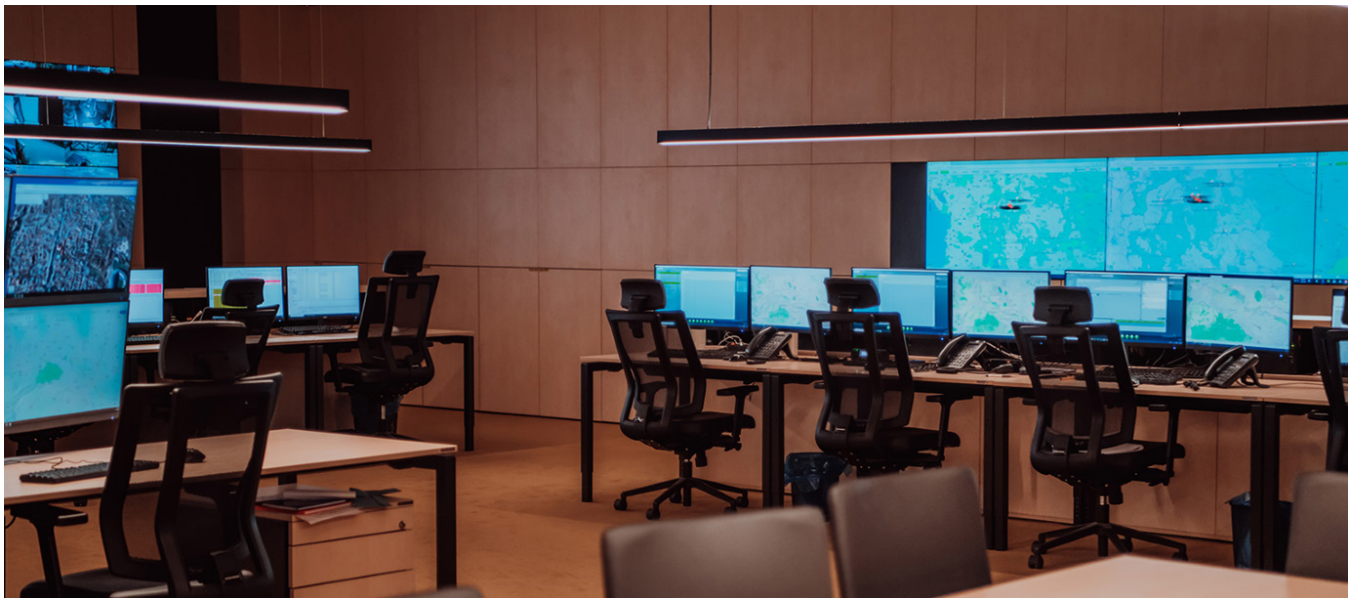
secure design

SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF)

by: Steve Kimball



A SCIF is a contained environment that provides high-level security for designated personnel to process sensitive and/or classified information. These facilities are primarily associated with agencies that require high levels of information security such as the federal Department of Defense (DoD), diplomatic and intelligence agencies, and related private sector companies that provide services to or for such agencies.

The National Counterintelligence and Security Center (NCSC) is the governing authority responsible for the development and maintenance of the Intelligence Community Technical Specification which outlines criteria for security risk management, and design and construction specifications for SCIFs. These criteria can be found in the NCSC Intelligence Community Directive/Specification ICD/ICS 705.

Application of the criteria is generally promulgated by the organization or agency's Accrediting Official (AO) in concert with the Site Security Manager (SSM). It is important to engage the AO and SSM early in the planning process to ensure design and construction meet the specific operational and site requirements.

general compartmented area (ca) requirements

The “Compartmented Area” is a space, room, or set of rooms within a SCIF that provides controlled physical and electronic separation. The “type” of compartmentation required is a key element in the development of appropriate design and construction standards. Compartmented areas must be separated in accordance with ICS 705-1 with approved acoustic, technical, and access control.

Type I: Open workstation or rooms used to securely view and process compartmented information via an approved computer. No storage or discussion is authorized in this space.

Type II: Open workstation/rooms where compartmented discussions and/or video conferencing may be conducted by authorized personnel. All Type II CAs must comply with the sound transmission class (STC) requirements of ICS 705-1. No storage is authorized in this space.

Type III: A restricted discussion area for viewing, processing, and storing compartmented information.

closed and open storage

The storage of information in a compartmented area within a SCIF is classified as “closed” or “open” as dictated by the level of information security required. The AO may approve open or closed storage within a SCIF.

Closed Storage: All compartmented information must be stored in a General Services Administration (GSA) approved safe when not in use.

Open Storage: SCIF perimeter acoustic, technical, and access control is required. GSA safe storage is not required when not in use.

design & construction

Chapter 3 of ICD/ICS 705 outlines the requirements for fixed facility SCIF design and construction. Chapter 3 provides criteria for the design and construction of each primary SCIF element, including suggested design details for compliance. SCIF design and construction requirements include three areas for security consideration: **Physical, Acoustic, Tempest.**

physical security

Access Control

Access control includes card readers, keypads, electric door strikes, communication interface devices, specialized locks, and other access control equipment located outside the SCIF perimeter.

Security access may include separation using a security vestibule. Access control often incorporates visual security via closed circuit TV and entry access requests via telephone. The non-secure vestibule is typically equipped with lockers for depositing personal electronic devices before passing through the SCIF secure perimeter.

Intrusion Detection System (IDS)

Intrusion Detection Systems are required for the interior areas of a SCIF to prevent unauthorized access. The IDS is an internal SCIF perimeter system that incorporates audible and visual annunciation of each IDS device. The IDS is separate from the access control and fire alarm systems and must be supported by an emergency electrical power system. IDS sensors typically include motion detectors, infrared sensors, and balanced magnetic switches.

Perimeter Construction

Perimeter construction provides a defined physical separation between secure and non-secure space as outlined in Chapter 3 of ICD/ICS 705. A single SCIF entrance is preferred with accommodation for a non-secure entry vestibule when warranted by the organization's location and operations. Windows and additional entry points into the SCIF are discouraged and should only be considered when there is a compelling operational need. The entire SCIF perimeter should provide access for periodic visual inspections to ensure the integrity of the secure perimeter has not been breached. Details and requirements for ongoing security inspections should be established as part of the project planning process. Physical penetration of the "SCIF wall" should be limited and properly addressed as required by ICS 705. Devices, conduit, ductwork, panels, equipment, etc. are to be surface mounted on the "SCIF wall" to minimize penetrations, thus maintaining the security perimeter.

Acoustic Security

SCIF acoustic separation is classified by Sound Transmission Class (STC) in two (2) Sound Groups: Sound Group 3 and Sound Group 4. Acoustic accreditation testing may be conducted by instrumental or non-instrumental means as determined by the AO/SSM.

Sound Group 3: STC 45 or better. Speech c

Chapter 3 of ICD/ICS 705 provides standard details for differing wall construction conditions. Understanding the acoustic requirements, construction conditions, potential failure areas, and testing methodology are key elements to the successful design and construction of a SCIF. HVAC ductwork penetrations though the SCIF perimeter will require sound mitigation via a "Z-duct" configuration or use of an inline sound attenuator.

Where sound mitigation cannot be met with normal construction the following supplemental mitigation strategies can be employed:

- **Application of sound deadening materials**
- **Use of a "stand-off" perimeter**
- **Application of a sound masking system**
- **Introduction of speakers / transducers**

Tempest Security

Depending on the client's activities, TEMPEST shielding may or may not be a SCIF requirement. When required, TEMPEST application should be reviewed during the planning stage with the AO and SSM. Discussion should include the type and application of TEMPEST materials, SCIF utility penetration locations and requirements, and RED/BLACK separation requirements.

TEMPEST mitigation protects against the deliberate technical / electronic interception of electromagnetic emanations from the processing equipment (laptops, servers, etc.). Where required, TEMPEST countermeasures provide a shielded enclosure which maintains a six-sided electronic boundary to secure classified electronic data.

Key TEMPEST Terms are highlighted in the chart.

RF Shielding	Strategies include the use of an RF shielding material applied as part of the SCIF envelope (walls, ceiling, and floor). Materials include foil-backed gypsum board and/or other foil-incorporated product(s) as part of the SCIF perimeter's physical envelope. Shielding must be electrically and continuously bonded withth no gaps on the walls, doors, or windows.
RF Filters	Power and telecommunications service penetrations to a SCIF should be limited and isolated with approved RF filters.
Utility Wall Penetrations	SCIF wall utility wall penetrations require a non-conductive break for all ferrous materials.
Red/Black Power & Telecommunications Systems	Mission (secure) and support services (non-secure) may require physica separation of equipment and conduit to prevent unauthorized detection of signals emanating from secure systems

challenges

Design and construction of SCIF spaces vary in complexity and can be challenging depending on the clients' requirements, location, existing site conditions, and the accreditation process. Following is a brief outline of specific items that merit special attention when planning, designing, and constructing a SCIF.

Accreditation

Although ICD/ICS 705 provides design and construction criteria for a SCIF environment, the agency, physical location, type and significance of operations, unique circumstances, and the accrediting authority are important considerations in the successful design and construction of a SCIF.

Access Control

Access control design is often in conflict with code-related egress requirements. A key consideration when developing an access control strategy requires discussion with the Authority Having Jurisdiction (AHJ) regarding "fail-safe" vs. "fail-secure" operation in the event of an emergency and/or power failure. Requirements for emergency egress should be reviewed and approved as an important element of the SCIF design and construction.

"Early and continuous engagement with Site Security Manager and Accrediting Official is key to a successful project."

Intrusion Detection System

It is important to discuss the IDS project design, specification, and installation requirements at the project planning stage. IDS's are often proprietary and are purchased and installed by the client. When this is the case, coordination is imperative to ensure the system is adequately designed and constructed.

Doors

SCIF STC doors are expensive and can become a primary reason for acoustic separation failure. The selection, specification, approval, and installation of SCIF STC doors should be closely coordinated with all stakeholders, including the AO/SSM. It is recommended that delivery and installation of SCIF doors include, at a minimum, the requirement for a technical representative of the manufacturer to be physically on site to supervise the installation. When possible, it is recommended SCIF doors be turnkey with the manufacturer responsible for delivery and installation.

Space Separation

Many SCIFs incorporate physically sub-divided rooms within the SCIF perimeter. A design and construction best practice is to prepare the internal rooms for future SCIF separation. Building "SCIF ready" walls will allow a sub-divided room to become a separate SCIF space in the future. This approach involves a nominal increase in the initial construction cost but minimizes operational disruptions in the future.

Ductwork Penetrations

Advance planning and design of the HVAC ductwork design is important so that appropriate measures are taken to mitigate sound transmission at SCIF perimeter penetrations. The use of a "Z-duct" configuration is generally the preferred solution, however application of a sound attenuator in lieu of a "Z-Duct" may be dictated by space constraints. When sound attenuators are used, it is important to understand the impact of air flow (cfm) requirements so that an adequate amount of air is delivered to the space.

TEMPEST Shielding

The use of a foil-backed gypsum board or another type of foil are common applications for perimeter TEMPEST shielding. AOs and SSMs often prefer the use of a separate foil for ease of installation and inspection. When a separate foil system is employed, the combined use of glue and staples is recommended for permanent installation.

It is important that TEMPEST foil be carefully installed by experienced personnel to avoid damage and/or gaps that would compromise the assembly. Regular engagement with the AO/SSM in discussion, review, inspection, and testing are critical for a successful project completion.

summary

The specialized nature of a secure SCIF environment poses unique design and construction challenges. The nature of the client's specific requirements, location, and engagement with the AO and SSM are essential elements of the early planning process.

Development of a SCIF checklist, understanding client-furnished systems and equipment, and awareness of lessons learned from specific challenges in the design and construction process will be the keys to project success.

steve kimball
PMP, LEED AP

Steve has over 40 years' experience with business leadership and project management. Prior to co-founding emersion, he was the President and CEO for a 100-person A/E firm with offices in Ohio and Florida.