Sensitive Compartmented Information Facility (SCIF)

Cheryl L. Wieser- Regional Security Officer
U.S. Department of Commerce
Office of Security (OSY)
Western Region Security Office
Seattle, WA 98115
206-526-6653

Updated: September 2006

OVERVIEW

- The following slides are designed to give you a brief overview of key definitions and some basic construction requirements associated with a SCIF.

- This overview is not all inclusive. All those specific Director of Central Intelligence Directives (DCIDs) pertinent to your particular program or project must be reviewed to determine the comprehensive requirements.

Sensitive Compartmented Information (SCI)

- **Definition**: "SCI," classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI).

SCI Facility (SCIF)

- **Definition**: "SCI Facility," an *accredited* area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed.

Need-to-know

- **Definition**: "Need-to-know," 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 DCID 6/4.

Accreditation of SCI Facilities (SCIFs)

- Definition: “Accreditation,” is the formal certification of a specific place referred to as a SCIF that meets those security requirements prescribed in DCID 6/9- Physical Security Standards for Sensitive Compartmented Information Facilities.

Cognizant Security Agency (CSA)

- Definition: “CSA,” are intelligence organizations or agencies as defined in E.0.12333 that have the authority and are responsible for all aspects of security program management with respect to the protection of intelligence sources and methods and for implementation of the DCIDs for activities under their purview.

Senior Officials of the Intelligence Community (SOIC)

- Definition: “SOIC,” the head of an agency, office, bureau, or intelligence element listed in Executive Order 12333, Section 3.4(f) (1 through 6) or successor orders, directives or laws.

SCI ACCESS

- Approvals shall be granted by the SOIC having cognizance of the persons involved. For persons in non-National Foreign Intelligence Board (NFIB) government organizations, SCI access approvals are granted by the DCI through the CIA.

Construction and Protection Requirements and Standards

- All SCI must be stored within accredited SCIFs.
- Accrediting authorities are responsible for ensuring that SCIFs are established only when there are clear operational requirements and when existing SCIFs are not adequate to support the requirement. The requirements justifying a new SCIF shall be documented and maintained with accreditation records. Physical security standards for the construction and protection of such facilities are prescribed in the current DCID 6/9- Physical Security Standards for Sensitive Compartmented Information Facilities.

Accreditation of SCIFs

- The DCI is the accrediting authority for all SCI Facilities, except where that authority has been delegated or otherwise provided for *(note: see DCID 6/1)*.
- Except where specific agreement exists, introduction of an additional program into a previously accredited SCIF requires the joint approval of the host SOIC and the responsible SOIC requesting tenant status.
- The CIA shall accredit SCIFs for Executive Branch departments and agencies outside the Intelligence Community, and for the Legislative and Judicial branches.

Accreditation of SCIFs (continued)

- The procedures for establishment and accreditation of SCIFs from conception through construction must be coordinated and approved by the SOIC or CSA.
- All SCIFs shall maintain on site current copies of:

  (1) DCID 6/9 Fixed Facility Checklist

  (2) Accreditation/Authorization documents (physical, EMSEC, AIS)

  (3) Inspection reports, including TSCM reports, for the entire period of SCIF accreditation

  (4) Operating procedures, Special Security Officer (SSO)/Contractor Special Security Officer (CSSO) appointment letters, Memoranda of Agreement, Emergency Action Plans, etc.

  (5) Copies of any waivers granted by the CSA

Accreditation of SCIFs (continued)

Co-Utilization

Agencies desiring to co-utilize a SCIF:

(1) Should accept the current accreditation and any waivers.

(2) Should fund any security enhancements they deem necessary to be able to co-utilize the facility *(note: these enhancements must be approved by the SOIC, and receive DCI concurrence prior to implementation).*

(3) Must execute a co-utilization agreement prior to occupancy.

Physical Security Construction Policy

- Physical security criteria is governed by whether the SCIF is located in the United States or not; and according to the following conditions:
  - (1) Closed Storage
  - (2) Open Storage
  - (3) Continuous Operations
  - (4) Secure Working Areas

Closed Storage

Inside United States:

(1) The SCIF must meet the specifications in DCID 6/9, Chapter 4- Permanent Dry Wall Construction.

(2) The SCIF must be alarmed in accordance with DCID 6/9, Annex B- Intrusion Detection Systems.

(3) SCI must be stored in GSA approved classified storage containers.

Closed Storage (continued)

(4) There must be a response force capable of responding to an alarm within 15 minutes *(up to 30 minutes with Security-In-Depth and CSA approval)* after annunciation, and a reserve response force available to assist the responding force.

(5) The CSA may require any SCIF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by DCID 6/9, Chapter 4- Expanded Metal construction requirement.

Closed Storage (continued)

Outside the United States:

(1) The SCIF must meet the construction specifications for SCIFs as set forth in DCID 6/9, Chapter 4- Steel Plate or Expanded Metal.

(2) The SCIF must be alarmed in accordance with DCID 6/9, Annex B- Intrusion Detection Systems.

(3) All SCI controlled material will be stored in GSA approved classified storage containers having a rating for forced and surreptitious entry equal to or exceeding that afforded by GSA Class 5 containers.

(4) There must be a response force capable of responding to an alarm within 10 minutes, and a reserve response force available to assist the responding force.

Open Storage

Inside United States:

When open storage is justified and approved by the CSA, the SCIF must:

(1) be alarmed in accordance with DCID 6/9, Annex B- Intrusion Detection Systems;

(2) have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the response force; and…

Open Storage (continued)

(3) meet one of the following:

(a) SCIFs within a controlled US government compound or equivalent may use specifications indicated in DCID, Chapter 4- Permanent Dry Wall Construction; or

(b) SCIFs within a controlled building with continuous personnel access control, may use specifications indicated in DCID, Chapter 4- Permanent Dry Wall Construction. The CSA may require any SCIF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by DCID, Chapter 4- Expanded Metal construction requirements; or

Open Storage (continued)

(c) SCIFS which are not located in a controlled building or compound may use specifications indicated in DCID, Chapter 4- Expanded Metal or Vault construction requirements.

Open Storage (continued)

Outside the United States:

When open storage is justified as mission essential vault construction as set forth in DCID 6/9, Chapter 4- Vaults is preferred *(note: open storage of SCI material outside of the Untied States will be avoided).* The SCIF must:

(1) be alarmed in accordance with DCID 6/9, Annex B- Intrusion Detection Systems.

(2) have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.

(3) have an adequate tested plan to protect, evacuate or destroy the material in the event of emergency or natural disaster.

Continuous Operation

Inside the United States:

(1) The SCIF must meet the construction specifications as identified in DCID 6/9, Chapter 4- Permanent Dry Wall Construction.

(2) An alert system and duress alarm may be required by the CSA *(note: based on operational and threat conditions)*.

(3) Provisions should be made for storage of SCI in GSA approved classified storage containers.

(4) There must be a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.

Continuous Operation

Outside the United States:

(1) The SCIF must meet the construction specifications as identified in DCID 6/9, Chapter 4- Expanded Metal.

(2) An alert system and duress alarm may be required by the CSA *(note: based on operational and threat conditions)*.

(3) The capability must exist for storage of all SCI in GSA approved classified storage containers.

(4) There must be a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.

Secure Working Areas

- Secure Working Areas are accredited facilities used for handling, discussing, and/or processing SCI, but where SCI *will not be* stored.

Secure Working Areas

Inside the United States:

(1) The Secure Working Area SCIF must meet the specifications set forth in DCID 6/9, Chapter 4- Permanent Dry Wall Construction.

(2) The Secure Working Area SCIF must be alarmed with a balanced magnetic switch on all perimeter entrance doors.

(3) No storage of SCI material is authorized.

(4) There must be a response force capable of responding to an alarm within 15 minutes after annunciation and a reserve response force available to assist the responding force.

Secure Working Areas

Outside the United States:

(1) The Secure Working Area SCIF must meet the specifications set forth in DCID 6/9, Chapter 4- Permanent Dry Wall Construction.

(2) The Secure Working Area SCIF must be equipped with an approved alarm system as set forth in DCID 6/9, Annex B- Intrusion Detection Systems.

(3) No storage of SCI material is authorized.

(4) There must be a response force capable of responding to an alarm within 10 minutes after annunciation and a reserve response force available to assist the responding force.

Common Requirements For All SCIFs

Construction: SCIF perimeter walls, floors and ceiling, will be permanently constructed and attached to each other. All construction must be done in such a manner as to provide visual evidence of unauthorized penetration.

Sound Attenuation: The SCIF perimeter walls, doors, windows, floors and ceiling, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of conversation. The requirements for sound attenuation are contained within DCID 6/9, Annex E- Acoustical Control and Sound Masking Techniques.

Common Requirements (continued)

Entrance, Exit & Access Doors:

(1) Primary entrance doors to SCIFs shall be limited to one.

(2) In some circumstances, an emergency exit door may be required. In cases where local fire regulations are more stringent, they will be complied with.

(3) All SCIF perimeter doors must be plumbed in their frames and the frame firmly affixed to the surrounding wall.

Common Requirements (continued)

(4) All SCIF primary entrance doors must be equipped with an automatic door closer, a GSA-approved combination lock and an access control device with the following requirements *(note: this requirement does not apply to the GSA approved Class 5, 6 & 8 vault doors)*:

(a) Doors with hinge pins on the exterior side of the door, where it opens into an uncontrolled area outside the SCIF, shall have the hinge pins treated to prevent removal of the door.

(b) If a SCIF entrance door is not used as an access control door and stands open in an uncontrolled area, the combination lock will be protected against unauthorized access/tampering.

Common Requirements (continued)

Control Doors: The use of a vault door for controlling daytime access to a facility is not authorized.

Emergency Exit Doors: Shall be constructed of material equivalent in strength and density to the main entrance door.

Common Requirements (continued)

Door Construction Types:

(1)Solid wood core door, a minimum of 1 3/4 inches thick.

(2) Sixteen gauge metal cladding over wood or composition materials, a minimum of 1 3/4 inches thick. The metal cladding shall be continuous and cover the entire front and back surface of the door.

(3) Metal fire or acoustical protection doors, a minimum of 1 3/4 inches thick. A foreign manufactured equivalent may be used if approved by the CSA.

(4) A joined metal rolling door, minimum of 22 gauge, used as a loading dock or garage structure must be approved on a case-by-case basis.

Common Requirements (continued)

Vents, Ducts & Pipes:

(1) All vents, ducts, and similar openings in excess of 96 square inches that enter or pass through a SCIF must be protected with either bars, or grills, or commercial metal duct sound baffles that meet appropriate sound attenuation class as specified in DCID 6/9, Annex E.

(2) All vents, ducts and pipes *may* require a non-conductive section installed at the interior perimeter of the SCIF, that is unable to carry electric current (note: based upon the EMSEC/TEMPEST accreditation).

(3) An access port to allow visual inspection of the protection in the vent or duct should be installed inside the secure perimeter of the SCIF.

Common Requirements (continued)

Windows:

(1) All windows which might reasonably afford visual surveillance of personnel, documents, materials, or activities within the facility, shall be made opaque or equipped with blinds, drapes or other coverings to preclude such visual surveillance.

(2) All windows at ground level will be constructed from or covered with materials which will provide protection from forced entry *(note: this should be interpreted to mean any windows which are less than 18 feet above the ground measured from the bottom of the window).*

(3) All perimeter windows at ground level shall be covered by an IDS.

In Conclusion

Applicability:

It is sometimes necessary for non-SCI programs to be afforded an equal level of protection by introduction of non-SCI material into SCIFs. Should this occur, the express approval of the accrediting authority is required. Appropriate documentation shall be included in the accreditation records.

SCIFs are established primarily for SCI, and are intended to provide the highest level of physical security protection.