SCI and SCIFs

Sensitive Compartmented Information

Sensitive Compartmented Information (SCI) is a program that segregates various types of classified information into distinct compartments for added protection and dissemination or distribution control. SCI introduces an overlay of security to Top Secret, Secret, and Confidential information. To be granted access to SCI material, one must first have TOP SECRET clearance and be indoctrinated into the SCI program. There are explicit indoctrinations for each compartment under the SCI program umbrella. The Director of National Intelligence has overarching authority concerning SCI policy.

SCI markings, or caveats, identify the specific compartment or compartments with which the material is affiliated. These caveats define the separation of SCI classified material from collateral classified material.

Information that requires a formal need-to-know determination, also known as a special access authorization, exists within Sensitive Compartmented Information.

Compromised SCI

A compromise occurs when a person who does not have the required clearance or access caveats comes into possession of SCI in any manner (i.e., physically, verbally, electronically, etc.).

You are required to contact your security Point of Contact (POC) to report the incident. Do not elaborate detailed information (that may be considered sensitive/classified) concerning the people, processes, technology, file location, specific system information, or URL that may be related to the nature of the incident until secure two-way communications (verbal or transmitted) may be achieved.

Marking SCI

When handling SCI:

- Mark classified information appropriately
    - Use proper markings, including paragraph portion markings
    - Use Security Classification Guides
    - Use Classification Management Tool (CMT) (ICS 500-8) for email and electronic documents
- Attach appropriate cover sheets
- Take precautions when transporting classified information through unclassified areas
- Complete annually required classification training

A Security Classification Guide:

- Provides precise, comprehensive guidance regarding specific program, system, operation, or weapon system elements of information to be classified, including:
    - Classification levels
    - Reasons for classification
    - Duration of classification
- Is approved and signed by the cognizant Original Classification Authority (OCA)
- Is an authoritative source for derivative classification
- Ensures consistent application of classification to the same information

Transmitting SCI

Use proper protections for transmitting and transporting SCI, such as proper wrapping and courier requirements.

- Dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued by the Director of National Intelligence

Printing:

- Retrieve classified documents promptly from printers
- Use appropriate classification cover sheets
- Ensure classified material is not mixed in with unclassified material being removed from SCIF
- Cover or place classified documents in a container even in an open storage environment

Fax:

- Mark SCI documents appropriately
- Send SCI information using an approved SCI fax machine
- Follow SCI handling and storage policies and procedures
- Immediately report security incidents to your Security POC

Courier:

- Authorization to escort, courier, or hand-carry SCI shall be in accordance with appropriate organization policy (agency-specific resources external to the course)
- Follow SCI transporting badge requirements and procedures
- Only transport SCI information if you have been courier-briefed for SCI
- Refer to agency-specific policies and requirements prior to transporting SCI information
- Contact your Special Security Office (SSO) or Security POC for questions/clarification

SCIF Security

Within a Sensitive Compartmented Information Facility (SCIF):

- Everyone must badge in – no piggybacking
- Personnel entering or leaving an area are required to secure the entrance or exit point
- Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's need-to-know and access
- Badges must be visible and displayed above the waist at all times while in the facility
- Badges must be removed when leaving the facility

SCIF Situational Awareness

Situational awareness and SCI:

- Do not discuss sensitive or classified information around non-cleared personnel, personnel without a need-to-know, or outside of a properly secured facility, as it could lead to a compromise of SCI.
- When discussing sensitive or classified information, physically assess that all personnel present or within listening distance have a need-to-know for the information being discussed
- Do not hold phone conversations on unencrypted phones in the vicinity in which classified or sensitive information is being discussed
- Ensure monitors do not provide unobstructed views of classified information – monitors facing windows should be turned or the window blinds should be closed
- Ensure uncleared persons are escorted by a cleared person familiar with the facility security procedures
- Warn those in the SCIF that uncleared personnel are present in the secure facility or working area

When sharing information in a SCIF:

- Follow security practices for protecting classified material; do not assume open storage just because you are in a SCIF
- Ensure that the person with whom you are sharing information is properly cleared and has a need-to-know
- Do not reference or hyperlink derivatively classified reports, documents, records, or articles that are classified higher than the audience in receipt
- Do not share any information with any individuals without checking need-to-know
- Balance the need to share intelligence with the need to protect sources and methods
- Appropriately mark and protect all classified material

Devices in a SCIF

No personal portable electronic devices (PEDs) are allowed in a SCIF. Government-owned PEDs must be expressly authorized by your agency. When using a government-owned PED:

- Only connect government-owned PEDs to the same level classification information system when authorized
- Only use devices of equal or greater classification than the information you are accessing or transmitting
- Ensure secure device is properly configured and updated
- Don't discuss classified information over smartphones
- Don't view classified information via device when not in a cleared space

As a general rule, there should be no Wi-Fi, Bluetooth, cellular, image capturing, video recording, or audio recording capabilities or wearable devices in the SCIF. Check with your security officer or your agency's policies.

Using Removable Media in a SCIF

When using removable media:

- Users must properly identify and disclose removable media with local Configuration/Change Management (CM) Control and Property Management authorities
- Users shall comply with site CM policies and procedures
- Media shall display a label inclusive of maximum classification, date of creation, POC, and CM Control Number

Removable Media Risks

The risks associated with removable media include:

- Introduction of malicious code
- Compromise of systems' confidentiality, availability, and/or integrity
- Spillage of classified information

Potential consequences:

- Shutdown of systems
- Compromise of information, systems, programs, and/or assets
- Loss of mission
- Loss of life

Incident Follow-up in a SCIF

If an incident occurs:

- Notify your security POC about the incident
- An analysis of the media must be conducted for viruses or malicious code
- The other workstations in the SCIF must also be analyzed
- If the incident was unintentional, then the person may have to attend a refresher training course in security awareness