. Appoint a Chief, SSPD, and delegate the authority/responsibility for administering the Department's SCI programs.

3. Develop policies and procedures in accordance with DCIDs for safeguarding SCI information and facilities to be implemented throughout the Department.

4. Ensure implementation of, and compliance with, this policy within DHS Headquarters, DHS Organizational Elements, and by DHS contractors, consultants, and state and local elements supporting DHS mission requirements.

B. The Chief, Special Security Programs Division is, by this management directive, delegated authority and responsibility for managing the SCI program within DHS. To facilitate management and administration of the program at organization element activities, the Chief, SSPD, will appoint a Special Security Officer (SSO) for each DHS Organization Element with an SCI mission, with the exception of the United States Coast Guard (USCG). Each applicable organizational element shall appoint a Special Security Representative (SSR). The Chief, SSPD will approve each appointee, under the authority of the CSA, and will ensure appointees are properly trained and certified, as necessary. The Chief, SSPD shall have oversight of all DHS SSOs and SSRs.

C. The United States Coast Guard, as a member of the Intelligence Community, shall independently administer its SCI program in accordance with its own instruction - Classified Information Management Program (COMDINST M5510.23). USCG guidance and instructions shall be consistent with DCI Directives.

D. The Chief, SSPD shall develop guidance for handling, safeguarding, storing, processing, and disseminating SCI within the Department, consistent with the DCIDs. Promulgation of DHS standards and policies by SSPD will ensure a consistent application of all security requirements throughout the Department.

E. DHS SSOs will report to the Chief, SSPD. Organizational element SSRs will report to the heads of their respective elements. Guidance and oversight will be provided by the supporting SSO.

F. The organizational element SSO /SSR will administer SCI programs within his/her respective element using the policies and standards developed by the Chief, SSPD as required for effective administration of the DHS SCI program.

VI. Policy & Procedures

A. The following is general guidance to DHS organizational elements regarding the storage, handling, use, discussion and processing of SCI information.

1. Basic SCI Controls. Specific administrative guidance concerning the control of SCI is contained in DCID 6/1, “Security Policy for Sensitive Compartmented Information and Security Policy Manual.”

a. SCI access approvals shall be granted by the CSA, or his designee, having cognizance of the persons involved.

b. SCI material will only be disseminated on a need-to-know basis to individuals who hold the proper clearance level and access approval for the information. If the specific accesses of an individual are not known, the organizational element SSO, or SSR, must be contacted for verification prior to sharing information with that individual.

c. SCI information may only be discussed, used, handled, electronically processed, or stored within an accredited Sensitive Compartmented Information Facility (SCIF). According to DCID 6/1, the Central Intelligence Agency or its designee shall accredit SCIFs for Executive branch departments and agencies outside the Intelligence Community.

d. SCI material will not be sent to a facility or building that does not have a SCIF, nor to an individual who does not have access to a SCIF.

e. SCI materials sent between accredited SCIFs will be hand-carried by individuals who are properly briefed on courier procedures, possess a valid courier card or letter, and who are cleared for the material being transported.

(1) Materials carried within a building should be in a sealed opaque envelope that is properly addressed.

(2) SCI shall be enclosed for shipment in two opaque envelopes or be otherwise suitably double-wrapped using approved containers.

(3) Outer containers shall be secured by an approved means that reasonably protects against surreptitious access. The inner and outer containers shall be annotated to show the package number and addresses of the sending and receiving SCIF. The notation “TO BE OPENED BY THE (appropriate SCI Special Security Officer)” shall be placed above the pouch address of the receiving SCIF on the inner container. The inner wrapper shall contain the document receipt and name of the person or activity for which the material is intended. The applicable security classification and the legend “CONTAINS SENSITIVE COMPARTMENTED INFORMATION” SHALL APPEAR ON EACH SIDE OF THE INNER WRAPPER ONLY.

(4) Materials transported between buildings will be double-wrapped in the same manner required for National Security Information.

f. All SCI materials will be properly marked and, when required, have cover sheets attached.

g. SCI can be processed only on a computer, or network of computers, that has been specifically certified and accredited for that level of classified information. Additionally, SCI materials may be electronically transferred between appropriately accredited machines (facsimile, computers, secure voice, secure e-mail, or any other means of telecommunication ensuring that such transmissions are made only to authorized recipients). It is essential to ensure that appropriate secure devices are used for any type transfer of SCI material.

h. Personnel who hold access to SCI material will receive periodic refresher briefings on the procedures for handling SCI materials. The Chief, SSPD, or SSO will provide periodic refresher briefings.

i. Any loss, compromise, or suspected compromise of SCI materials will be immediately reported to the organizational element SSO and to the Chief, SSPD.

2. SCI Access Authorizations.

a. For DHS Headquarters-supported organizational elements, requests for access to SCI shall be submitted in writing to the Chief, SSPD, through the organizational element SSO and OE Chief of Staff. The request must be approved by an SCI-accessed individual in the person's management chain, who can accurately specify the access required, need-to-know, and justification for the access request. After reviewing and approving the request, the Chief, SSPD, will forward the request to the Personnel Security Division for processing.

b. For DHS organizational elements authorized to grant access to SCI, a similar process shall be used, including final approval by the Senior Intelligence Official having cognizance of the persons involved.

c. In order for an individual to be considered for access to SCI, they must have a Top Secret security clearance based on a Single Scope Background Investigation (SSBI). If an appropriate SSBI has not been completed, the responsible organizational element's personnel security division shall initiate the appropriate background investigation.

d. The organizational element's personnel security division shall adjudicate the Background Investigation in accordance with guidelines established by DCID 6/4, and shall designate eligibility for SCI access accordingly. The Personnel Security Division shall notify the Chief, SSPD if, during the adjudication process, an SCI nominee is determined ineligible for any reason. If appropriate, the nominee will then be processed for a waiver in accordance with DCID 6/4. Waivers to the requirements of DCID 6/4 shall only be requested when the benefit of access clearly outweighs any security concern. Requests for waivers must be concurred with by the directorate chief of staff or organizational element director. Requests for waivers must be approved by the Chief, SSPD and the CSA. The DCI is the exclusive authority for granting an exception to the requirement that the subject be a U.S. citizen.

e. As a condition of access to SCI, individuals must sign a DCI-authorized SCI Nondisclosure Agreement (NdA) (Form 4414), which includes a provision for prepublication review. The NdA establishes explicit obligations on both the government and the individual signer for the protection of SCI. Failure to sign an NdA is cause for denial or revocation of existing SCI access.

f. Prior to signing the SCI NdA or being afforded access to SCI, persons approved for SCI access shall be briefed by the SSO or SSR. The briefing shall consist of non-SCI-revealing information of a general nature: procedures for protecting the SCI to which they will be exposed; advised of their obligations both to protect that information and to report matters of security concern; and allowed to express any reservations concerning the NdA or access to SCI. After the person has signed the NdA, they will be further indoctrinated into the specific SCI programs for which they have been approved access. Upon transfer, resignation, retirement, or separation from DHS, OE SSOs or SSRs will conduct a debrief and the individual shall sign the Form 4414 in the appropriate block.

3. Reporting Requirements.

a. Persons currently approved for SCI access who plan official or unofficial travel to or through foreign countries, or who are being assigned to duty in foreign countries, shall provide the SSO or SSR advance written notice of the travel. Prior to the official assignment or unofficial travel, the individual will receive an appropriate defensive security briefing. These travel briefings will be given at least annually.

b. Persons with SCI access have a continuing responsibility to report, within 72 hours, to their immediate supervisor or local SSO/SSR all contacts:

(1) That are of a close, continuing personal association, characterized by ties of kinship, affection, or obligation with foreign nationals. Casual contacts and associations arising from living in a community normally need not be reported.

(2) In which illegal or unauthorized access is sought to classified, sensitive, or proprietary information or technology, either within or outside the scope of the employee's official activities.

c. Persons who are currently, or were previously, employed by DHS and indoctrinated for SCI access, will submit proposed articles and publications for prepublication review. This review process applies to all printed publications and oral presentations that reference DHS intelligence data or related activities, at any classification level, or to information derived as a result of affiliation with DHS. Request for review will be submitted to the Chief, SSPD.

4. Sensitive Compartmented Information Facility. All SCI material must be stored, used, discussed, and/or electronically processed within accredited SCIFs. Organizational elements shall request the establishment of a SCIF only when there are clear operational requirements and when existing SCIFs are not adequate to support the requirements. DHS organizational elements shall make use of existing SCIFs or consolidated SCIFs whenever possible. DHS procedures for establishing SCIFs are as follows:

a. The requirements justifying a new SCIF shall be documented and maintained with accreditation records. When it is determined that a SCIF is necessary for an SCI program, the organizational element SSO or SSR will contact the Chief, SSPD and provide a Concept of Operations (CONOPS) document detailing the requirements for the SCIF establishment and a pre-construction, DCID 6/9, Fixed Facility Checklist, completed to the maximum extent possible. The Chief, SSPD, will provide these materials to the Central Intelligence Agency or its designee, for review. The Chief, SSPD, will provide assistance, as necessary, during this process in accordance with DCID 6/9.

b. The Chief, SSPD shall ensure the SCIF is constructed in accordance with the security specification provided in DCID 6/9. Upon completion of construction, the Chief, SSPD, will ensure an inspection is conducted with qualified personnel to ensure it meets DCID 6/9 standards.

c. The organizational element SSO/SSR shall prepare the required Fixed Facility Checklist and Standing Operating Procedures (SOP). The SSO or SSR shall ensure the SOP is fully implemented.

d. The Chief, SSPD will ensure Technical Surveillance Countermeasures (TSCM) inspections and TEMPEST inspections are conducted in accredited SCIFs, as necessary. The organizational element SSO/SSR will coordinate requirements and consider mitigation strategies as necessary.

e. The Central Intelligence Agency or its designee will conduct a final inspection of the SCIF, and review and approve the required SCIF documentation and procedures. SCIF accreditation documentation will be approved by the Central Intelligence Agency or its designee.

f. The organizational element SSO/SSR shall obtain the approval of the Central Intelligence Agency (CIA) or its designee for any significant change affecting the integrity of any CIA-accredited SCIF, prior to any change in the SCIF construction or operating procedures. These may include, but are not limited to, changes in perimeter, alarms, or anything that might introduce a vulnerability to the facility.

5. SCI Computer Systems.

a. Telecommunications and automated information systems, (TAIS) used to process, store, or handle SCI, will be operated so that the information is protected against unauthorized disclosure, modification, access, use, destruction, or delay in service.

b. The Principal Accrediting Authority for DHS TAIS is the Secretary. This authority has been delegated to the Assistant Secretary for Information Analysis who is the Designated Accrediting Authority (DAA).

c. All TAIS that process, store, or handle SCI will be certified and accredited by the DHS DAA prior to operation. The Chief, SSPD shall support the DAA, as necessary, during the lifecycle of DHS SCI systems.

d. All TAIS processing SCI will follow the requirements delineated in Director of Central Intelligence Directive (DCID) 6/3.

e. SCI systems will not be placed in operation until authorized, in writing, by the DAA.

f. When the need to process SCI information becomes apparent, the organizational element SSO will contact the Chief, SSPD. The Senior Agency Official, in concert with the DHS Chief Information Officer (CIO), will provide support in defining the organization's needs and the requirements necessary to meet those needs. The Chief, SSPD, shall provide support to the CIO/ISSM/ISSO in developing security-related documentation for the certification and accreditation process.

6. Clearance Certifications.

a. DHS employees holding SCI access who plan to attend meetings, document reviews, conferences, or other similar events at other organizations where the discussion of SCI will occur, may be required to have their SCI access certified to the agency or organization sponsoring the event.

b. The Chief, SSPD, shall establish procedures for transmitting and receiving SCI clearances between organizations.

c. All appropriately appointed organizational element SSO/SSRs are authorized to transmit and receive clearances in support of Department requirements and mission obligations.

7. Transferring SCI Eligibility. Transfer-in-Status (TIS) is a process through which an individual may transfer from one DHS organizational element to another DHS organizational element and remain in an SCI-indoctrinated status. Re-indoctrination of those individuals is not required.

a. The gaining organizational element may request a TIS, of an individual scheduled for a permanent transfer, based on the existence of a need-to-know in the individual's new position. The gaining organizational element is responsible for initiating the process by providing the specified, required data elements using the DHS approved TIS form. The losing organizational element will debrief the individual from any SCI accesses not transferred, and will provide a TIS effective date, which is the anticipated departure date from the losing organizational element.

b. The TIS process is generally accepted between government agencies, subject to the approval of the servicing Special Security Officer, and shall be used within DHS to the maximum extent possible.

c. TIS will only be accepted if the person being transferred is accessed without any waiver or condition.