Physical Security of Sensitive Compartmented Information Facilities (SCIF)

NAVFAC NORTHWEST
Presented by: Richard Cofer, P.E.
Naval Facilities Engineering Command Atlantic
Capital Improvements Business Line
Engineering Criteria and Programs

November 14, 2012

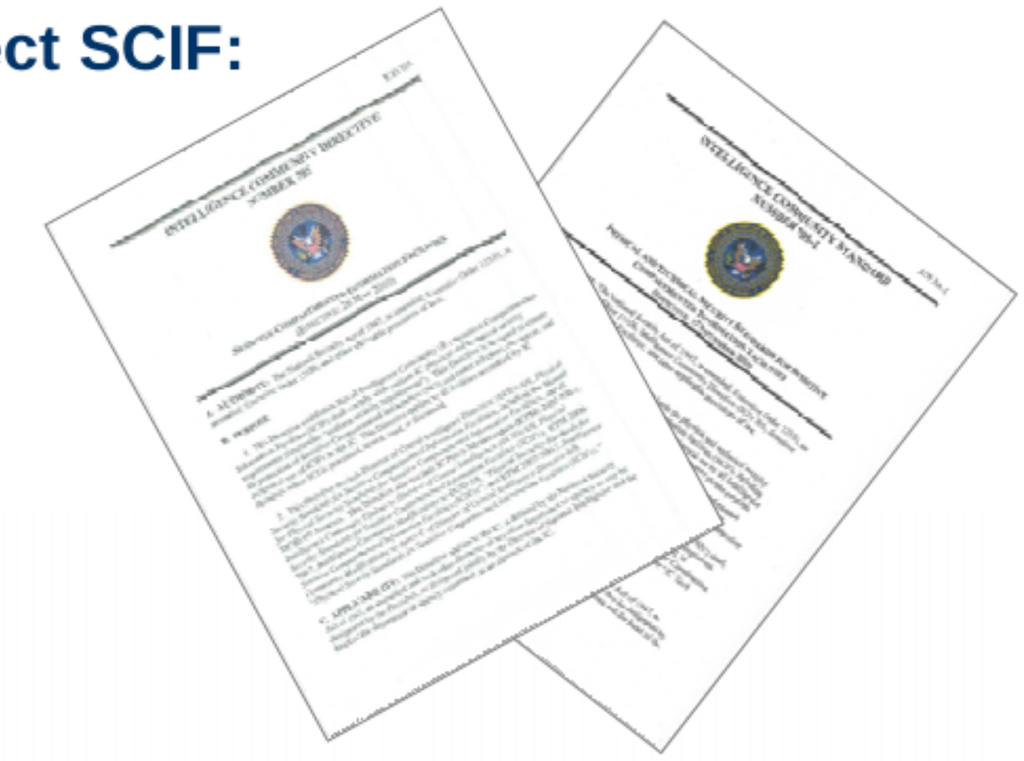
- THIS IS AN INTRODUCTION TO SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIF) AND IS NOT INTENDED TO BE A STEP-BY-STEP INSTRUCTION ON SCIF PLANNING, DESIGN, OR CONSTRUCTION.
- WORK CLOSELY WITH THE DESIGNATED SITE SECURITY MANAGER (SSM) AND THE CERTIFIED TEMPEST TECHNICAL AUTHORITY (CTTA) TO DETERMINE THE REQUIREMENTS FOR EACH PROJECT.
- BOTTOM LINE: PLAN, PROGRAM, DESIGN, AND CONSTRUCT EACH SCIF ON A PROJECT BY PROJECT BASIS.

ICD/ICS Documents

- **POLICY:**
  - **Intelligence Community Directive (ICD) 705 Sensitive Compartment Information Facilities (Effective Date 26 May 2010)**
  - **Intelligence Community Standard Number 705-1 (ICS 705-1) Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (Effective: 17 September 2010)**
  - **Intelligence Community Standard Number 705-2 (ICS 705-2) Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information (Effective: 17 September 2010)**
  - **IC Tech Spec-for ICD/ICS 705: Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (April, 2012)**

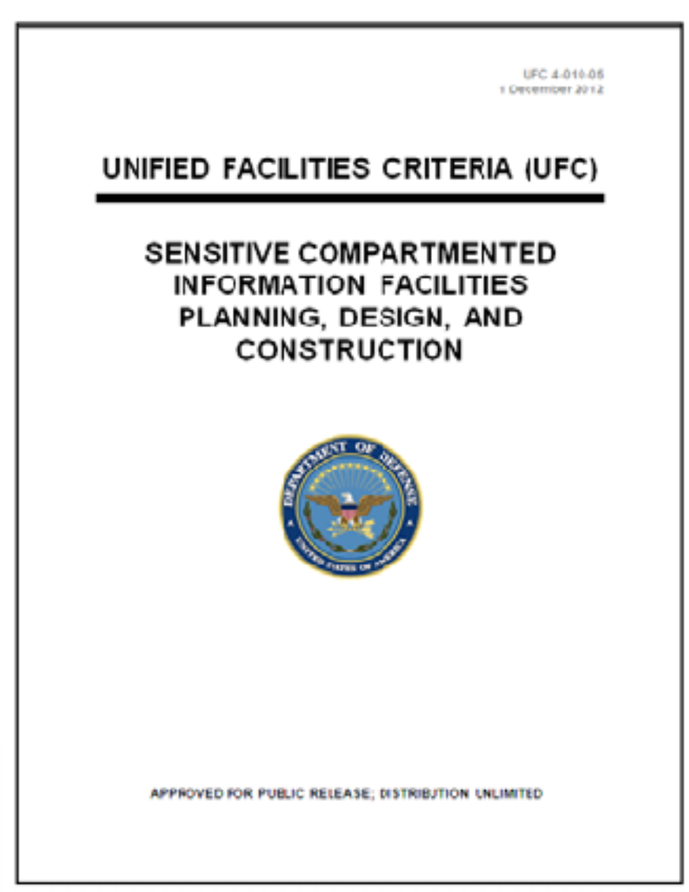
Responsibilities

- As a design and construction agent for the Department of Defense, it is imperative that we understand the requirements contained in ICD 705 and the associated ICS documents and include them in project requirements.
- ICD/ICS Documents effect SCIF:
  - Planning
  - RFP Development
  - Design
  - Construction
  - Accreditation



UFC 4-010-05 Sensitive Compartmented Information Facilities PLANNING, DESIGN, AND CONSTRUCTION

- **PURPOSE:** Provide unified criteria and make the planning, design and construction communities aware of SCIF requirements and ensure appropriate implementation.
- **PREPARING ACTIVITY:** NAVFAC
  - Point of contact: Richard Cofer
  - Author: Richard Cofer
- **CURRENT DOCUMENT STATUS:**
  - Draft awaiting publication, Available on the Whole Building Design Guide Website (www.wbdg.org) 1 December 2012



Sensitive Compartmented Information

Sensitive Compartmented Information (SCI) is classified Secret or Top Secret information that is derived from intelligence sources, methods or analytical processes

- **SCI can only be handled, processed, discussed, or stored in an accredited Sensitive Compartmented Information Facilities (SCIF).**

Sensitive Compartmented Information Facilities

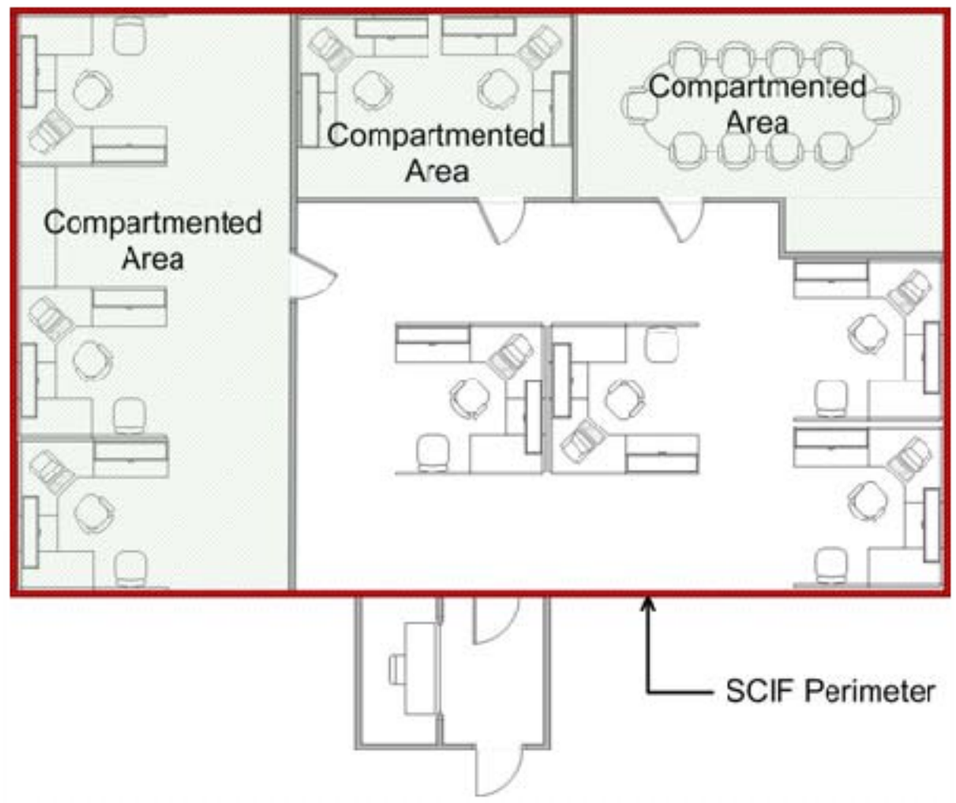
SCIF is an area, room, or building, where sources and methods, including Sensitive Compartmented Information (SCI), is stored, used, processed, or discussed.

–**Typically found in:**

- Command Headquarters
- Operation Centers
- Communication Centers

Sensitive Compartmented Information Facilities

Compartmented Area (CA) is a room, a set of rooms, or an area that provides controlled separation between the compartments within a SCIF.



Accreditation

- **SCIF are established when there is a clear operational requirement that is crucial to the command's mission.**
- **To be operational, a SCIF must be Accredited.**
  - **Accreditation is the formal approval that a SCIF meets the prescribed physical, technical, and operational standards.**
- **If a SCIF cannot be accredited, it cannot be operational… and the command is not mission capable!**

Accreditation Process

- SCIF inspections and evaluations are performed by the Accrediting Official (AO), or designated Site Security Manager (SSM), prior to initial accreditation.
- The SSM is responsible for assembling and submitting documents for AO approval. Documents include, but not be limited to:
  - Fixed Facility Checklist
  - Construction Security Plan
  - TEMPEST countermeasures evaluation from CTTA
  - Standard Operating Procedures
  - Emergency Plans
  - When applicable, waiver request packages.

Fixed Facility Checklist (FFC)

- The FFC is a standardized document used in the process of SCIF accreditation.
  - documents physical, technical, and procedural security information for obtaining an initial or subsequent accreditation.
- To support the accreditation process, the Designer of Record, Project Manager, and Construction Manger will have to provide the AO/SSM site plans, building floorplans, IDS plans, and other information related to perimeter and compartment area wall construction, doors, locks, deadbolts, IDS, telecommunication systems, acoustical protection, and TEMPEST countermeasures.

Construction Security Plan (CSP)

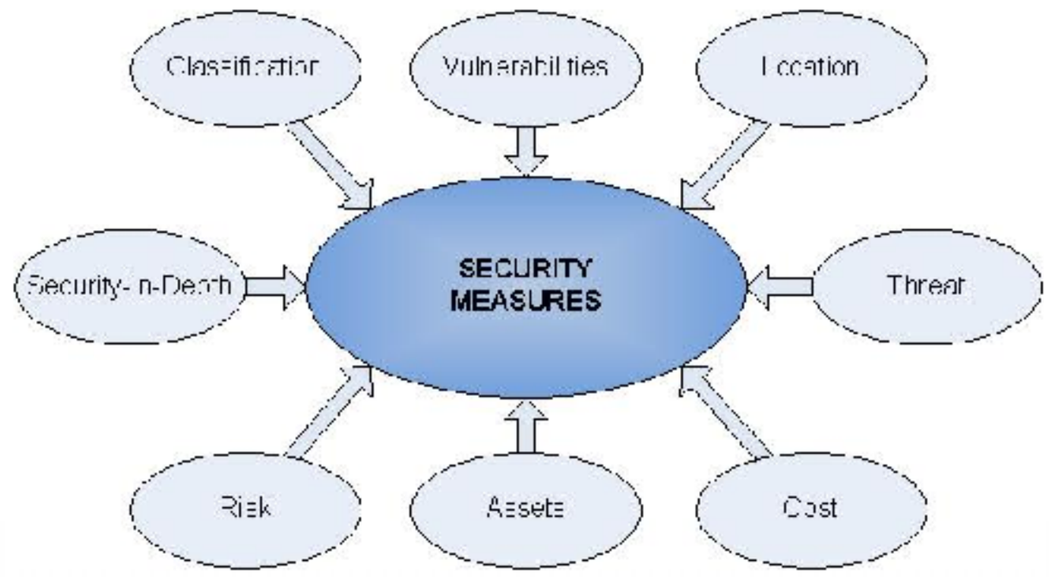
- Each SCIF construction project shall have CSP
- The CSP:
  - Developed by the SSM and approved by the AO.
  - Addresses the application of security to SCIF planning, design, and construction.
  - Format and content is based on extent of SCIF construction and security concerns.
- Policy states the CSP must be approved prior to construction.
- TO LATE! CSP should be approved during the planning process to accurately capture the project costs associated with security.

Determining Project Requirements

- Planner, Designers, and Project Managers must work closely with the supported command, AO's representative (SSM), and the Certified TEMPEST Technical Authority (CTTA) to determine the requirements for each SCIF.
- The AO and the CTTA will use risk management to determine project requirements.
  - Analytical risk management is the process of assessing threats against vulnerabilities and implementing security enhancements to achieve the protection of information and resources at an acceptable level of risk, and within acceptable cost.

Determining Project Requirements

- To determine project requirements the AO will consider factors such as:
  - SCIF Classification
  - SCIF Location
  - Threat
  - Vulnerabilities
  - Security in Depth
  - Type of classified information being processed
  - TEMPEST Review
  - Cost
  - Risk



Classifications of SCIF

- There are six classifications:
  - Secure Working Area (SWA) - Area where SCI is handled, discussed, and/or processed but not stored.
  - Temporary Secure Working Area (TSWA) - Secure working area used less than 40 hours per month.
  - Temporary SCIF - limited time to meet tactical, emergency, or immediate operational requirements.
  - Open Storage - SCI openly stored and processed.
  - Closed Storage - SCI material stored in GSA approved storage containers.
  - Continuous Operation - Staffed and operated 24/7

Classifications of SCIF

- **Closed Storage:**
  - SCI material are stored in GSA approved storage containers when not in use. This includes documents, computer hard drives, and storage media.
- **Open Storage:**
  - SCI may be openly stored and processed and may be left out when not in use.
- **Continuous Operation:**
  - Staffed and operated 24/7. Depending on operational procedures, SCI documents may be left out or stored when not in use.

Classifications of SCIF

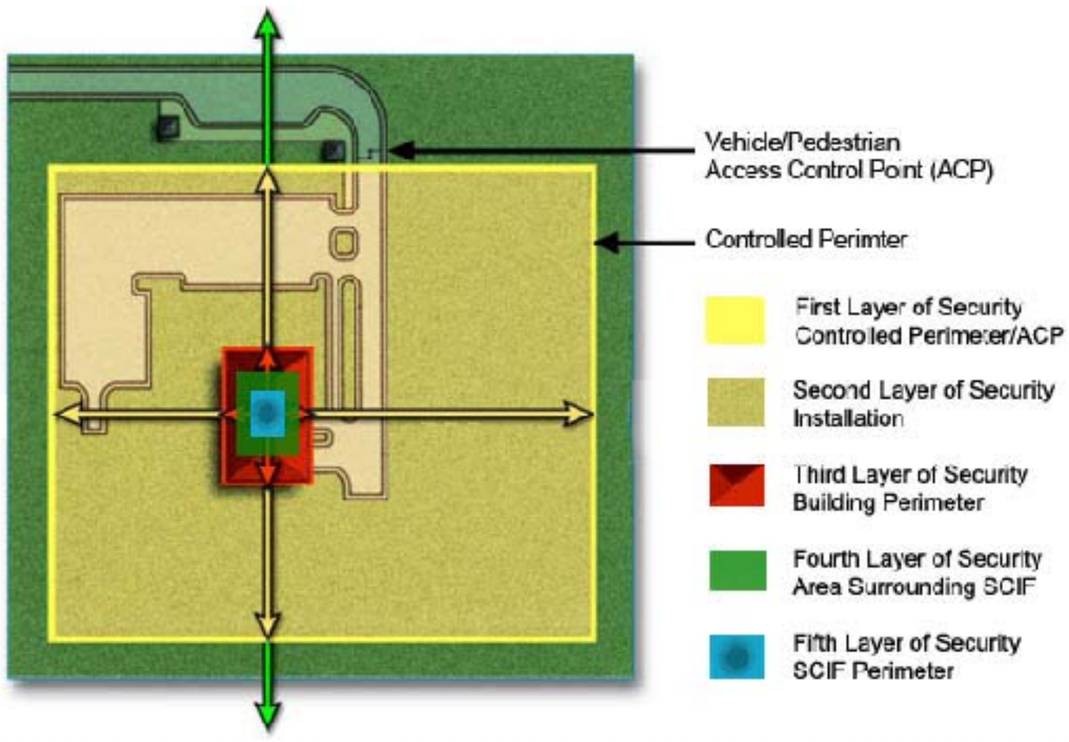
- **Open Storage SCIF outside the United States:**
  - In low and medium threat areas, Open Storage shall only be allowed when the SCIF is under continuous operation or in which the host facility is staffed 24 hours per day by a cleared U.S. presence.
  - In high and critical threat areas, the head of the Intelligence Community (IC) element or CSA shall certify mission essential need, and approve open storage on case-by-case basis.

SCIF Security Requirements

- Where a SCIF is located (threat), how it is classified, security-in-depth, and how it is operated will determine the security requirements.
- For overseas SCIF, AO shall use the Department of State (DoS) Security Environment Threat List (SETL) for the threat ratings. The DoS SETL and its contents are Classified.

SCIF Security Measures

- Security in Depth (SID)
- Security in Depth is a multilayered approach, which effectively employs human and other physical security measures throughout the installation or facility to create a layered defense against potential threats.
- Security in Depth is intended to increase the possibility of detection and response prior to SCIF penetration.
  - SID is required for all SCIF located outside the United States
  - SID inside the United States may decrease the construction requirements



SCIF Security Measures - Security in Depth

- The primary means to achieve Security in Depth :
  - Locate on a Military installation or compounds with a dedicated response force of U.S. persons.
  - Locate within controlled buildings with separate building access controls, alarms, elevator controls, stairwell control required to gain access to building or elevator.
  - Controlled office areas adjacent to or surrounding SCIFs that are protected by alarm.
  - Fenced compound with access controlled vehicle gate and/or pedestrian gate.
- The AO may develop additional strategies to mitigate risk and increase probability of detection of surreptitious entry.

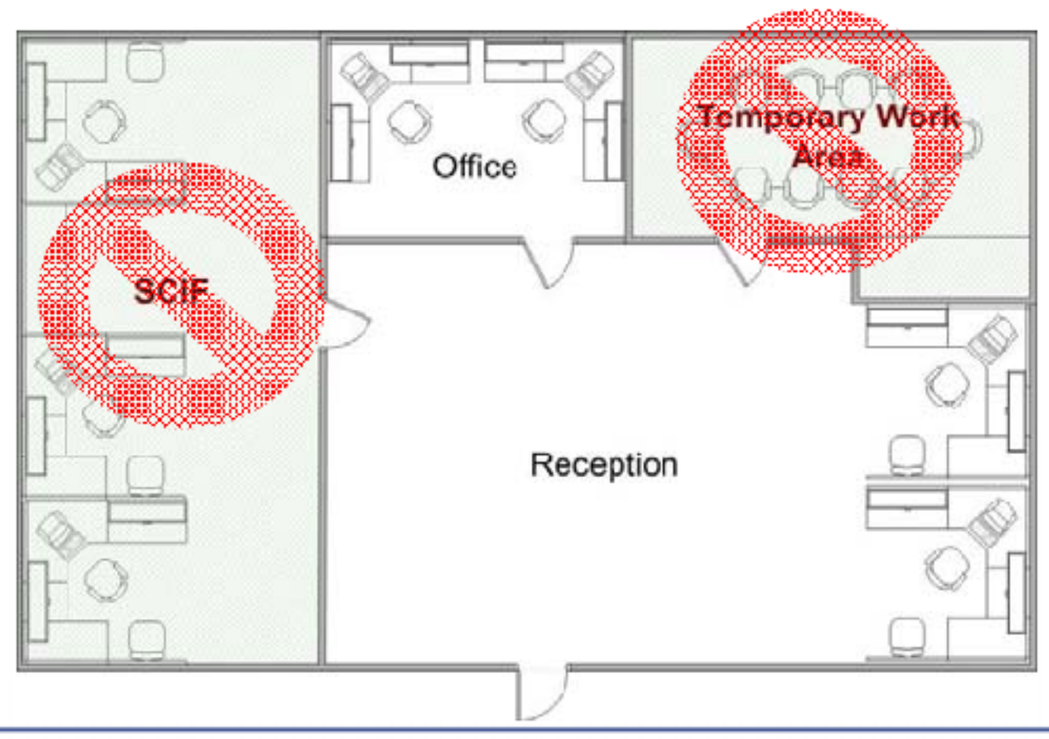
TEMPEST Review

- The CTTA shall conduct a TEMPEST Countermeasure review for each SCIF.
- In conducting the review, the CTTA may evaluate factors such as:
  - Volume and sensitivity of Information processed
  - Profile of Equipment used to process National Security Information (NSI)
  - Location
  - Inspectable space boundary
  - Access control of facility

  } Security- in-Depth
- Project Managers may need to provide site plans and building floorplans to assist CTTA in the evaluation of inspectable space.

Information Security

- Construction plans and all related documents shall be handled and protected in accordance with the Construction Security Plan
- Do not identify SCIF locations on planning or construction documents
- With accrediting official's approval, areas may be identified as "secure area" or "controlled area"



Information Security

- Under no circumstances shall plans or diagrams that are identified for SCI be sent or posted on unprotected information technology systems or Internet venue without encryption.
- Department of State (DoS) Security Environment Threat List (SETL) is classified information.
  - Project Managers, Designers, and contractors may not need to know SETL Category, but they do need to know the resulting mitigation.
  - Do not include the DoS SETL or the SETL Category in project documentation.
  - Do not send or post DoS SETL information on unprotected information technology systems.

SCIF Construction and Design: United States

- SCIF construction and design shall be performed by U.S. companies using U.S. persons
  - U.S. persons is not limited to U.S. Citizens.
  - U.S. person: An individual who has been lawfully admitted for permanent residence as defined in 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by Title 8 U.S.C. 1324b (a)(3), and able to provide two forms of identification listed on Department of Homeland Security Form I-9, Employment Eligibility Verification.
- Intrusion Detection System (IDS) installation and testing shall be performed by U.S. companies using U.S. citizens.
- The AO shall ensure mitigations are implemented when using non-U.S. citizens. These mitigations shall be documented in the CSP.

SCIF Construction and Design: Outside United States

- SCIF design shall be performed by U.S. companies using U.S. Persons.
- General SCIF construction shall be performed using U.S. citizens and U.S. firms.
  - On military facilities, the AO may authorize foreign national citizens or firms to perform general construction of SCIFs. In this situation, the SSM shall prescribe, with AO approval, mitigating strategies. These mitigations shall be documented in the CSP.

SCIF Construction and Design: Outside United States

- **U.S. Top Secret-cleared personnel shall perform finish work in SETL Category I and II countries. U.S. Secret-cleared personnel shall perform finish work in Category III countries escorted or other mitigations are applied as documented in the CSP.**
  - Finish work is defined as closing up walls structures, installing, floating, taping, and sealing wallboard, installing trim, chair rail, molding, flooring, painting, etc.

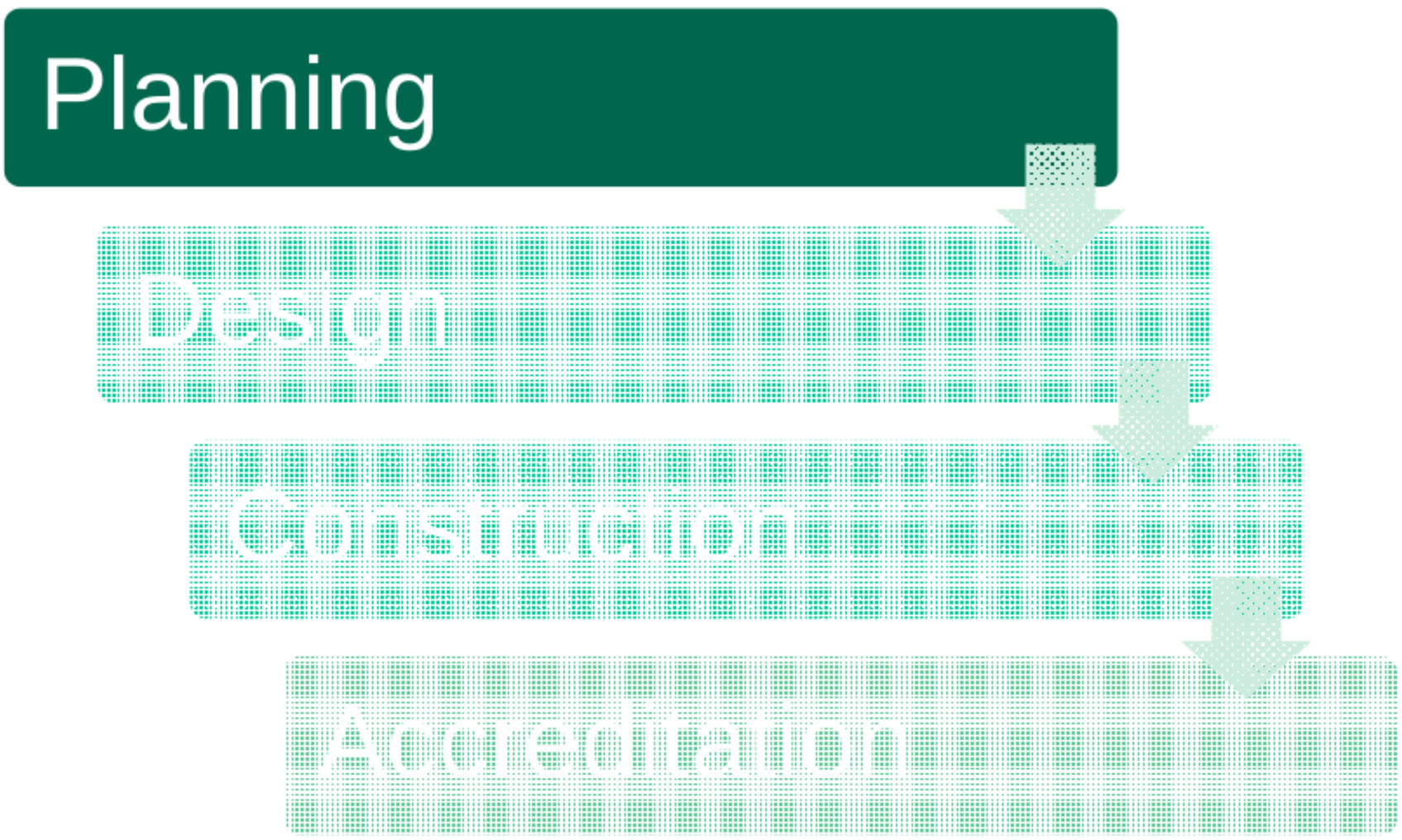
SCIF Construction and Design: Outside United States

- **Intrusion Detection System (IDS) installation and testing shall be performed by personnel who are U.S. TOP SECRET-cleared or U.S. SECRET-cleared and escorted by SCIF personnel.**

SCIF Construction and Design: Outside United States

- **Depending on the location of the SCIF, the Accrediting Official may impose procedures for the procurement, shipping, and storing of SCIF construction materials at the site.**
  - **These procedures must be documented in the Construction Security Plan (CSP).**

SCIF Phases



Planning Team

- Establish an interdisciplinary planning team with local considerations to include the following:
  - Planning
  - Supported Command
  - Site Security Manager (SSM)
  - Certified TEMPEST Technical Authority (CTTA)
  - Communications
  - Security
  - Engineering
  - Cultural resources (if historical building)
- Planning team must work together to determine and document the minimum/enhanced security requirements.

Minimum and Enhanced Security.

- ICS 705-1 and the IC Tech Spec-for ICD/ICS 705 provide the minimum and enhanced security requirements for SCIF.
- Minimum security requirements are generally based on classification and location.
- To implement security enhancements above the minimum, the SSM and CTTA will evaluate the threat, TEMPEST, SID and balance the security enhancements with cost at acceptable risk.

Minimum SCIF Construction Requirements

	CLASSIFICATION	WALL CONSTRUCTION[1]	IDS[3]	ACS[4]	DURESS
INSIDE UNITED STATES	Open Storage without SID[5]	Wall B - Enhanced Wall (Expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	NO
	Open Storage with SID[5]	Wall A - Standard Wall[2]	YES	YES	NO
	Closed Storage	Wall A - Standard Wall[2]	YES	YES	NO
	Continuous Operations	Wall A - Standard Wall[2]	YES	YES	NO
	Secure Working Area (SWA)	Wall A - Standard Wall[2]	YES	YES	NO
OUTSIDE UNITED STATES	SETL Cat I				
	Open Storage	Vault [2]	YES	YES	RECOMMENDED
	Closed Storage	Wall B - Enhanced Wall (Expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	NO
	Continuous Operation	Wall B - Enhanced Wall (expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	YES
	SETL Cat II & III				
	Open Storage	Wall B - Enhanced Wall (expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	RECOMMENDED
	Closed Storage	Wall B - Enhanced Wall (Expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	NO
	Continuous Operation	Wall A - Standard Wall[2]	YES	YES	RECOMMENDED
	Secure Working Area (SWA)	Wall A - Standard Wall[2]	YES	YES	RECOMMENDED

1. Table indicates the minimum wall construction, Accrediting Official shall determine construction requirements based on Risk Assessment.
2. Refer to IC Tech Spec-for ICD/ICS 705 for wall construction definitions and details. Include Radio Frequency (shielding) protection and sound attenuation as required.
3. IDS - Intrusion Detection System
4. ACS - Access Control System: Automated ACS is not required.
5. SID - Security In Depth

Space Configuration

- **If a facility has more than one SCIF, consideration should be given to consolidate into one SCIF with compartmented areas within.**
  - **Any consolidation of spaces will reduce accrediting requirements, initial cost, and the sustainment costs associated with infrastructure and electronic security systems**
- **This must be coordinated with Supported Command and SSM to insure configuration will meet operational and compartmented requirements.**

Historic Preservation

- In a SCIF, every effort should be made to minimize or eliminate windows, especially on the ground floor.
- Windows and doors shall be protected against forced entry and meet the requirements for the SCIF perimeter which may include visual, acoustic and TEMPEST mitigation.
- State Historic Preservation Officers (SHPO) may consider window and door modifications to have an adverse effect but may allow if the impact is minimize and the effect mitigated.
- Planners will need to consult with the State Historic Preservation Office (SHPO) to determine options that meet security requirements and are compatible with the Secretary of the Interior's Standards for Rehabilitation.

SCIF Security Requirements

- Additional considerations that may effect the design and construction are sound ratings of the SCIF perimeter and if TEMPEST countermeasures are required.
  - Any areas designated as non-discussion? Ex: stair wells, vestibules, storage area.
  - What areas will have amplified discussion? (Speakerphones, Video Teleconferencing, or Conference Rooms) What areas will have non-amplified discussion?
  - Is there be there equipment that will be processing national security information (NSI) such as computers, faxes, and printers?
- Again, sound ratings and TEMPEST requirements must be determined, documented, and budgeted for during the planning process!

Construction Security

- For locations outside the United States, the AO may also impose procedures for the procurement, shipping, and storing of construction materials at the site.
- In addition, the AO may require access control to the construction materials and the SCIF construction area. Since these additional security measures may have significant cost impacts on project, they must be determined during project development.

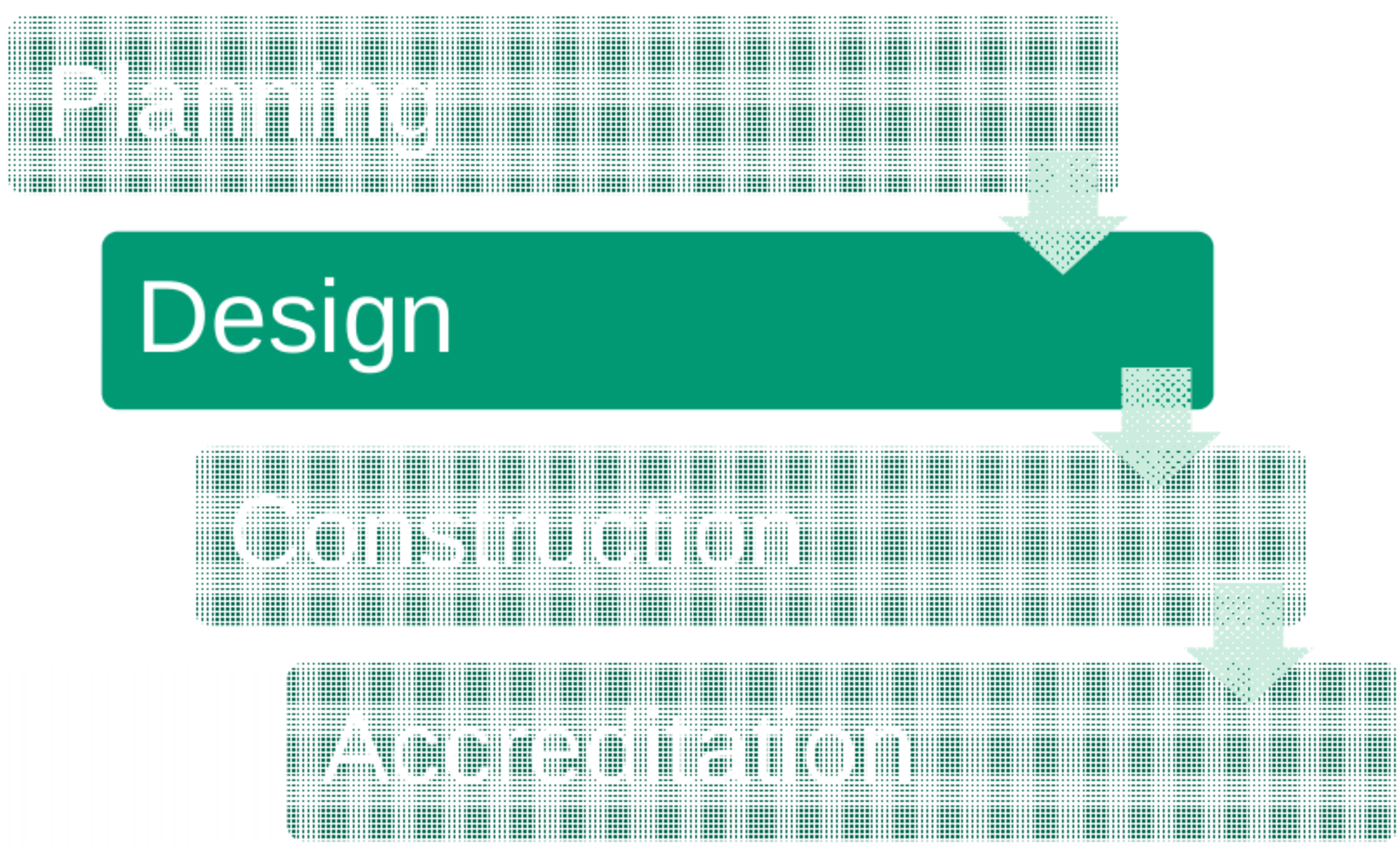
Planning SCIF Security Requirements

- Work with the supported command and the SCIF Accrediting Official to determine and document the classification, operation, and resulting protective measures for each SCIF.
  - Is the SCIF the entire facility or an area within the building?
  - Will there be more than one SCIF, if so how many?
  - What is the classification of each SCIF?
  - Will the SCIF perimeter wall be standard, enhanced, or vault construction?
  - What is the required sound rating for each SCIF perimeter?
  - Are there Compartmented Areas within each SCIF? If so, how many?
  - What is the required sound rating for each Compartmented Area perimeter?

Planning SCIF Security Requirements

- **Continued.**
  - Is there equipment that will be processing national security information (NSI)? Will this result in a TEMPEST requirement? If so, what will be required TEMPEST countermeasures?
  - Are there special procurement, shipping, and storing of SCIF construction materials at the site required? If so, what will be required?
  - Are there additional access control requirements for the construction materials and the SCIF construction area?
- **This must be determined, documented, and budgeted for during the planning process and re-validated during RFP and Design development.**
- **GET A COPY OF THE CSP DURING THE PLANNING PROCESS!**

SCIF Phases

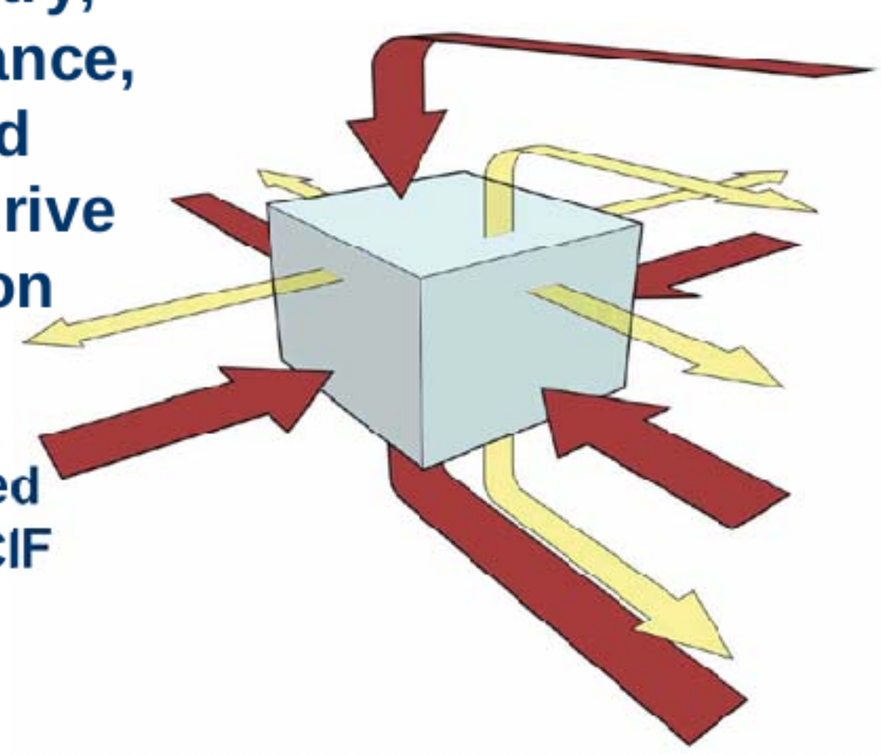


GENERAL DESIGN STRATEGY

- **GENERAL DESIGN STRATEGY**
  - **The general design strategy is defined as the basic approach to developing a protective system to mitigate the effects of that tactic. It governs the general application of construction, building support systems, equipment, manpower, and procedures.**

General Design Strategy

- **SCIF design will vary depending on type of SCIF, location, Security in Depth, and SCI discussion and processing requirements.**
  - **Mitigation against forced entry, covert entry, visual surveillance, acoustic eavesdropping, and electronic emanations will drive SCIF design and construction requirements.**
    - **Designers must take a six-sided approach when developing SCIF requirements.**



General Design Strategy

- **SCIF Perimeter**
  - **The perimeter of the SCIF includes all walls that outline the SCIF confines, floors, ceilings, doors, windows and penetrations by ductwork, pipes, and conduit.**
- **SCIF Perimeter shall provide:**
  - **Resistance to forced entry**
  - **Resistance to covert entry**
  - **Visual evidence of surreptitious penetration****
  - **Sound Attenuation**
  - **Radio Frequency (RF) Shielding (when required)**

**** The SSM must be able to easily detect surreptitious entry to include audio or video probes.**

General Design Strategy

- **Intrusion Detection System**
  - **All Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, shall be protected by IDS, unless continuously occupied.**
    - If the occupants of a continuously occupied SCIF cannot observe all potential entrances to the SCIF, the SCIF shall be equipped with a system to alert occupants of intrusions into the SCIF.
  - **Emergency exit doors shall be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication.**

General Design Strategy

- **Sound Attenuation**
  - **Acoustical protection measures and sound masking systems are designed to protect SCI against being inadvertently overheard by the casual passerby.**
  - **SCIF perimeter shall meet Sound Group 3, unless additional protection is required.**
    - This applies to the entire perimeter of the SCIF to include walls, ceilings, floors, and perimeter penetrations such as conduit, pipe, ducts, doors, and windows.
  - **Compartmented Area: If compartmented areas are required within the SCIF, the dividing office walls must meet Sound Group 3, unless additional protection is required.**
  - **Sound Group 4 is generally required for conference rooms, where multiple people discuss SCI, or other areas where amplified audio is used.**

General Design Strategy

- **TEMPEST**
  - **The Certified TEMPEST Technical Authority (CTTA) has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures.**
  - **Failure to consult the CTTA could result in installation of unnecessary and/or expensive countermeasures or the omission of needed countermeasures.**

General Design Strategy

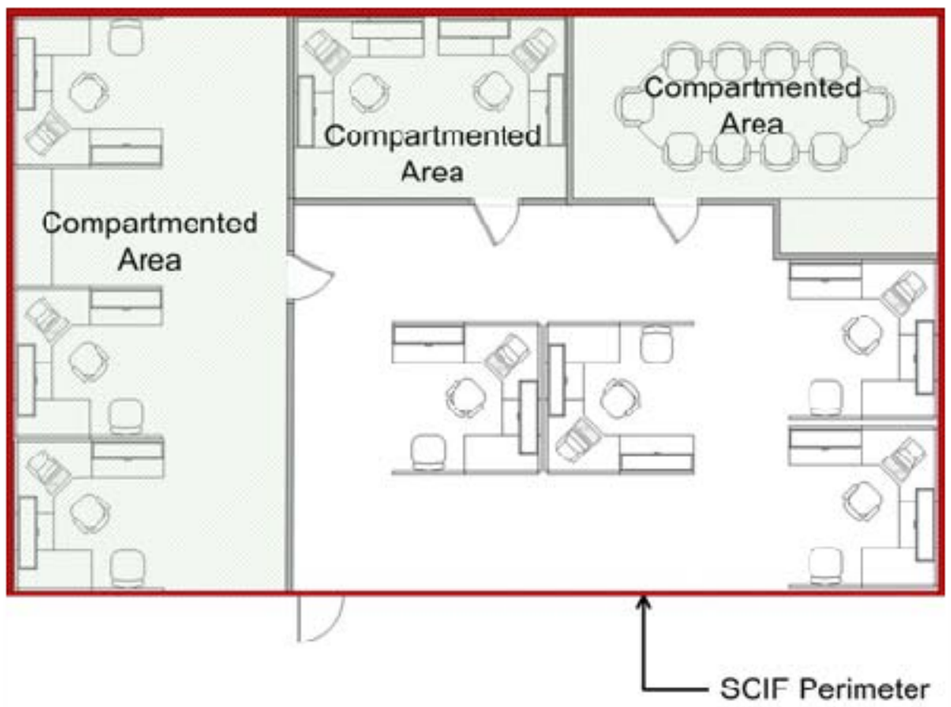
- **TEMPEST (continued)**
  - In general, TEMPEST countermeasures are required when the SCIF contains equipment that will be processing National Security Information (NSI).
  - However, having equipment that will be processing NSI does not necessarily imply the need to implement TEMPEST countermeasures. The CTTA has the responsibility for recommending TEMPEST countermeasures.
  - If required TEMPEST countermeasures are omitted, the facility will not be accredited and the Supported Command will not be mission capable.

SPECIFIC DESIGN STRATEGY

- **SPECIFIC DESIGN STRATEGY**
  - The specific design strategy governs how the general design strategy varies for different levels of protection or threat severity. They may vary by the sophistication of the protective measures and the degree of protection provided. The specific design strategies reflect the degree to which assets will be left vulnerable after the protective system has been employed.
  - ICS 705-1 and the IC Tech Spec for ICD/ICS 705 provide the minimum and enhanced construction requirements for SCIF

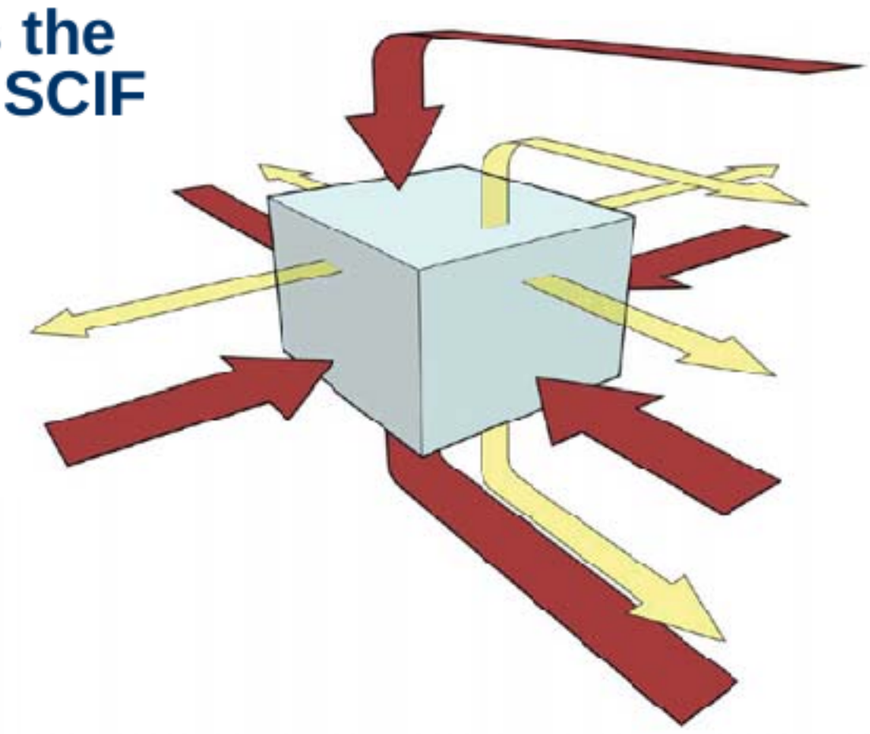
Specific Design Strategy

- **PERIMETER CONSTRUCTION.**
  - **The SCIF and Compartmented Area perimeters and the penetrations to those perimeters are the primary focus of SCIF design.**
  - **Mitigation against forced entry, covert entry, visual surveillance, acoustic eavesdropping, and electronic emanations will drive the design of the perimeter.**



Specific Design Strategy

- **SIX-SIDED APPROACH**
  - **Ceilings and floors are considered part of the perimeter and shall meet the same requirements as the perimeter walls of the SCIF**



Specific Design Strategy

- **Walls:**
  - **Perimeter walls, floor and ceiling shall be permanently and solidly constructed and attached to each other. Walls must go from true floor to true ceiling.**
  - **Seal partition continuously with acoustical foam or sealant (both sides) and finished to match wall wherever it abuts another element such as the floor, ceiling, wall, column, or mullion.**
  - **Seal wall penetrations on both sides with acoustical foam or sealant finished to match wall.**
    - Note: Fire Stop System maybe required for fire rated wall assemblies.
  - **Uniformly finish wall from true floor to true ceiling.**

Specific Design Strategy

Acoustic Protection for SCIF:

- **Acoustical protection measures and sound masking systems are designed to protect SCI against being inadvertently overheard by the casual passerby, not to protect against deliberate interception of audio.**
- **The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC).**
- **Architectural Graphics Standards (AGS) established Sound Groups I through 4, of which Groups 3 and 4 are considered adequate for specific acoustical security requirements for SCIF construction. Per AGS:**
  - Sound Group 3 – (STC of 45) or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.
  - Sound Group 4 – (STC of 50) or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume, can be heard only faintly or not at all.

Specific Design Strategy

- **Acoustic Protection for SCIF**
  - **The amount of sound energy reduction may vary according to individual facility requirements. However, Sound Group ratings shall be used to describe the effectiveness of SCIF acoustical security measures afforded by various wall materials and other building components.**
    - SCIF Perimeter walls shall meet Sound Group 3, unless additional protection is required for amplified sound.
    - Comparmented Area Walls: If compartmented areas are required within the SCIF, the dividing office walls must meet Sound Group 3, unless additional protection is required for amplified sound.
  - **ASTM E-90, Standard Method for Laboratory Measurement of Airborne Sound Transmission.**

Specific Design Strategy

- **Sound Attenuation**
  - **Conference rooms, where multiple people discuss SCI, or other areas where amplified audio is used shall meet Sound Group 4 performance criteria.**
    - This applies to the entire perimeter of the space to include walls and wall penetrations such as ducts, doors, and windows.

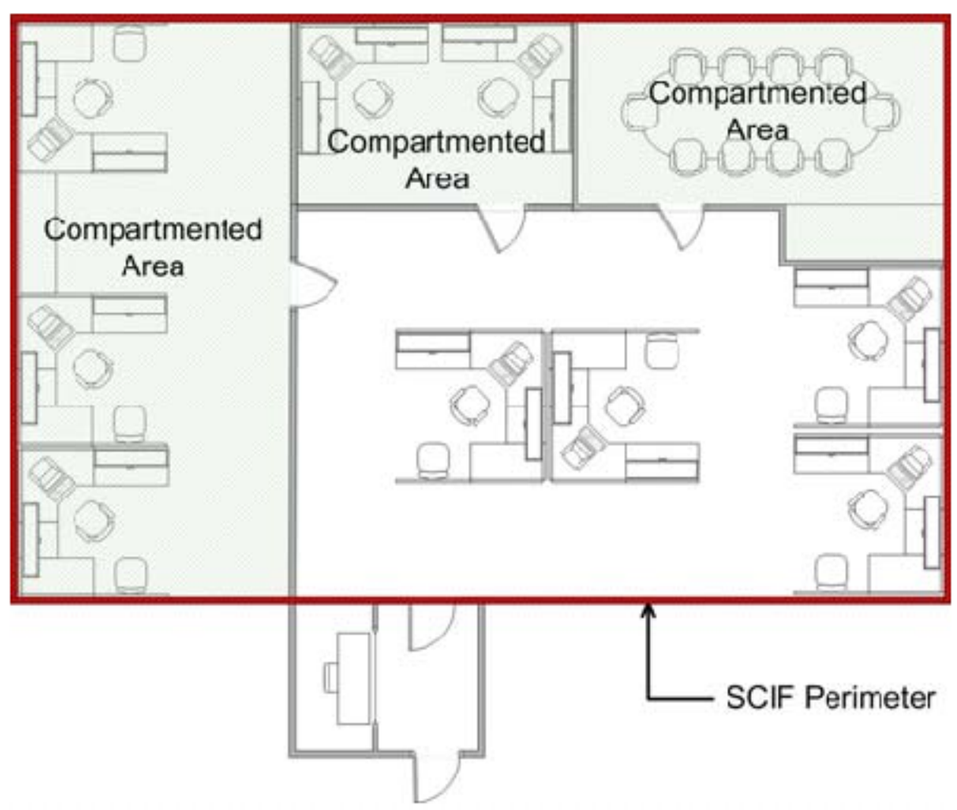
Specific Design Strategy

- **Acoustic Protection for SCIF**
  - **When normal construction and baffling measures have been determined to be inadequate for meeting Sound Group 3 or 4, as appropriate, sound masking shall be provided.**
    - A sound masking system may utilize a noise generator as a noise source, an amplifier, and speakers or transducers located on the perimeter of the SCIF.
    - When required, provide sound masking devices at penetrations to the SCIF perimeter such as doors and duct penetrations.

TRANSDUCER

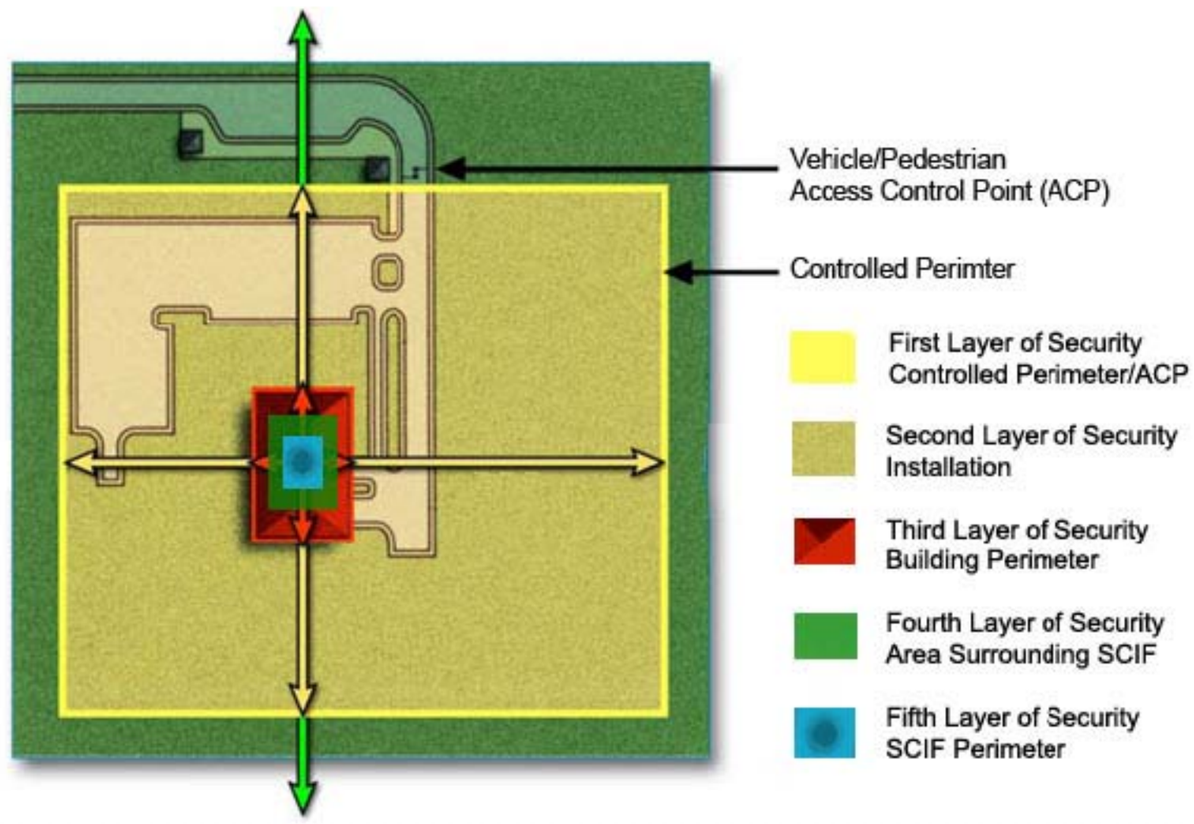
Specific Design Strategy

- **VESTIBULE.**
  - **When practical, the entrance into a SCIF should incorporate a vestibule to preclude visual observation and enhance acoustic protection.**



Specific Design Strategy

- **ADJACENT SPACE.**
  - **To increase Security in Depth (SID), locate other areas that require access control adjacent to or surrounding SCIF.**



Specific Design Strategy

- **Wall A (Standard Wall) - Sound Group 3 (STC 45 or better)**
  - **3-5/8" metal or 2 x 4 wood studs**
  - **Continuous runners (same gauge as studs) attached to true floor and true ceiling.**
  - **Three layers of 5/8 inch foiled back Type X gypsum, one layer on the outside and two on the inside of the SCIF wall. When R-foil or foil back gypsum is employed, it shall be placed inside the SCIF between the first and second layer of gypsum board. Stagger interior seams, mount one layer vertically and one layer horizontally to ensure seams do not align.**
  - **Provide acoustic fill between studs in a manner to prevent slippage.**

Wall A (Standard Wall) Sound Group 3 (STC 45 or better)

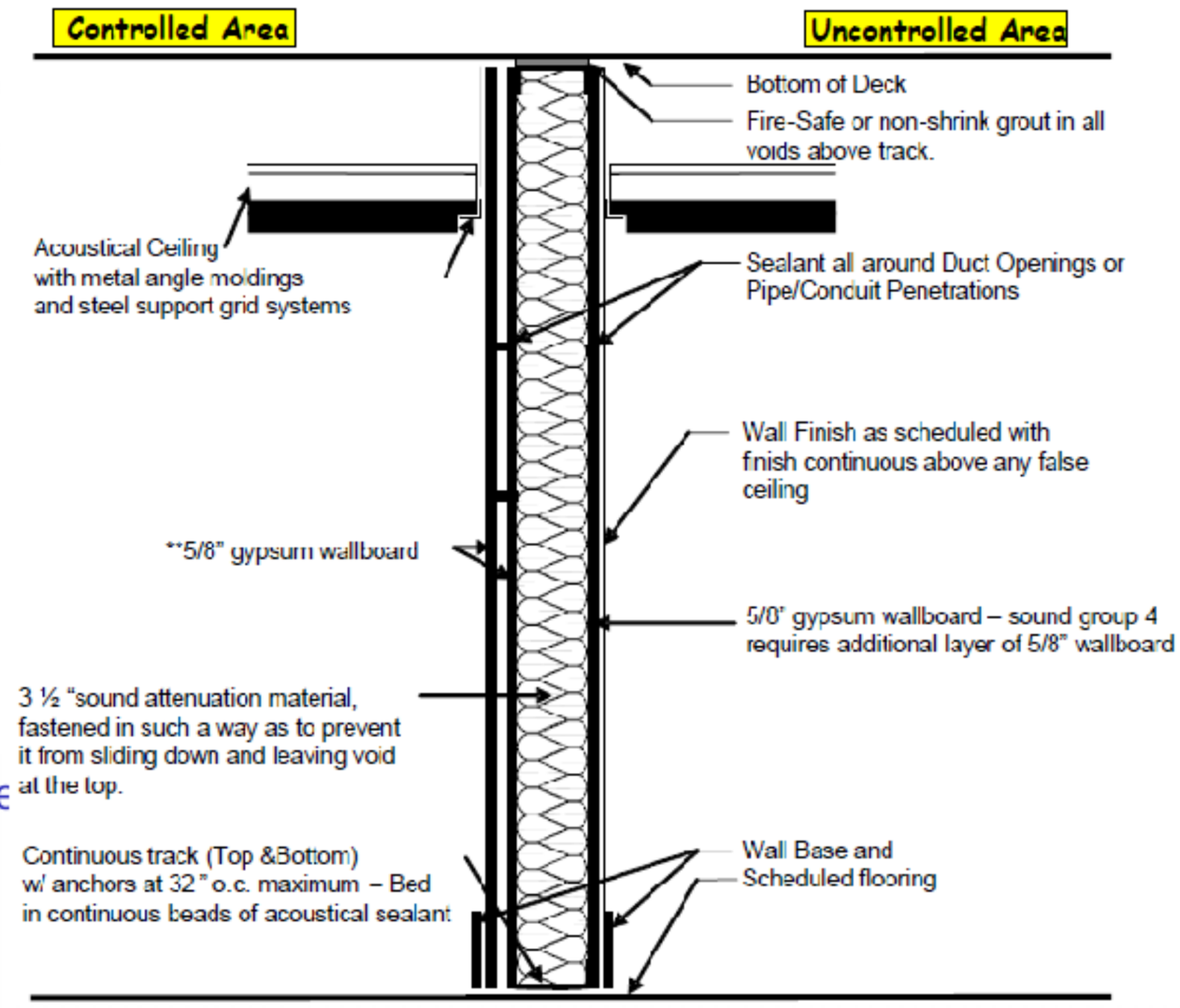
Only for sound attenuation of wall: Don't Forget Ceiling and Floors

* Sound Group 4 wall requires four layers of 5/8" GWB and special acoustic door or vestibule.

** When required by CTTA. Foil backed GWB or a layer of approved Ultra Radiant R-Foil may be used.

***Depending on height, true floor to true ceiling and weight, metal studs shall be in a range of 20 gauge to 16 gauge.

Any utilities required on the perimeter wall shall be surface mounted.



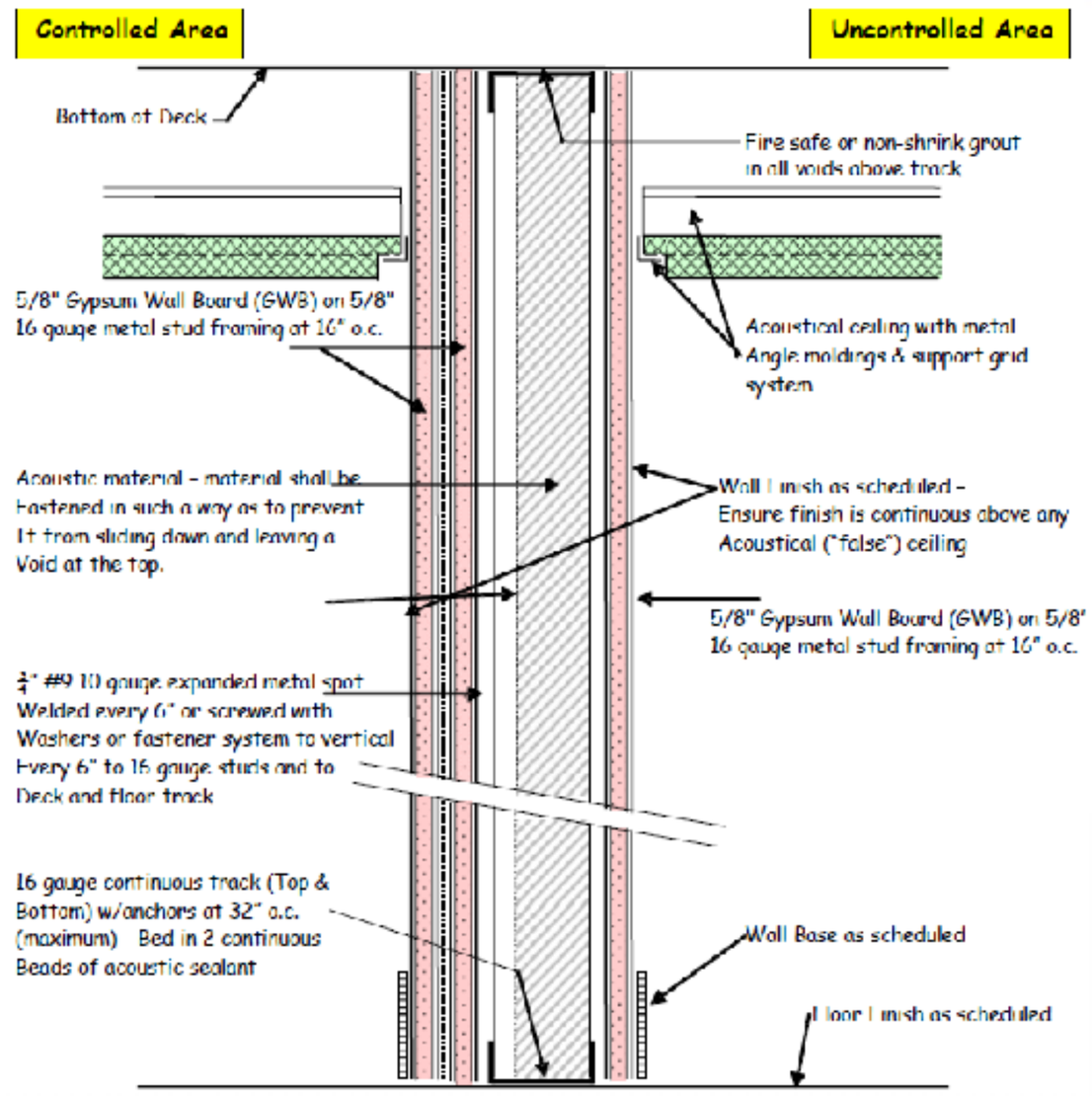
Specific Design Strategy

- **Wall B (Enhanced Wall) Expanded Metal Sound Group 3 (STC 45 or better):**
  - **Same as Wall A except:**
    - **Metal studs and runners shall be 16 gauge**
    - **Wood or Metal Studs shall be 16" on center**
    - **Provide ¾" #9 (10 gauge) case hardened expanded metal affixed to the interior side of SCIF perimeter studs.**

Wall B (Enhanced Wall) Sound Group 3 (STC 45 or Better) Expanded Metal

Only for sound attenuation of wall: Don't Forget Ceiling and Floors

- **This Detail is intended for "New Construction": AO must approve any variations in expanded metal use.**
- **CTTA recommended countermeasures (foil bracketed wallboard or R-foil shall be installed in accordance with Best Practices Guidelines for Architectural Frequency Shielding.**
- **Any utilities required on wall shall be surface mounted.**



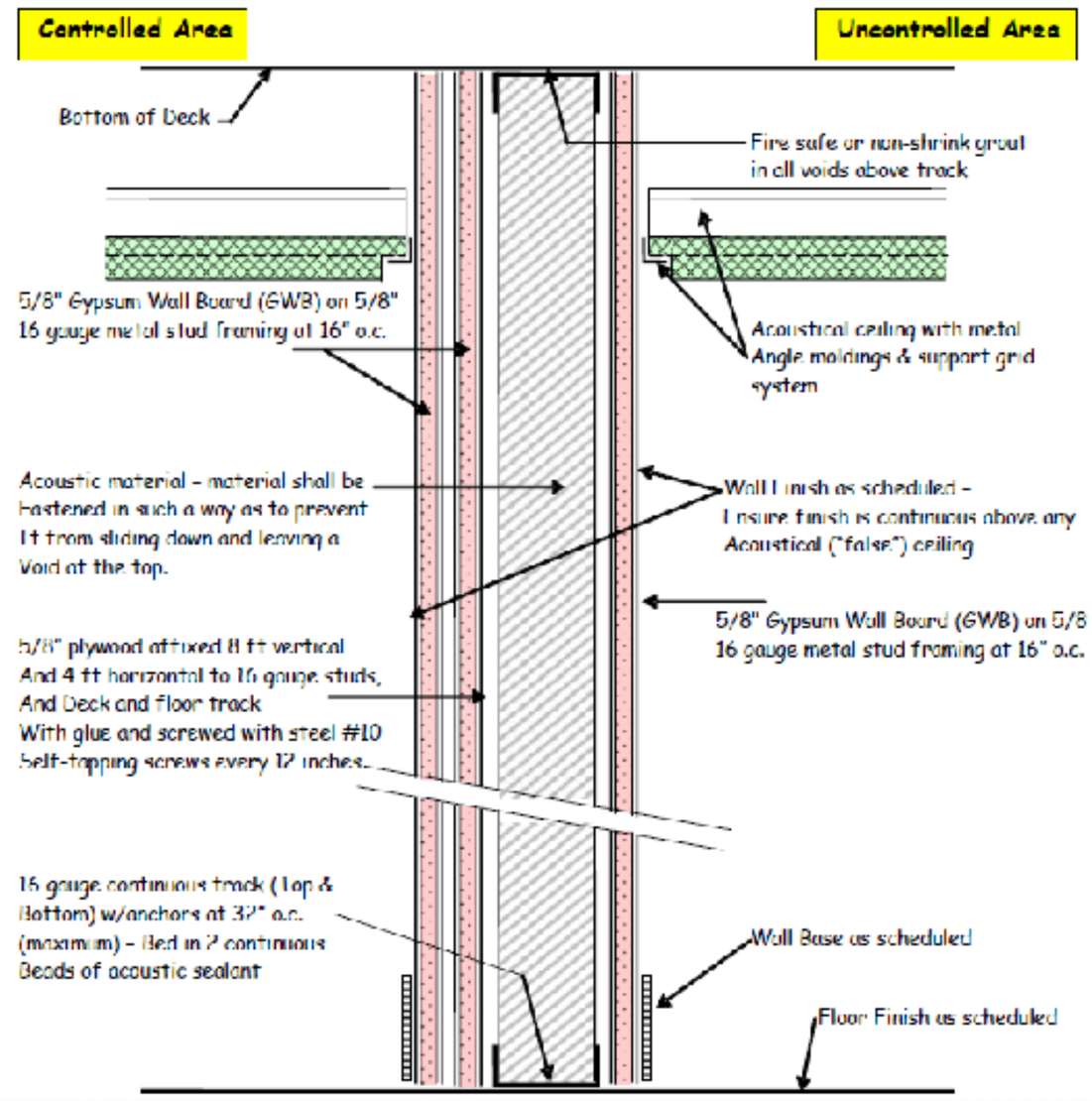
Specific Design Strategy

- **Wall C (Enhanced Wall) Perimeter walls with Fire Rated Plywood:**
  - **Wall assembly the same as Wall B except:**
  - **One layer of 5/8" thick "fire retardant" plywood shall be substituted for expanded metal and first interior layer of gypsum board on the interior side of the SCIF wall assembly.**
  - **The plywood shall be continuously glued and screwed to the studs every 12 inches along the length of each stud.**

Wall C (Standard Wall) Sound Group 3
"Fire Rated" Plywood

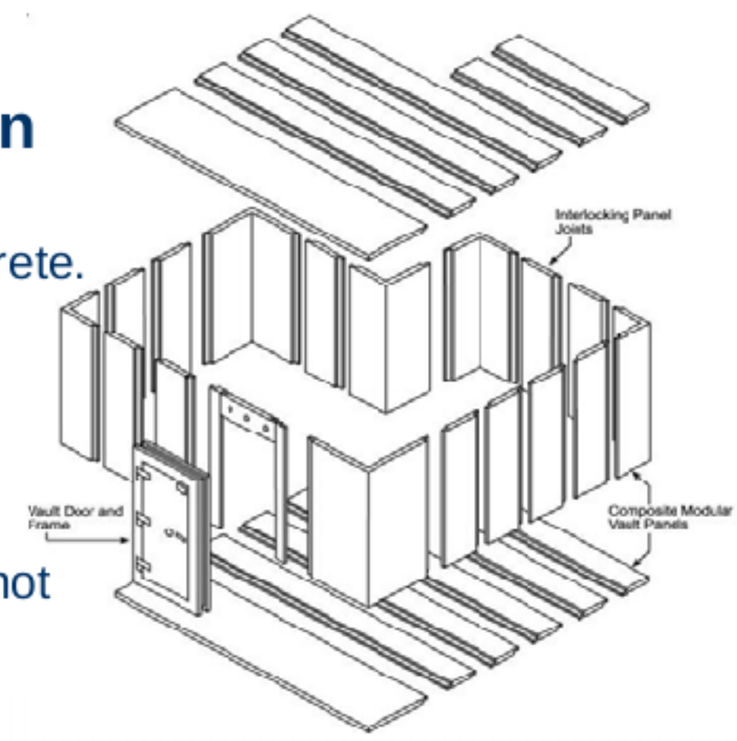
Only for sound attenuation of wall: Don't Forget Ceiling and Floors

- **This Detail is intended for "New Construction": AO must approve any variations in expanded metal use.**
- **CTTA recommended countermeasures (foil bracketed wallboard or R-foil shall be installed in accordance with Best Practices Guidelines for Architectural Frequency Shielding.**
- **Any utilities required on wall shall be surface mounted.**



Specific Design Strategy

- **Minimum requirements for Vault walls:**
  - **Reinforced Concrete Construction**
    - Walls, floor, and ceiling will be a minimum thickness of eight inches of reinforced concrete.
  - **GSA-approved modular vaults**
    - Federal Specification FF-V-2737
  - **Steel-lined Construction**
    - Where unique structural circumstances do not permit construction of a concrete vault



- **Minimum requirements for doors**
  - **GSA-approved Class 5 or Class 8 vault door**
  - **Within the US, a Class 6 vault door is acceptable**

Specific Design Strategy

- Utilities such as power, signal, or plumbing on the interior of a perimeter/compartmented wall treated for acoustic or RF shall be surface mounted or a furred out wall shall be constructed for routing of the utilities.
  - If the construction of an additional wall is used, gypsum board may be 3/8 inch and shall terminate above the false ceiling.
  - No recessed fire extinguisher cabinets on walls treated for acoustic or RF.

Specific Design Strategy

Specific Design Strategy

- Ducts, conduits, pipes, or anything that penetrate the SCIF perimeter present a vulnerability that needs to be addressed.
- Penetrations of SCIF perimeter shall be kept to a minimum.
- HVAC ducts: Provide a nonconductive break (flex connection) using material appropriate for the climate, for a 2- to 6-inch section of the duct adjacent to the duct penetration through the SCIF perimeter wall (inside wall).

Specific Design Strategy

- All metallic penetrations through SCIF walls may be considered carriers of compromising emanations (CE) and pose TEMPEST hazards. Unless directed otherwise by the CTTA:
  - Metallic conduit: install dielectric union ~~or a dissimilar metal fitting/union~~ adjacent to the pipe penetration through the SCIF perimeter wall (inside wall), or ground the conduit using a no. 4 wire (0.2043-diameter copper wire) to the building ground.
  - Metallic sprinkler (fire suppression) pipes: provide a UL Listed dielectric union inside the SCIF perimeter adjacent to the penetration, or ground using a no. 4 wire (0.2043-diameter copper wire) to the building ground.
  - Mechanical system refrigerant lines: ground the line using a no. 4 wire (0.2043-diameter copper wire) to the building ground.

Specific Design Strategy

- **VENT, PIPE, AND DUCT OPENINGS :**
  - **All vents or duct openings exceeding 96 square inches that penetrate the perimeter walls of a SCIF shall be protected with permanently affixed bars or grills.**
    - If one dimension of the penetration measures less than 6 inches, bars or grills are not required.

Specific Design Strategy

- **Provide an accessible 12” x 12” access panel in the bottom within the perimeter of the SCIF to allow visual inspection of the vent or duct (greater than 96 sq. in.)**
  - **If the area outside the SCIF is controlled (SECRET or equivalent proprietary space), the inspection port may be installed outside the perimeter of the SCIF, and be secured with a GSA approved high security lock.**

MANBARS

INSPECTION PORT

Specific Design Strategy

- **Seal wall penetrations on both sides with acoustical foam or sealant finished to match wall.**
  - Note: Through Penetration Fire Stop System maybe required for fire rated wall assemblies.

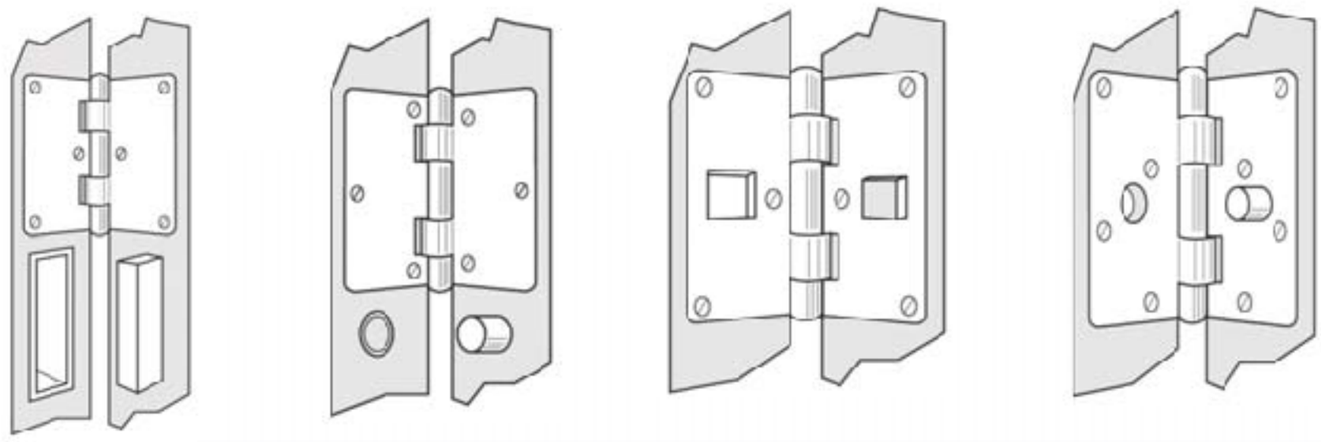
NOTE: PICTURE TAKEN PRIOR TO PAINTING

Specific Design Strategy

- **Utilities (power and signal) should enter the SCIF at a single point.**
  - **All utility penetrations must be sealed to mitigate acoustic emanations and covert entry.**
  - **It is permissible to install an additional conduit penetration for future utility expansion.**
    - **Metal conduit caps shall be spot welded and painted.**
    - **PVC shall have the cap permanently glued to the pipe.**
- **Utilities servicing areas other than SCIF shall not transit the SCIF Perimeter unless mitigation is provided.**

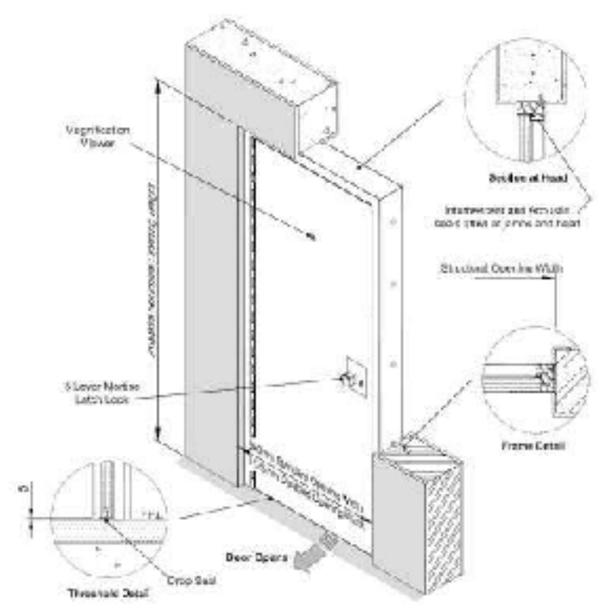
Specific Design Strategy

- **SCIF PERIMETER DOORS: Shall be equipped with an automatic door closer with controls to prevent unauthorized entry.**
  - Perimeter doors with day access controls for SCIF residents shall be dead bolted at night or meet the primary entrance door requirements.
  - Hinge pins on SCIF doors that open into an uncontrolled area shall be modified to prevent removal of the door, e.g., welded, set screws, etc.



Specific Design Strategy

- **SCIF PERIMETER DOORS (continued):**
  - SCIF doors and frame assemblies shall meet acoustic requirements (vestibule of two doors may be used) unless declared a non-discussion area.
  - A steel door shall be used when RF shielding is required.
  - Perimeter doors shall comply with U.S. National Fire, and the Architectural Barriers Act Accessibility Guidelines (ABAG) .
  - All perimeter doors shall be alarmed.



Specific Design Strategy

- Sound Attenuation and Forced Entry govern door material and door hardware.
- From ICS guidelines:
  - Wood doors shall have:
    - 1 ¾ inch thick solid wood core (wood stave)
    - Acoustic seals
    - Frames with a sill designed for the acoustic system used in the door.
  - Steel doors shall have:
    - 1 ¾ inch thick - face steel equal to 18 gauge
    - Acoustic seals and sweep
    - Hinges reinforced to 7 gauge
    - Door closure reinforced to 12 gauge
    - Lock area predrilled and/or reinforced to 10 gauge

Specific Design Strategy

- 1 ¾ inch thick - face steel equal to 18 gauge over wood or composite materials will not meet STC 45 rating.
  - 1 ¾" Solid core door – factory sealed
    - Best STC obtainable = 38 STC
  - 1 ¾" Solid core door – field assembly
    - Best STC obtainable = 35 STC
  - 2" Solid core door – factory sealed
    - Best STC obtainable = 42 STC

- Unsealed gaps and clearances in door assemblies cancel the soundproofing qualities of acoustical doors. A 1% opening around a door will allow up to 50% of the sound to pass through.
- Consider this: A 1/8-inch opening around all four sides of a door will reduce the effective rating of an STC 52 door down to an STC 21.
- In order to obtain a true STC 45 or 50 rated door specify a acoustical assembly to include door, seals, hinges, and threshold.

Specific Design Strategy

- PRIMARY ENTRANCE TO SCIF
  - Only one primary SCIF entrance where visitor control is conducted.
  - Should incorporate a vestibule to preclude visual observation and enhance acoustic protection.
  - Shall be equipped with an approved automated access control device.
  - Shall be equipped with a GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L- 2890 and combination lock meeting Federal Specification FF-L 2740A. Note: FF-L-2890 requires FF-L 2740A Combination lock.
- DO NOT SPECIFY AN X-09 or CDX-09 LOCKS!
  - THESE ARE TRADEMARKS. SPECIFY HARDWARE TO MEET FEDERAL SPECIFICATION FF-L-2890

Specific Design Strategy

- ROLL-UP DOORS: Shall only be located in an area of the SCIF that is a non discussion area due to the inability to treat for acoustics. Roll-up doors shall be
  - 18 gauge or greater and
  - Secured with dead bolts on each side of the door.
- DOUBLE DOORS: Because of acoustical concerns, double doors are not preferred. If double doors are used:
  - One side shall be secured top and bottom with deadbolts
  - Have an astragal strip attached to the fixed door to prevent observation of the SCIF through the opening between the doors.
  - Each door shall be alarmed (have a balanced magnetic switch).
  - A GSA approved lock shall be installed on the moving door.

Specific Design Strategy

- **EMERGENCY EXIT DOORS: Shall meet perimeter door requirements and:**
  - **Have no exterior hardware**
  - **Secured with deadlocking panic hardware**
  - **Alarmed 24/7 and equipped with a local annunciation**
  - **Delayed-egress may be permitted with NFPA 101 compliance.**

Specific Design Strategy

- **WINDOWS:**
  - **No windows are preferred. Therefore, every effort should be made to minimize or eliminate windows in the SCIF, especially on the ground floor.**
  - **Windows shall be non-opening.**
  - **Windows shall provide RF (when required), visual, and acoustic protection.**
  - **All windows less than 18 feet above the ground or from the nearest platform such as canopy or mechanical equipment which affords access to the window (measured from the bottom of the window) shall:**
    - Meet the standards of the SCIF perimeter
    - Be protected against forced entry.
    - Be alarmed
  - **SCIF windows located above 18 feet shall be permanently sealed or equipped with an approved locking device to preclude opening.**

Specific Design Strategy

- **Flashing or Rotating Light:**
  - Per DoDM 5105.21 Vol 2 *Department of Defense Sensitive Compartmented Information Administrative Security Manual:*
    - SCIF personnel must be informed when non-SCI-indoctrinated personnel have entered and departed the SCIF. This may be accomplished either verbally or through visual notification methods.
    - When used , lights shall be placed to ensure visual observation by SCIF personnel
    - Controls shall be placed by each door including emergency exit doors.

- **Fire Alarm and Mass Notification System (MNS)**
  - **The introduction of electronic systems that have components outside the SCIF should be avoided. Speakers or other transducers, which are part of a system that is not wholly contained in the SCIF, are sometimes required to be in the SCIF by Life Safety regulations and Antiterrorism Standards. In such instances, the system can be introduced if protected as follows:**
    - TEMPEST concerns may require electronic isolation, validate requirements with CTTA.
    - All incoming wiring shall penetrate the SCIF perimeter at one point.
    - In systems that require notification only, the system shall have a high gain buffer amplifier.
    - In systems that require two-way communication, the system shall have electronic isolation. SCIF occupants should be alerted when the system is activated.
    - When required, all electronic isolation components shall be installed within the SCIF as near to the point of SCIF penetration as possible.

Specific Design Strategy

- **Intrusion Detection System**
  - **IDS installation, related components, and monitoring stations shall comply with Underwriters Laboratories (UL) 2050 Extent 3 standards.**
  - **NOTE: Systems developed and used exclusively by the U.S. Government do not require UL certification but shall comply with UL 2050 Extent 3 standards for installation.**
  - **UL 2050 is the National Industrial Security Systems standard.**
    - UL 2050 is not applicable to SCIF operated by the DoD
    - UL 2050 materials are restricted and only distributed to those demonstrating relevant national industrial security involvement.

Specific Design Strategy

- **UL 2050 Extent 3 standards for installation**
  - **UL 2050 implements UL 681, *Installation and Classification of Burglar and Holdup Alarm Systems for alarm system installation*.**
  - **UL 681 is available to NAVFAC personnel through the Information Handling System (IHS) on the Whole Building Design Guide Website: http://www.wbdg.org/references/ngstandards.php?a=nav**

Specific Design Strategy

- **Intrusion Detection System Requirements:**
  - The IDS shall be independent of systems safeguarding other facilities and compatible with Installation's central monitoring system.
  - All Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, shall be protected by IDS, unless continuously occupied
  - Emergency exit doors shall be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication.
  - Provide point sensors on all windows, doors, and man-passable openings.
  - Provide motion sensors within SCIF to protect all windows, doors, and man-passable openings and detect movement within the SCIF to include compartmented areas.

Specific Design Strategy

- **Intrusion Detection System Requirements**
  - If a monitoring station is responsible for more than one IDS, there shall be an audible and visible annunciation for each IDS.
  - IDS shall be separate from and independent of other systems such as fire alarm and building control systems.
  - If the IDS incorporates an access control system (ACS), notifications from the access control system shall be subordinate in priority to IDS alarms.
  - Motion detection sensors are not required above false ceilings or below false floors. However, these detectors may be required by the AO for critical and high threat facilities outside the U.S.

Specific Design Strategy

- **Intrusion Detection System Sensors**
  - **Motion Detection Sensors**
    - Shall be UL 639 listed
    - Dual-Technology Sensors are authorized when each technology transmits alarm conditions independent of the other technology.
  - **Point Sensors**
    - Shall be UL 634 high security switches (HSS) level 1 or 2. HSS Level 2 is preferred.
    - Balanced Magnetic Switches meet HSS Level 2.

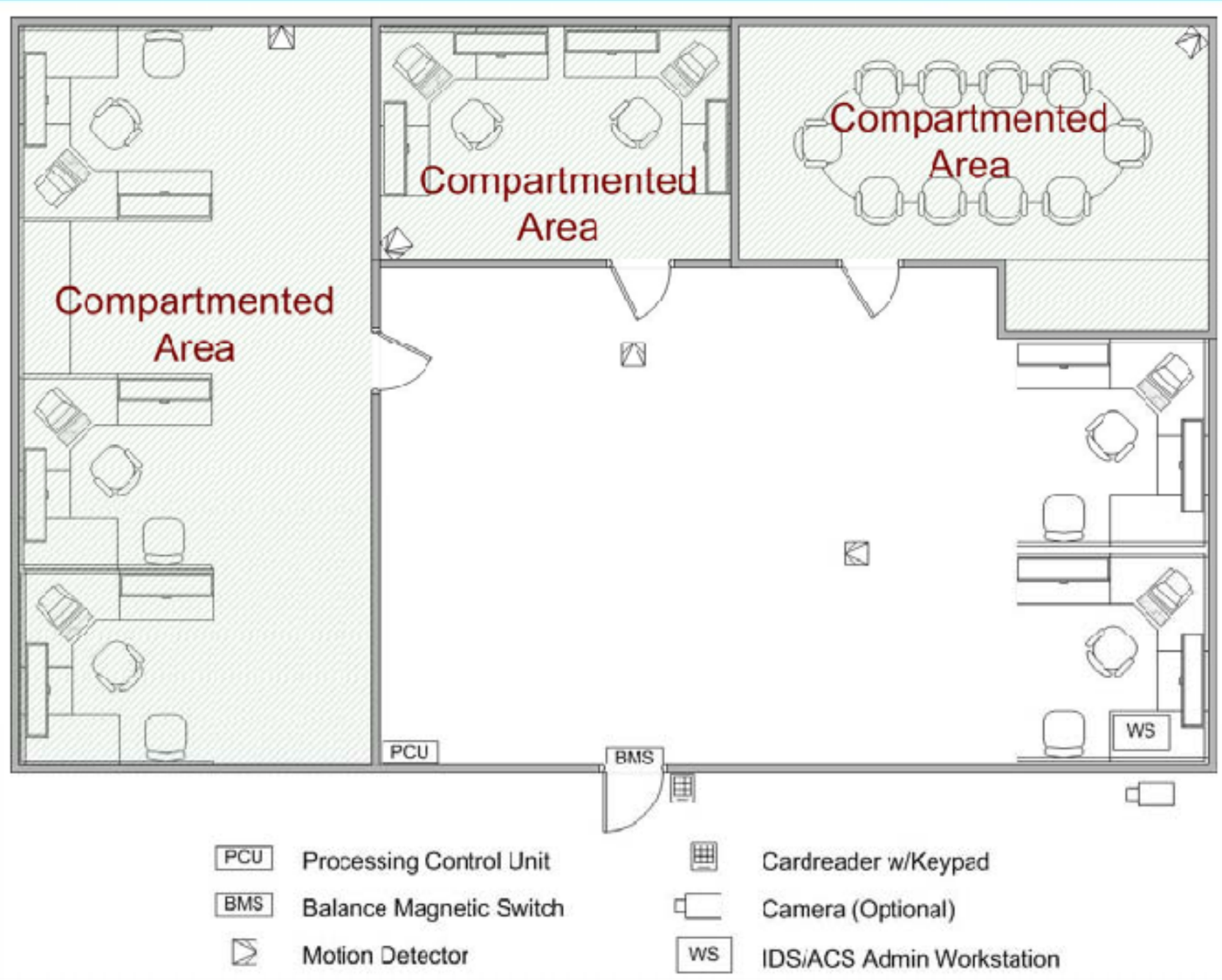
Specific Design Strategy

- **Intrusion Detection System Requirements:**
  - **Premise Control Unit (PCU):** Must be located within the SCIF
    - PCU is a term used to describe a specific IDS control panel.
    - Only SCIF personnel may initiate changes in access modes. Operation of the access/secure mode shall be restricted by using a device or procedure that validates authorized use.
  - **Tamper protection:** Tamper protection for IDS can be physical protection, line supervision, encryption, and/or tamper alarming of enclosures and components.
    - Sensor Cabling Security: Cabling between the sensors and the PCU shall be dedicated to the IDE and contained within the SCIF. If the wiring cannot be contained within the SCIF, such cabling shall be encrypted and protected from tamper.
    - External Transmission Line Security: When any IDS transmission line leaves a SCIF, line security shall be employed.
  - Refer to UFC 4-021-01NF, Security Engineering Electronic Security Systems for more on system design including tamper protection.

Specific Design Strategy

- **IDS Electrical Power**
  - **Electrical Power:**
    - In the event of primary power failure, the system shall automatically transfer to an emergency electrical power source without causing alarm activation.
  - **Emergency Backup Electrical Power.**
    - Twenty four hours of uninterruptible backup power is required and may be provided by an uninterruptible power supply (UPS), batteries or generators, or any combination.
  - **Electrical Power Source and Failure Indication.**
    - An audible or visual indicator at the PCU shall provide an indication of the primary or backup electrical power source in use.
    - Equipment at the monitoring station shall visibly and audibly indicate a failure in a power source or a change in power source.
    - The individual system that failed or changed shall be indicated at the PCU or monitoring station as directed by the AO.

Specific Design Strategy



Specific Design Strategy

- **Access Control Systems**
  - **Access is restricted to authorized personnel. Access control methods shall be approved by the Accrediting Official (AO).**
  - **Access control methods may include anyone of the following but are not approved for securing SCIF entrances when the SCIF is unoccupied:**
    - **Electromechanical, mechanical or personal recognition (in small facilities and/or where there is a single monitored entrance).**
    - **Automated access control systems using at least two technologies (badge, PIN, biometric, etc.)**
      - **Default is card reader with Keypad**

Specific Design Strategy

- **IDS Installation, Testing, and Approval**
  - **For Installations inside the United States:**
    - Shall be performed by U.S. companies using U.S. citizens.
  - **For installations outside the U.S.**
    - As documented in the CSP, U.S. TOP SECRET-cleared personnel or U.S. SECRET-cleared personnel escorted by SCIF personnel shall perform installation and testing of Intrusion Detection System (IDS)

Specific Design Strategy

- **IDS Installation, Testing, and Approval**
  - **IDS installation plans shall be controlled on a restricted basis.**
  - **IDS Approval**.
    - The AO shall approve IDS proposals and plans prior to installation within a SCIF as part of the SCIF construction approval process.
    - Final IDS acceptance tests as described ICS Technical guidelines and as prescribed in applicable manufacturer's literature shall be included as part of the SCIF accreditation package.

Requirements for TEMPEST

- **National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 7000, "TEMPEST Countermeasures for Facilities," establishes guidelines and procedures that shall be used by departments and agencies to determine the applicable TEMPEST countermeasures for national security systems.**
  - **In general, TEMPEST countermeasures apply when the SCIF contains equipment that will be processing national security information (NSI).**

- **Note: Having equipment that will be processing NSI does not necessarily imply the need to implement TEMPEST countermeasures.**

Requirements for TEMPEST

- The Certified TEMPEST Technical Authority (CTTA) has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures, including RED/BLACK installation measures.
  - Failure to consult the CTTA could result in installation of unnecessary and/or expensive countermeasures or the omission of needed countermeasures.
- Get the CTTA involved during the planning phase!
- If required TEMPEST countermeasures are omitted, the facility will not be accredited and the Supported Command will not be mission capable.

Requirements for TEMPEST

- The CTTA will use a risk based approach outlined in NSTISSI No. 7000 to determine applicable countermeasures for each SCIF.
- In conducting TEMPEST countermeasure review, the CTTA shall evaluate the following factors:
  - Location
  - Inspectable space boundary
  - Volume and sensitivity of Information processed
  - Access control of facility
  - Profile of Equipment used to process NSI
- Project Managers may need to provide site plans and building floorplans to assist CTTA in the evaluation of inspectable space.

Requirements for TEMPEST

- In General, any FCC Class B approved equipment can be used in a facility that meets 25 db of facility attenuation (e.g., R-foil or foil backed gypsum) or has adequate "inspectable space."
  - Inspectable space: The three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.
  - The CTTA shall determine the Inspectable Space for a facility.

Possible TEMPEST Countermeasures

- RF mitigation shall be provided at the direction of the CTTA when the SCIF utilizes electronic processing and does not provide adequate RF attenuation at the inspectable space boundary.
- RF mitigation is recommended for all applications where RF interference from the outside of the SCIF is a concern inside the SCIF.
  - The use of R-foil or aluminum foil backed gypsum is required if the facility does not provide adequate RF attenuation at the inspectable space boundary and recommended for all other applications.
  - When R-foil is employed it shall be placed inside the SCIF between the first and second layer of gypsum board.
  - Don't forget the ceiling and floor

Possible TEMPEST Countermeasures

- **Physical separation**
  - **All equipment, wirelines, components, and systems that process NSI are considered RED.**
  - **All equipment, wirelines, components, and systems that process encrypted NSI and non-NSI are considered BLACK.**
  - **The RED/BLACK concept is utilized to establish minimum guidance for physical separation to decrease the probability that electromagnetic emissions from RED devices might couple to BLACK systems.**
  - **Red/Black line separation guidelines**
    - 39 inches if neither line is in ferrous conduit
    - 9 inches if one line is in ferrous conduit
    - 3 inches if both lines are in ferrous conduit
    - 0 inches if one line is optical fiber

Possible TEMPEST Countermeasures

- **Distribution Equipment (Telecommunication Rooms/Closets).**
  - Distribution equipment must be designed with separate RED and BLACK connector blocks to prevent improper connection of RED and BLACK lines.
- **Protected Distribution Systems (PDS).**
  - A signal distribution system containing unencrypted NSI which enters an area of lesser classification, an unclassified area or uncontrolled (public) area must be protected according to the requirements of the current PDS standard.
  - For a SCIF, that means a signal distribution system containing unencrypted NSI that leaves the SCIF.
- **Signal Line Isolators and Filters**
  - BLACK lines and other electrically conductive materials that egress the inspectable space are potential carriers of Compromising Emanations (CE) that can inadvertently couple to the Red lines. Various signal line isolation techniques can be used to protect the signal line, the distribution system or other fortuitous conductors from conducting compromising signals beyond secure areas.
  - Signal line isolation should only be considered if the minimum separation recommendations cannot be met.

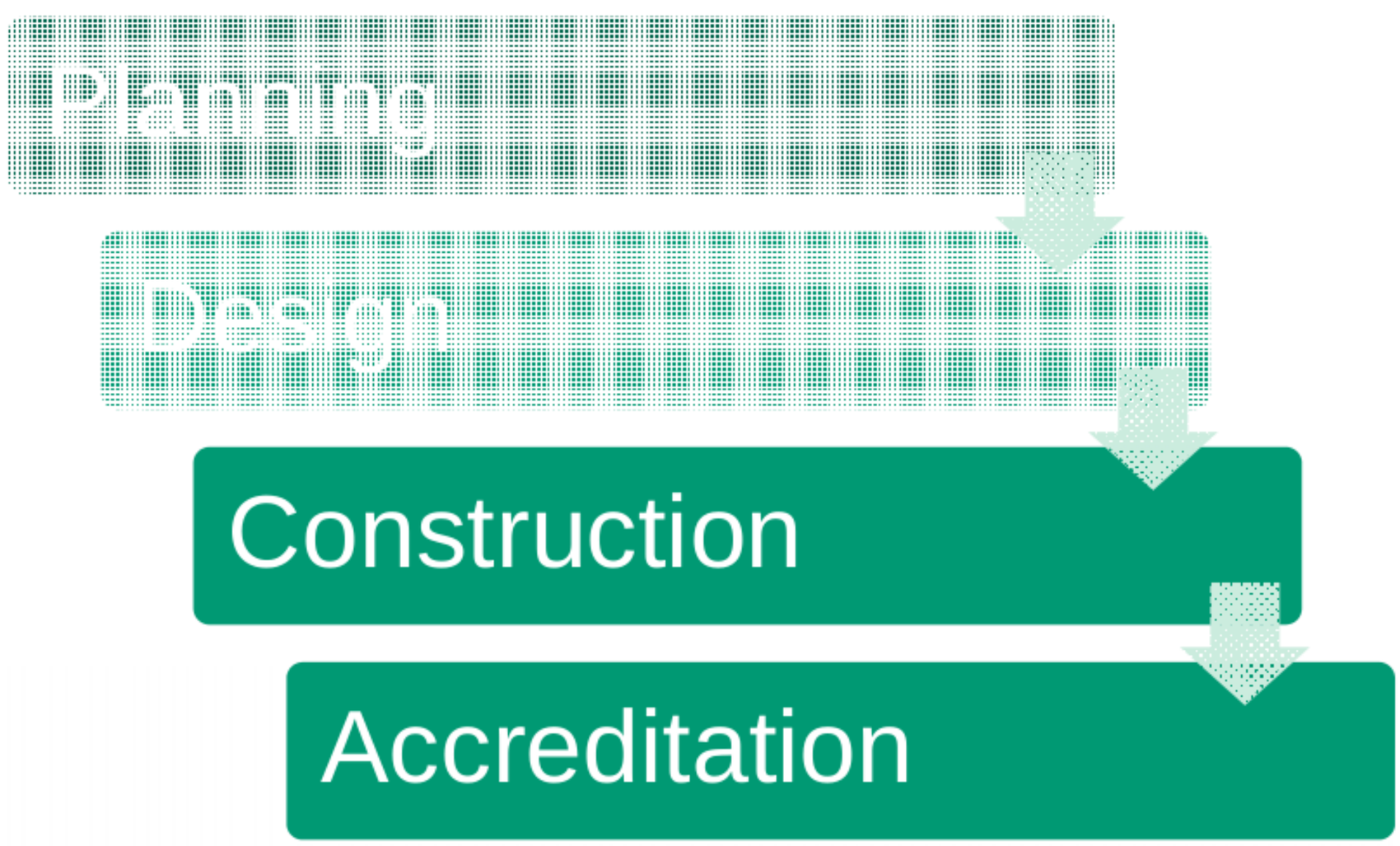
Combining RED SCI and RED non SCI

RED sensitive compartmented information (SCI) and RED non-SCI (secret/top secret) may be processed through components of a single RED distribution system to reduce infrastructure costs. This must be approved by the CSA and CTTA.

Section 6 of NSTISSAM TEMPEST/2-95 provides additional criteria related to:

- Routing of SCI Cables
- Termination (Outlet) Boxes
- Distribution Frame
- Patch Panels
- Access Points
- Multiplexers, Video and Audio Switches, and Other Multiple Circuit Equipment
- Cables
- Power and Signal Line Filtering
- Telephone Lines

SCIF Phases



SCIF Accreditation Cycle

- ISC 705-2 provides accreditation policy requirements.
  - SCIF inspections and evaluations are performed by the AO, or designee (SSM), prior to initial accreditation.
  - The accreditation includes a review of documents relating to SCIF design and construction and include a Fixed Facility Checklist (FFC).
  - To facilitate this process, Project/Construction managers shall provide the AO/SSM site plans, building floorplans, IDS plans, and information related to perimeter and compartment area wall construction, doors, locks, deadbolts, IDS, telecommunication systems, acoustical protection, and TEMPEST countermeasure.

SCIF Accreditation Cycle

- Coordinate preliminary walkthrough with the accreditation official prior to substantial completion of SCIF space.
- Assemble required documents for accreditation process and equipment providers. (Requirements vary depending on project)
  - Drawings:
    - Civil Site Plan
    - Architectural
      - Floor and Reflective Ceiling Plans
      - Wall sections (floor to ceiling)
      - Floor and Ceiling section
      - Door Schedule
      - Door head, jamb, and threshold details
      - Window schedule and details
    - Fire Protection
      - Sprinkler piping including penetration details
      - Fire Alarm system
      - Mass Notification System

SCIF Accreditation Cycle

- **Drawings (continued):**
  - **Mechanical**
    - HVAC plans, sections and details of SCIF penetrations, ductwork details sheets
    - Plumbing floor plans, detail for SCIF penetrations
  - **Electrical**
    - Site plan
    - Lighting, Power, Telecommunications, Electronic Security System (ESS) plans
      - » Plans must indicate device and panel location to include strobe lights
    - One-line diagrams for Power, Telecommunications, and ESS
    - ESS Door wiring details
    - Detail of SCIF penetrations
- **Submittals**
  - Doors
  - Door Hardware (locks, closers, and hinges)
  - Acoustical ratings
  - Electronic Security Systems
  - Sound masking equipment
  - As-Built drawings

SCIF Accreditation Cycle

- **Conduct periodic inspections of SCIF area to document and validate:**
  - **Stud wall construction**
  - **Acoustic batting installation**
  - **R-foil or aluminum foil backed gypsum installation (TEMPEST requirement)**
  - **Enhanced wall construction**
  - **Gypsum Wallboard installation**
  - **Finished wall**
    - True Floor to True Ceiling
    - Top and bottom sealed (both sides) with acoustical foam or sealant finished to match wall
    - Finished from true floor to true ceiling
  - **Wall Penetrations**
    - Sealed (both sides) with acoustical foam or sealant finished to match wall
  - **Metallic penetrations at perimeter (non-conductive break (e.g., canvas, rubber) installed at the interior perimeter (TEMPEST requirement) .**
  - **Man-bar installation**
  - **Inspection ports**

SCIF Accreditation Cycle

- **Photographic Construction Surveillance Record may be accomplished by SSM or approved personnel to expedite the accreditation process.**
- **It is important to capture areas which will be covered up during construction. Pictures shall include the SCIF and CA perimeters and should capture:**
  - **Wall construction**
    - Stud walls
    - Acoustic installation
    - Enhanced wall construction (9 gauge expanded metal)
    - R-foil or aluminum foil backed gypsum installation (TEMPEST)
  - **Wall finishes (true floor to true ceiling)**
  - **Perimeter penetrations**
  - **Duct construction including inspection ports and acoustic baffle**
  - **Man-bar construction**
  - **Sound masking devices**

Take Away

- **As a construction agent for the Department of Defense, we must understand the SCIF requirements and ensure the SCIF we plan, design, and build meet the policy based accreditation requirements.**
  - **If a SCIF cannot be accredited, it cannot be operational… and the supported command is "not mission capable!"**
- **Be Proactive: Find out who the designated Site Security Manager (SSM) and the Certified TEMPEST Technical Authority (CTTA) are and get them involved early in the project planning and keep them involved throughout the project.**

Definitions

Accrediting Official (AO)
- Person designated by the Cognizant Security Authority (CSA) that is responsible for all aspects of SCIF management and operations to include security policy implementation and oversight.

Black LAN:
- A term applied to equipment, cables, or fiber that processes or carries only unclassified and/or encrypted information.

Certified TEMPEST Technical Authority (CTTA)
- U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a U.S. Government department or agency.

Closed Storage:
- The storage of SCI material in properly secured GSA approved security containers within an accredited SCIF.

Cognizant Security Authorities (CSA):
- The single Principal designated by a SOIC (see definition of SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.

Compartmented Area (CA)
- The a room, a set of rooms, or an area that provides controlled separation between compartments within a SCIF.

Construction Security Plan (CSP)
- A plan developed by the Site Security Manager (SSM) and approved by the CSA, which outlines security measures to be followed to ensure security of the construction site and compliance with the SCIF construction requirements.

Continuous Operation:
- This condition exists when a SCIF is staffed 24 hours every day.

Open Storage:
- The storage of SCI material within a SCIF in any configuration other than within GSA approved security containers.

Red LAN:
- A term applied to equipment, cables, or fiber that processes or carries unencrypted National Security Information (NSI) that requires protection during electrical/electronic processing.

Definitions

Secure Working Area:
- An accredited SCIF used for handling, discussing and/or processing of SCI, but where SCI will not be stored.

SCIF Security Officer (SSO)/Site Security Manager (SSM):
- Person designated by the Cognizant Security Authority (CSA) that is responsible for all aspects of SCIF management and operations to include security policy implementation and oversight.

Sensitive Compartmented Information (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.

Sensitive Compartmented Information Facility (SCIF):
- Accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed.

Sound Transmission Class (STC):
- The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value.

SOIC:
- Senior Officials of the Intelligence Community

STC Rating:
- STC is a single number rating used to determine the sound barrier performance of walls, ceilings, floors, windows, and doors.

TEMPEST:
- TEMPEST refers to the investigation, study, and control of Compromising Emanations of National Security Information (NSI) from telecommunications and information processing systems.

Temporary Secure Working Areas (TSWAs)
- An accredited facilities where handling, discussing, and/or processing of SCI is limited to less than 40-hours per month and the accreditation is limited to 12 months or less.

Vault:
- A room(s) used for the storing, handling, discussing, and/or processing of SCI and constructed to afford maximum protection against unauthorized entry.