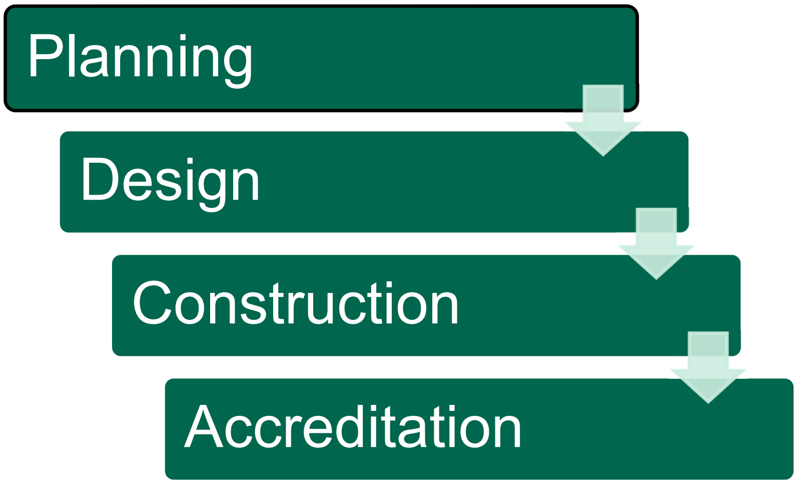
NAVFAC SOUTHWEST
Naval Special Warfare Command Sensitive Compartmented Information Facilities (SCIF) and Special Access Program Facilities (SAPF)

Richard Cofer, PE
Jonathan Rau, RA
Naval Facilities Engineering Systems Command
Facilities Criteria Office

July 2022

Welcome

Today we will provide an introduction to SCIF & SAPF Policy and Criteria and discuss the four phases of a project


Planning
Design
Construction
Accreditation

Sensitive Compartmented Information Facility (SCIF)

A 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

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).**

Special Access Program Facility (SAPF)

A SAPF is a specific physical space that has been formally accredited in writing by the responsible Program Security Officer (PSO) that satisfies the criteria for generating, safeguarding, handling, discussing, and storing classified or unclassified program information, hardware, and materials.

–Typically found in:

- Hangers
- Trainers

Other Secure Spaces Associated with Classified Information or Materials

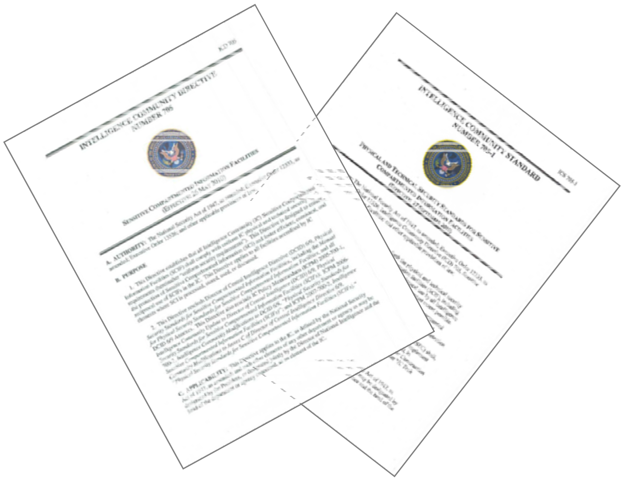
- **The following are not the same as a SCIF or SAPF and do not require the same security procedures or follow the same accreditation process.**
  - **Top Secret or Secret Open Storage**
    - Open storage area (also called a secure room)
    - DoDM 5200.01 Vol 3, DoD Information Security Program: Protection of Classified Information
  - **COMSEC Storage**
    - Stored separately from other classified material
    - CMS-1A DON COMSEC Policy and Procedures Manual
  - **Restricted Access Area**
    - CNSSI No.7003 Protected Distribution Systems (PDS)
  - **Controlled Access Area**
    - CNSSI No.7003 Protected Distribution Systems (PDS)

Accreditation

- The Accreditation process starts during the planning phase.
- Accrediting Official (AO) is responsible to accredit (approve) the facility for operation. The AO is different for a SCIF and SAPF.
- Accreditation must be achieved before the facility can become operational for the supported command.
- Proper planning, communication and execution must occur throughout the project in order to achieve accreditation.
- Facility Accreditation must occur prior to or concurrent with facility BOD/turnover in order not to adversely impact the mission of the facility and supported command.

Responsibilities

- **As a design and construction agent for the Department of Defense, it is imperative that NAVFAC understands the requirements contained in DoD Manuals and the Intelligence Community Standards and include them in project requirements.**
- **Documents affect :**
  - **Planning**
  - **RFP Development**
  - **Design**
  - **Construction**

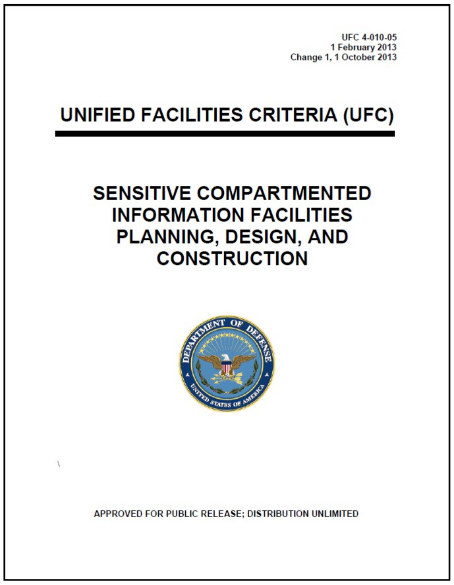

INTELLIGENCE COMMUNITY DIRECTIVE
NUMBER 705
SENSITIVE COMPARTMENTED INFORMATION FACILITIES
INTELLIGENCE COMMUNITY STANDARD
NUMBER 705-1
PHYSICAL AND TECHNICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES

Design and Construction Criteria Documents

- UFC 4-010-05 Sensitive Compartmented Information Facilities Planning, Design and Construction, 01 Oct 2013 (Being updated to include SAPF)
- NAVFACINST 4700.1A Planning, Design and Construction of Navy Sensitive Compartmented Information Facilities
- ICD/IDS 705 Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, 13 Mar 2020
- UFGS 01 14 00 WORK RESTRICTIONS
- UFGS 01 45 00.00 20 QUALITY CONTROL
- UFGS 01 45 00.05 20 QUALITY CONTROL (DESIGN BUILD)
- DoDM 5105.21-Vol 1-3, Sensitive Compartmented Information (SCI) Administrative Security Manual
- DODM 5205.07 Volume 1-3, DoD Special Access Program (SAP) Security Manual: Physical Security

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

- **PURPOSE:** To provide unified criteria and make the planning, design and construction communities aware of policy requirements and ensure appropriate implementation.
- **PREPARING ACTIVITY:** NAVFAC
  - –Point of contact: Richard Cofer
- **CURRENT DOCUMENT STATUS:**
  - –Published February 2013, Available on the Whole Building Design Guide Website (www.wbdg.org)
  - –Change 1 Published 1 October 2013
  - –Revision in progress: Pre-Final
    - Will Include SAPF



UFC 4-010-05
1 February 2013
Change 1, 1 October 2013

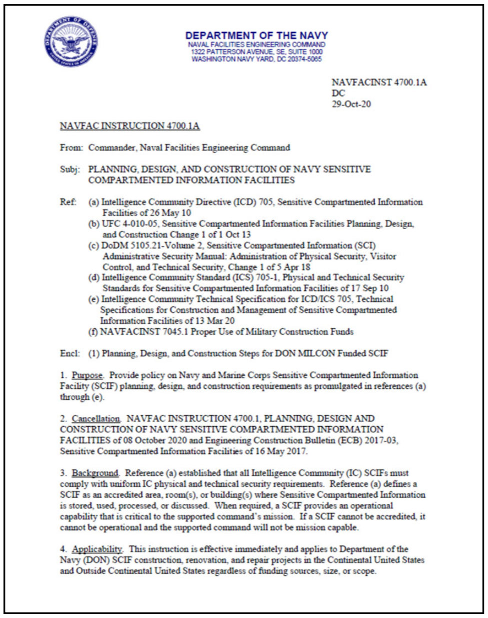
UNIFIED FACILITIES CRITERIA (UFC)

SENSITIVE COMPARTMENTED INFORMATION FACILITIES PLANNING, DESIGN, AND CONSTRUCTION

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

NAVFAC INST 4700.1A Planning, Design, and Construction of Navy Sensitive Compartmented Information Facilities

- **PURPOSE:** Provide NAVFAC policy on the planning, design and construction of Department of the Navy SCIFs
- **SUPERSEDES: ECB 2017-03**
- **PREPARING ACTIVITY:** NAVFAC Engineering and Criteria Office
  - This document was coordinated with SSO Navy, USMC HQ and NAVFAC Components through the Navy Tasker system to include NAVFAC HQ BD and the Chief's office.
- **DOCUMENT STATUS:**
  - Published September 2020
  - Updated October 2020
  - Update in for signature (Version B)
  - Future update to include SAPF



DEPARTMENT OF THE NAVY
NAVAL FACILITIES ENGINEERING COMMAND
1322 PATTERSON AVENUE, SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5065

NAVFACINST 4700.1A
DC
29-Oct-20

NAVFAC INSTRUCTION 4700.1A

From: Commander, Naval Facilities Engineering Command

Subj: PLANNING, DESIGN, AND CONSTRUCTION OF NAVY SENSITIVE COMPARTMENTED INFORMATION FACILITIES

Ref: (a) Intelligence Community Directive (ICD) 705, Sensitive Compartmented Information Facilities of 26 May 10
(b) UFC 4-010-05, Sensitive Compartmented Information Facilities Planning, Design, and Construction Change 1 of 1 Oct 13
(c) DoDM 5105.21-Volume 2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security, Change 1 of 5 Apr 18
(d) Intelligence Community Standard (ICS) 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities of 17 Sep 10
(e) Intelligence Community Technical Specification for ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities of 13 Mar 20
(f) NAVFACINST 7045.1 Proper Use of Military Construction Funds

Encl: (1) Planning, Design, and Construction Steps for DON MILCON Funded SCIF

1. Purpose. Provide policy on Navy and Marine Corps Sensitive Compartmented Information Facility (SCIF) planning, design, and construction requirements as promulgated in references (a) through (e).

2. Cancellation. NAVFAC INSTRUCTION 4700.1, PLANNING, DESIGN AND CONSTRUCTION OF NAVY SENSITIVE COMPARTMENTED INFORMATION FACILITIES of 08 October 2020 and Engineering Construction Bulletin (ECB) 2017-03, Sensitive Compartmented Information Facilities of 16 May 2017.

3. Background. Reference (a) established that all Intelligence Community (IC) SCIFs must comply with uniform IC physical and technical security requirements. Reference (a) defines a SCIF as an accredited area, room(s), or building(s) where Sensitive Compartmented Information is stored, used, processed, or discussed. When required, a SCIF provides an operational capability that is critical to the supported command's mission. If a SCIF cannot be accredited, it cannot be operational and the supported command will not be mission capable.

4. Applicability. This instruction is effective immediately and applies to Department of the Navy (DON) SCIF construction, renovation, and repair projects in the Continental United States and Outside Continental United States regardless of funding sources, size, or scope.

Classifications of Facilities

- **There are Six Classifications, we typically deal with three.**
  - **Closed Storage:**
    - Materials are stored in GSA approved storage containers when not in use.
      - This includes documents, computer hard drives, and storage media.
  - **Open Storage:**
    - Materials may be openly stored and processed and may be left out when not in use and facility is occupied.
  - **Continuous Operation:**
    - Staffed and operated 24/7. Depending on operational procedures, materials may be left out or stored when not in use.

SCIF Requirement

- Per DoDM 5105.21-Volume 2:
  - The Concept Approval is the first critical element in the establishment of a SCIF.
    - Concept Approval certifies that a clear operational requirement exists for the SCIF and there is no existing SCIF to support the requirement.
  - Once a need for SCI has been identified, the requesting command (mission) will submit a request for Concept Approval for SCI.
  - The Service CSAs, their designees, or DoD Component SIOs are required to grant Concept Approval to establish a SCIF.
- Without the Concept Approval, the Supported Command is not authorized to initiate a SCIF project.
  - When a command tells NAVFAC they want a SCIF, first question should be, do you have Concept Approval?
  - Need confirmation (email) from requesting command or their SSM.
  - No Concept Approval = no requirement = no SCIF.

SAPF Requirement

- SAPFs do not require Concept Approval.
  - The requirement for a SAPF is generated by the Program associated with the facility. Typically associated with a weapon or communication platform.
- Some SAPFs include SCIFs or are also SCIFs. In this case a Concept Approval would be required for only the SCIF.
  - The design and construction of the facility would not change, only the accreditation process.

Determining Project Requirements

- A site security manager (SSM) is designated for each construction or renovation project by the requesting command.
- The SSM is responsible for security requirements.
  - SSM is responsible for assembling and submitting documents to the AO for approval. Documents include, but not be limited to:
    - Construction Security Plan (CSP)
    - Fixed Facility Checklist (FFC)
    - TEMPEST addendum
    - When applicable, waiver request packages.

Construction Security Plan (CSP)

- Each project requires a CSP. The CSP:
  - Developed by the SSM and approved by the AO.
  - Addresses the application of security to planning, design, and construction.
  - Format and content is based on extent of construction and security concerns.
- DNI Policy states the CSP must be approved prior to construction. THIS IS TOO LATE!
  - MILCON budgets are locked 3 years prior to construction start.
    - A preliminary CSP must be developed during the planning phase to capture the scope and cost associated with security.
  - CSPs must be finalized and approved by the AO during design phase.
  - Construction contracts cannot be awarded without and approved CSP.

Fixed Facility Checklist (FFC)

- The FFC is a standardized document developed by the requesting command to support the accreditation process.
  - The FFC documents physical, technical, and procedural security information for accreditation.
- To support the accreditation process, the Planner, Designer of Record, Project Manager, and Construction Manger may have to provide the SSM site plans, building floorplans, IDS plans, and other information related to perimeter and compartment area's wall construction, doors, locks, deadbolts, Electronic Security System (ESS), telecommunication systems, acoustic protection, and TEMPEST countermeasures.

TEMPEST Countermeasure Review (TCR)

- Each facility that process National Security Information (NSI) requires a TEMPEST Countermeasures Review (TCR), performed by Certified TEMPEST Technical Authority (CTTA), as part of the accreditation process.
  - To request a TCR, the SSM will submit the TEMPEST addendum (TEMPEST Checklist) to the FFC.
  - Per DoDM 5105.21-Vol 2 (SCIF), The addendum will be submitted during the planning phase of the construction. DODM 5205.07 Volume 1-3 (SAPF) is silent on submittal timing.
    - While some specific information may not be known prior to construction, as much information as possible must be provided in order to minimize costly changes.
    - These TEMPEST countermeasures are based upon risk management principles using factors such as location, volume of information processed, sensitivity, and perishability of information, physical control, and the TEMPEST profile of equipment used.

Design and Construction: United States

- SCIF/SAPF construction and design shall be performed by U.S. companies using U.S. citizens or U.S. persons.
  - 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 with a trustworthiness determination.
- The AO shall ensure mitigations are implemented when using non-U.S. citizens.
- These are documented in the CSP.

Design and Construction: Outside United States

- SCIF/SAPF design shall be performed by U.S. companies using U.S. citizens or U.S. persons.
- General SCIF/SAPF construction shall be performed by U.S. companies using U.S. citizens.
  - General construction includes construction activities such as building sitework, utilities, foundations, structure, and enclosure or shell, including doors, windows and façade work. Utility work that penetrates the secure area and installation of doors in these areas are not general construction.
- Applicable to the SCIF/SAPF and possibly the adjacent space.

Design and Construction: Outside United States

- **U.S. Top Secret-cleared or Secret-cleared personnel shall perform finish work in the SCIF/SAPF as documented in the CSP.**
  - Finish Work includes activities such as insulation, floor/partition/ceiling systems, cabinet work, conveyor systems, specialties, building furnishings/fixtures/equipment, mechanical/electrical services and equipment including those specialized for fire protection, security, communication, control, energy conservation, safety, comfort, convenience, and similar purposes.
- **Applicable to finish work in the SCIF/SAPF, not other areas of the facility.**

Design and Construction: 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 U.S. Personnel with a TS clearance.**
  - **UFGS 01 14 00 Work Restrictions**

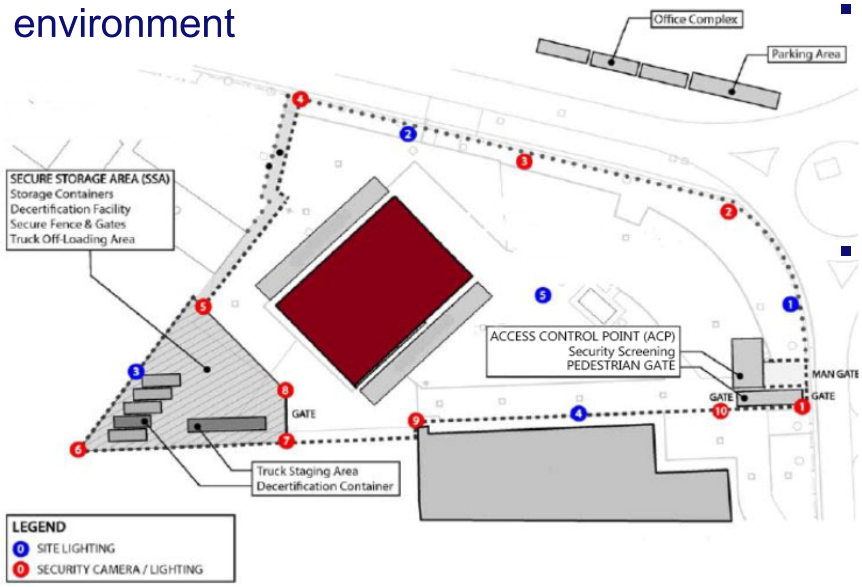
Construction Security

- AO will 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 construction area, i.e. storage and inspection areas. Since these additional security measures may have significant cost impacts on project, they must be determined during project development.

When required, these procedures are documented in the Construction Security Plan (CSP).

Construction Security - Site

This example is from a site outside the U.S. in a high threat environment

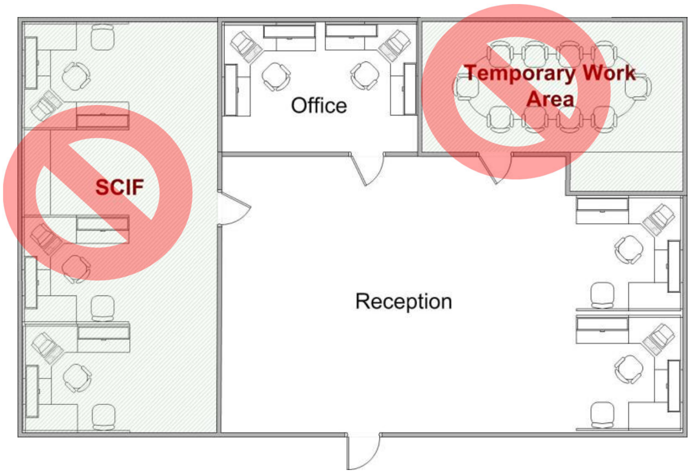


Consider:
- Secure perimeter
- Access Control and Security Screening
  - Vehicle
  - Personnel
  - Material Shipment
- Material Storage
  - Size
  - Access Control

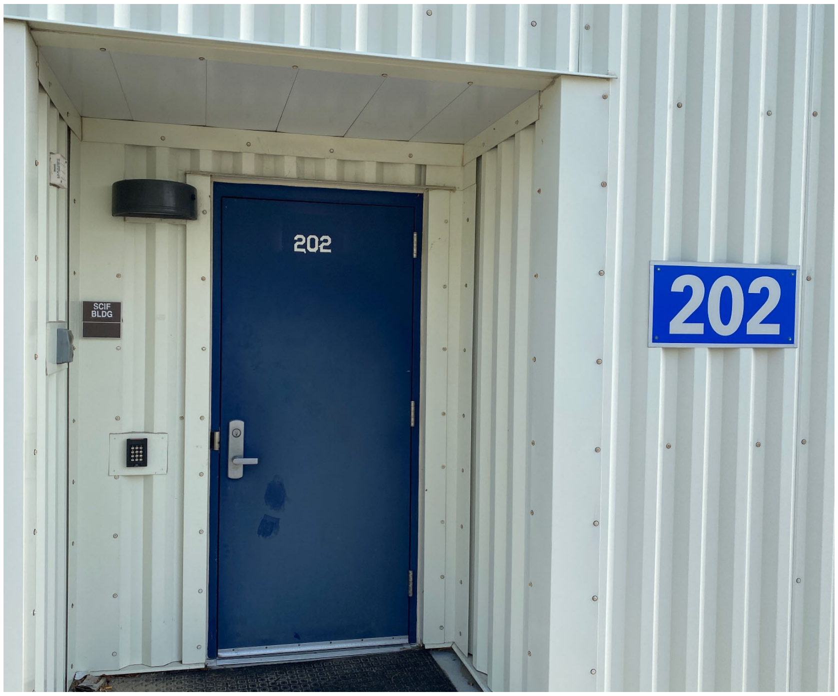
Information Security

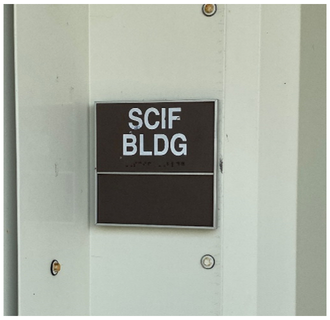
- Construction plans and related documents are handled and protected in accordance with the Construction Security Plan
- Do not identify SCIF/SAPF locations on planning or construction documents

- With accrediting official's approval, areas may be identified as "controlled space", "secure area" or "controlled area"



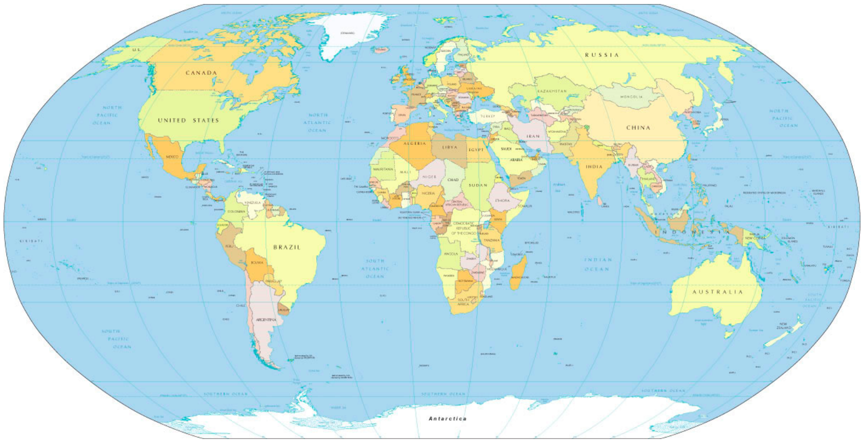
Information Security





Security Requirements

- The location (threat), its classification, security-in-depth, and how it is operated will determine the security requirements.
- For overseas, AO uses the Department of State (DoS) Security Environment Threat List (SETL) for the threat ratings.
  - <u>The DoS SETL and its contents are Classified Secret.</u>



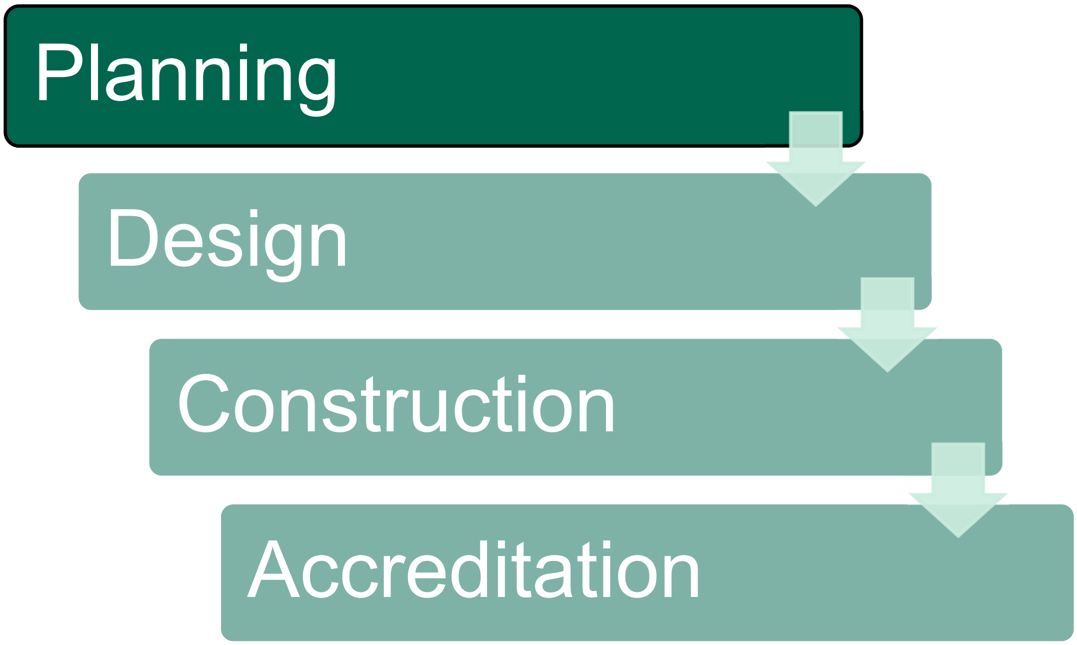
Information Security

- 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 Secret information.
  - Planners, 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 unclassified information technology systems.

Project OPSEC

- The OPSEC process provides a means of screening information prior to public release.
- Publicly released documents such as field investigations, reports, studies, Basis of Design, calculations, drawings, specifications, or Design-Build Request for Proposals (RFP) cannot reveal sensitive or critical information.
- Include an OPSEC review by the requesting activity as part of the normal review and SAT-TO process.
  - Where applicable, modify details and identifying information in order to eliminate information the requiring activity has identified as sensitive or critical.
  - Refer to FC 1-300-01 Navy and Marine Corps Design Procedures for more information. Some Examples:
    - Do not identify the location of a SCIF or SAPF
    - Do not identify purpose or frequency range of antennas or communication systems

Project Phases



Planning

Design

Construction

Accreditation

Planning Team

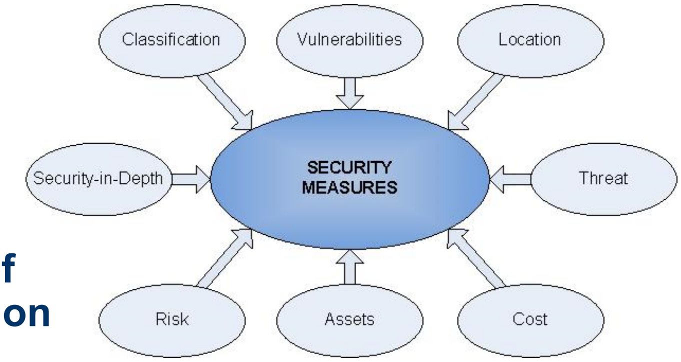
- Establish an interdisciplinary planning team with local considerations to include the following:
  - Planning
  - Supported Command
  - Site Security Manager (SSM)
  - Communications
  - Security
  - Engineering
  - Cultural resources (if historical building)
- Planning team must work together to determine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

Determining Project Requirements

- Planner must work closely with the supported command and the AO’s representative (SSM) to determine the requirements.
- The SSM, AO and the Certified TEMPEST Technical Authority (CTTA) 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/SSM/CTTA will consider factors such as:
  - Classification
  - Location
  - Threat
  - Vulnerabilities
  - Security in Depth
  - Type and amount of classified information being processed
  - TEMPEST Review
  - Cost**
  - Risk



** Design and Construction Agent needs to make sure the AO/SSM understands the cost implications of the security requirements.

Determining Project Requirements

- The NAVFAC Facility Planner assigned to the project must assist the SSM in documenting the facility and site requirements necessary for the preparation of the CSP, FFC and TEMPEST Addendum.
  - The SSM will send the preliminary versions to the AO for review.
- Upon review of the preliminary CSP, the AO will issue an approval or acknowledgment message along with the SCIF Identification Number (SCIF ID).
  - An approval is considered the AO's Concept Design Approval.
  - If an acknowledgment message is sent, it will contain guidance that the SSM must be incorporated into the CSP and ultimately, the project.

Historic Preservation

- **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 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 minimized 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.**

Planning Security Requirements

- **Work with the supported command and the SSM to determine and document the classification, operation, and resulting protective measures for each project.**
  - Is the SCIF or SAPF the entire facility or an area within the facility?
  - Will there be more than one SCIF or SAPF in the facility, if so how many?
    - If more than one, can they be consolidated?
  - What is the classification of each space?
  - Will the perimeter wall be standard, enhanced, or vault construction?
  - What is the required Sound Transmission Class (STC) rating for the perimeter?
  - Will there be Compartmented Areas? If so, how many?
    - Is there a STC requirement for the compartmented areas (Type I or Type II)?
  - Are there any Electronic Security System (ESS) requirements above that required by IC Tech Spec-for ICD/ICS 705?

Planning Security Requirements

- Continued.
  - Is there equipment that will be processing National Security Information (NSI)?
    - Has the supported command provided the CTTA with a completed TEMPEST Addendum for the TCR?
    - If so, what will be the required TEMPEST countermeasures? RED/Black Separation, Dielectric Breaks, Filters, Shielding?
  - Are there special procurement, shipping, and storage of construction materials required at the site? If so, what will be required?
  - Are there access control requirements for the construction site?
  - Are there access control and storage requirements for the construction materials?
  - Will U.S. companies using U.S. citizens or Persons be required for construction?

Planning Security Requirements

- Continued.
  - For project outside the United States, its possessions or territories:
    - Will U.S. Secret or U.S. Top Secret cleared personnel be required to perform finish work?
  - Will installation and testing of the ESS be performed by U.S. TOP SECRET-cleared personnel or escorted U.S. SECRET-cleared personnel?
  - Will any mitigations or countermeasures above the minimum be required?
    - If so, is there an approved waiver?
  - Some of these requirements are documented in the CSP. Therefore, it is very important to obtain the preliminary CSP during project development to ensure appropriate security requirements are documented and included in the project scope and budget.

Planning Security Requirements

- Construction Surveillance
  - Intelligence Community and the Tech Spec for ICD/ICS 705 do not require Cleared American Guards (CAGs) or Construction Security Technicians (CSTs) for projects within the United States, its territories or possessions.
  - The Tech Spec also states that for projects on U.S. military installations, when the AO considers the risk acceptable, alternative countermeasures may be substituted for the use of a CST as prescribed in the CSP.
- Construction security surveillance such as CSTs and CAGs, may be client funded using appropriations available for operations or with resource sponsor’s approval, funded by MILCON.
  - Refer to NAVFACINST 4700.1, 7045.01 and CRB Guidelines.

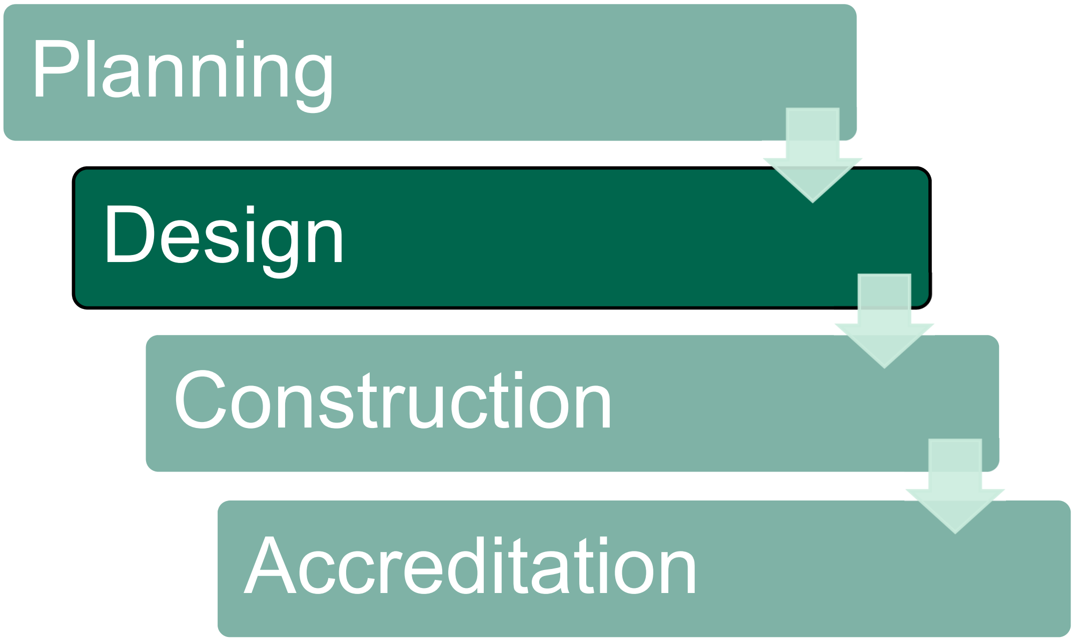
NAVFAC INST 4700.1A Planning, Design, and Construction of Navy Sensitive Compartmented Information Facilities

- During the project planning stage and development of a DD1391:
  - The NAVFAC Asset Management (AM) Facility Planner will work with the SSM to ensure security requirements are included in the Basic Facility Requirement and Facility Planning Document.
  - The SSM should send the preliminary CSP and the FFC and the TEMPEST addendum to the AO.
    - Upon review of the preliminary CSP, the AO will issue an approval or acknowledgment message along with the SCIF identification number (SCIF ID).
  - The NAVFAC Facility Planner assigned to the project must assist the SSM in documenting the facility and site requirements necessary for the preparation of these documents.
- Do not finalize a project scope or budget without an approved or acknowledged Preliminary CSP

NAVFAC INST 4700.1A Planning, Design, and Construction of Navy Sensitive Compartmented Information Facilities

- Serious consideration should be given to the acquisition strategy to be used on a project.
  - The Design Bid Build (DBB) acquisition strategy will enhance the security of the project and allow the CSP requirements and TEMPEST countermeasures to be refined during the design development.
- DBB acquisition strategy must be used when the entire facility is a SCIF.
- DBB acquisition strategy should be the first consideration when a major portion of the facility is a SCIF or when the project is outside of the United States, its possessions or territories.
  - The strategy will be selected with joint concurrence of DC/OP/AQ during the development of the 1391.

Project Phases



Planning

Design

Construction

Accreditation

Design Team

- Design shall be performed by U.S. Companies using U.S. Citizens
  - Documented in CSP
- Past experience is preferred and will be beneficial

Preliminary Design Phase

- Project Manager, Design Manager and Designer of Record must work closely with the supported command and the AO's representative (SSM) to validate the security requirements for the project.
  - The SSM must validate the preliminary CSP requirements.
    - The CSP may be adjusted by the SSM due to changes in operational requirements or the local threat.
    - Project Manager/Project Team must inform supported command and SSM of the scope or budget implications.
  - SSM must complete and submit the updated CSP and the Preliminary Fixed Facility Checklist (FFC) with the TEMPEST addendum.
  - AO sends TEMPEST Countermeasure Review (TCR) Message.

TEMPEST Countermeasures

- In general, TEMPEST countermeasures are required when the space contains equipment that will be processing National Security Information (NSI).
  - In the past, having equipment that will be processing NSI does not necessarily imply the need to implement TEMPEST countermeasures beyond RED/BLACK separation.
  - Projects requiring TEMPEST Countermeasures are on the increase.
- If required TEMPEST countermeasures are omitted, the facility will not be accredited.

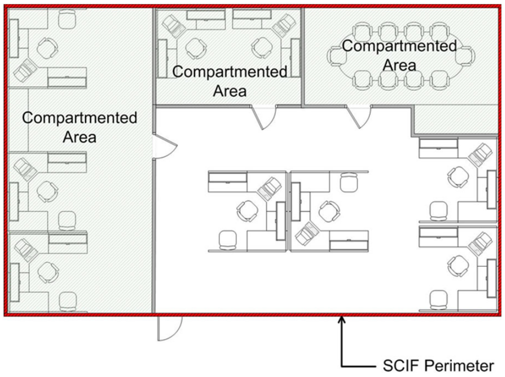
TEMPEST Review

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

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

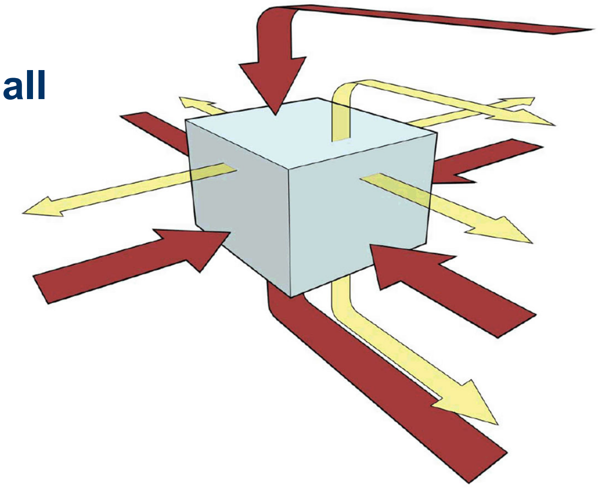
General Design Strategy: Consolidate Spaces

- When a facility has more than one SCIF or SAPF, serious consideration should be given to consolidate the multiple spaces into one.
  - Consolidation of spaces will reduce initial and sustainment costs for infrastructure, electronic security systems, and the associated accrediting requirements.
  - This must be coordinated with the supported commands to insure the configuration will meet their operational and compartmented requirements.



General Design Strategy

- The design will vary depending on type, location, SID, discussion, and NSI processing requirements.
- Designers must take a six-sided approach when developing design.
  - The perimeter includes all walls, floors, ceilings, doors, windows and penetrations in the perimeter such as ductwork, pipes and conduit.



General Design Strategy: Perimeter

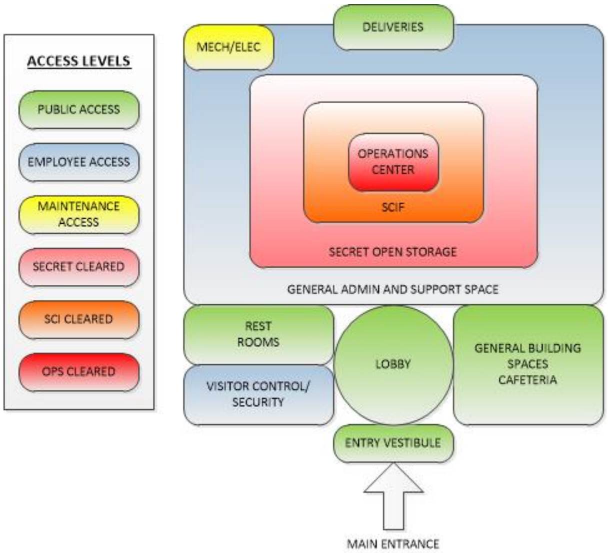
- The perimeter and the penetrations to the perimeter are the primary focus of secure space design and construction.
- At a minimum, the perimeter provides:
  - Resistance to forced entry
  - Resistance to covert entry
  - Visual evidence of surreptitious penetration
  - Sound Attenuation for acoustic eavesdropping
  - TEMPEST Countermeasures (when required)

General Design Strategy: Building Layout

- To optimize the building layout for security and function, the designer must understand:
  - The various secure spaces in the facility
  - The security clearances of the occupants
  - Visitor access and escort requirements
  - Separations or adjacencies required
  - Compartmented Areas
- This takes an integrated design approach that balances the occupant's operational and space requirements, visitor control, security-in-depth and the concept of zoning.

General Design Strategy: Zoning

- Zoning is the concept of grouping functional areas by security or access levels to enhance security.



ACCESS LEVELS

PUBLIC ACCESS

EMPLOYEE ACCESS

MAINTENANCE ACCESS

SECRET CLEARED

SCI CLEARED

OPS CLEARED

MECH/ELEC

DELIVERIES

OPERATIONS CENTER

SCIF

SECRET OPEN STORAGE

GENERAL ADMIN AND SUPPORT SPACE

REST ROOMS

VISITOR CONTROL/ SECURITY

LOBBY

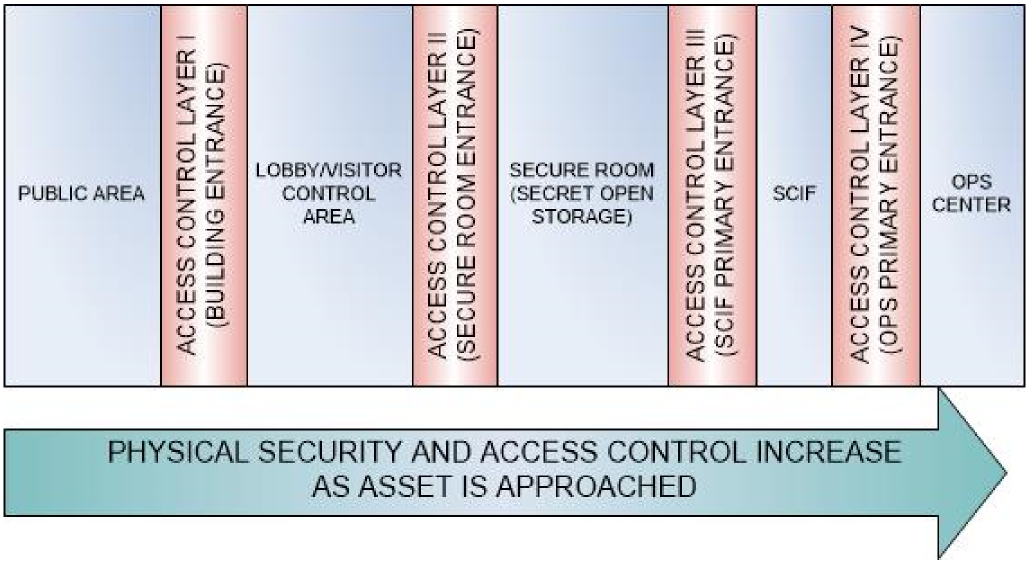
GENERAL BUILDING SPACES CAFETERIA

ENTRY VESTIBULE

MAIN ENTRANCE

General Design Strategy: Zoning

- ACCESS LAYERS.



PUBLIC AREA

ACCESS CONTROL LAYER I (BUILDING ENTRANCE)

LOBBY/VISITOR CONTROL AREA

ACCESS CONTROL LAYER II (SECURE ROOM ENTRANCE)

SECURE ROOM (SECRET OPEN STORAGE)

ACCESS CONTROL LAYER III (SCIF PRIMARY ENTRANCE)

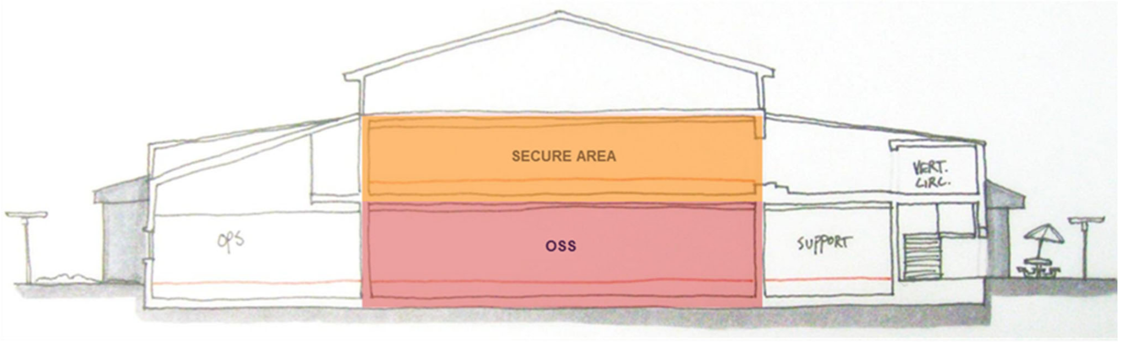
SCIF

ACCESS CONTROL LAYER IV (OPS PRIMARY ENTRANCE)

OPS CENTER

PHYSICAL SECURITY AND ACCESS CONTROL INCREASE AS ASSET IS APPROACHED

General Design Strategy: Building Layout



SECOND FLOOR SECURE AREA
LOCATED DIRECTLY OVER THE OPEN
SECRET STORAGE (OSS) SPACE.

BUILDING SECTION

General Design Strategy: Building Layout

- **When developing a building layout:**
  - **Maximize the vertical and horizontal separation between the lowest and highest security areas.**
  - **Maximize grouping of secure areas to enhance floor/ceiling security and to minimize locations of secure elements.**
  - **In large facilities, the highest security area should be located in the building center, on an upper floor or basement.**
  - **When a facility has multiple security levels, access to the highest security area should be through the area with the next lower security level.**
    - An example would be to access a SCIF through a secret open storage area.

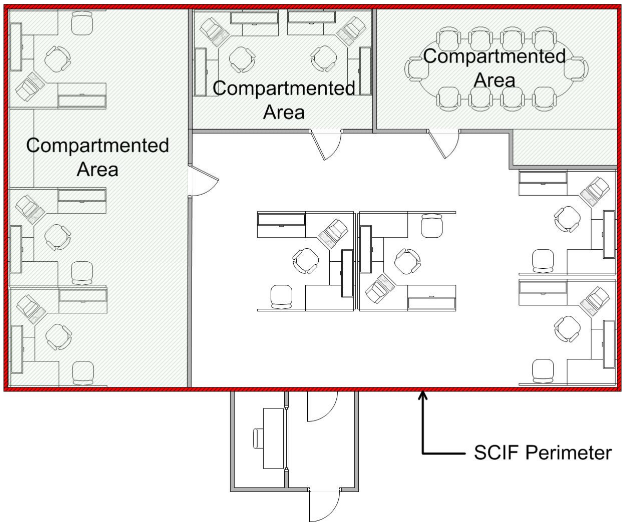
General Design Strategy: Building Layout

- **When developing a building layout (Continued):**
  - **Are foreign nationals allowed in the facility to work or participate in training given at the facility?**
    - If so, building layout should consolidate security areas and provide the appropriate separation to minimize the technical threat and escort requirements.
  - **Locate telecommunication spaces that contain the encryption equipment within or adjacent (shared wall) to eliminate the need for a Protected Distribution System (PDS) requirements.**
  - **Egress paths from the lower security areas must not pass through a higher security area.**
  - **Entry into a lower security area cannot be through a higher security area (would require escorts and halt operations).**

General Design Strategy: Compartmented Area (CA)

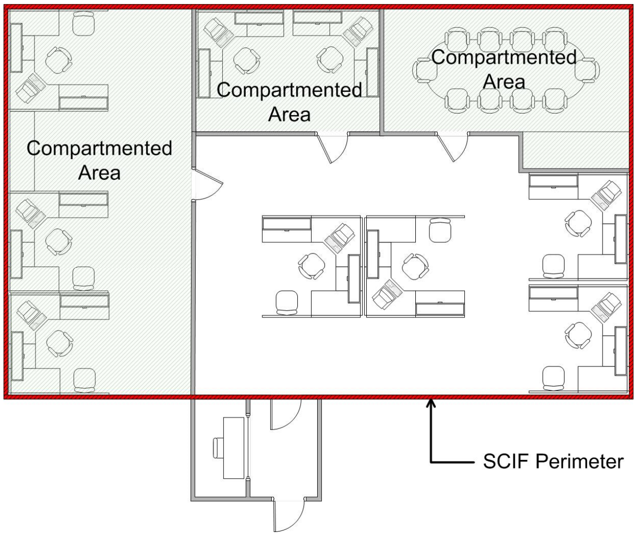
Compartmented Area (CA) is a room, a set of rooms, or an area that provides controlled separation between the compartments within a SCIF or SAPF.

- **Type I: Area where discussion is not authorized**
- **Type II & III: Room, or set of rooms that require acoustic protection**



General Design Strategy: Layout

- **ADJACENT SPACE.**
  - To increase SID, locate secure space within areas that require access control.
- **VESTIBULE.**
  - When practical, the entrance into a secure area should incorporate a vestibule to preclude visual observation and enhance acoustic protection.
  - This is not intended to be a mantrap



Specific Design Strategy: Acoustic Protection

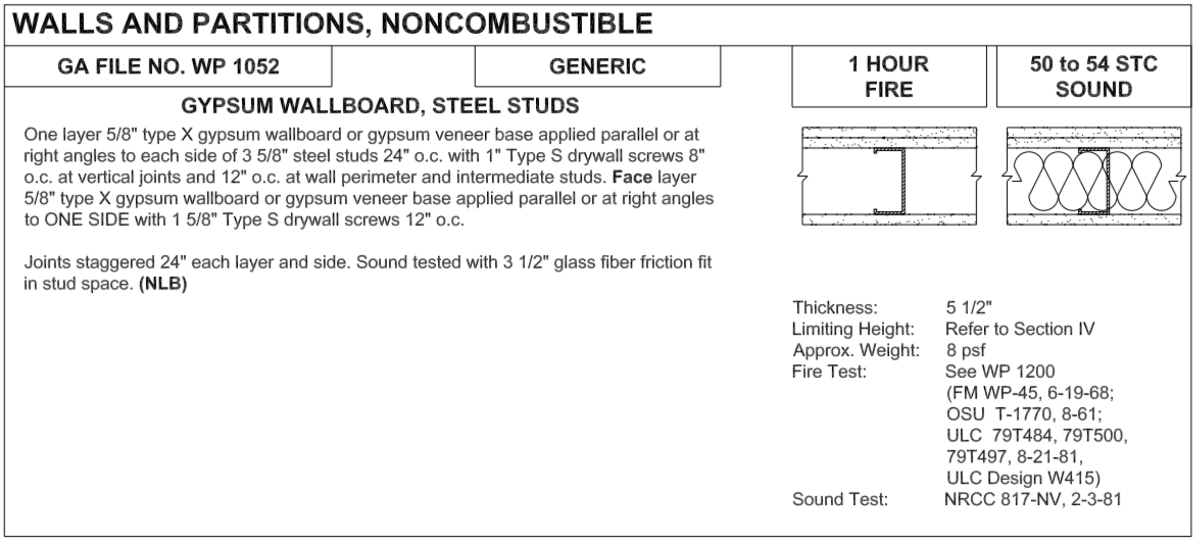
- Acoustical protection measures are designed to protect the occupants from being inadvertently overheard.
  - Not intended to protect against deliberate technical interception of audio emanations.
- The ability of a structure to retain sound within the perimeter is rated using a descriptive value, the 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.

- Sound Group ratings shall be used to describe the effectiveness of acoustical security measures afforded by various wall materials and other building components.
  - Perimeter walls shall meet Sound Group 3 (STC 45), unless additional protection is required for amplified sound.
  - Where amplified audio is used, or in rooms where multiple people discuss such as training or conference rooms shall meet Sound Group 4 (STC 50) performance criteria.
- This applies to the entire perimeter of the space to include walls floors, and ceiling and perimeter penetrations such as ducts, doors, and windows.

- Provide sound rated assemblies that are no less than STC 50 when STC 45 perimeter is required and no less than STC 55 when STC 50 perimeter is required when factory tested in accordance with ASTM E90.
  - This will ensure the sound rated assemblies meet the minimum STC requirement when installed correctly.
- UFGS 09 29 00 Gypsum Board requires ASTM E 90 laboratory Test Report for assemblies and has an option for ASTM E 336 Field Test.

Specific Design Strategy: Acoustic Protection

- Test Report, ASTM E90, *Standard Test Method for Laboratory Measurement of Airborne Sound Transmission Loss of Building Partitions and Elements*



WALLS AND PARTITIONS, NONCOMBUSTIBLE

GA FILE NO. WP 1052	GENERIC	1 HOUR FIRE	50 to 54 STC SOUND

GYPSUM WALLBOARD, STEEL STUDS

One layer 5/8" type X gypsum wallboard or gypsum veneer base applied parallel or at right angles to each side of 3 5/8" steel studs 24" o.c. with 1" Type S drywall screws 8" o.c. at vertical joints and 12" o.c. at wall perimeter and intermediate studs. **Face** layer 5/8" type X gypsum wallboard or gypsum veneer base applied parallel or at right angles to ONE SIDE with 1 5/8" Type S drywall screws 12" o.c.

Joints staggered 24" each layer and side. Sound tested with 3 1/2" glass fiber friction fit in stud space. **(NLB)**

Thickness:	5 1/2"
Limiting Height:	Refer to Section IV
Approx. Weight:	8 psf
Fire Test:	See WP 1200 (FM WP-45, 6-19-68; OSU T-1770, 8-61; ULC 79T484, 79T500, 79T497, 8-21-81, ULC Design W415)
Sound Test:	NRCC 817-NV, 2-3-81

Specific Design Strategy: Perimeter

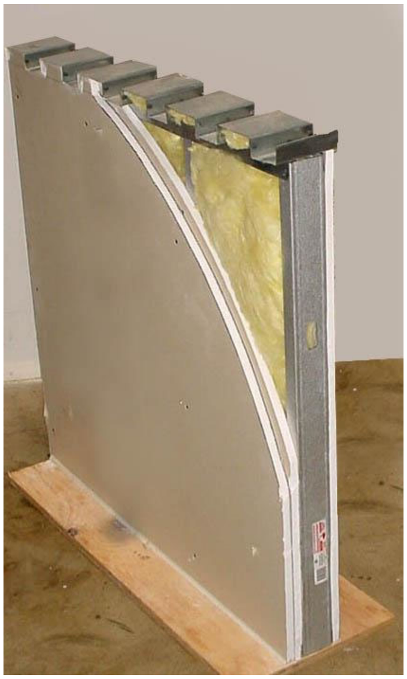
- Perimeter walls, floor and ceiling shall be permanently and solidly constructed and attached to each other.
- Perimeter walls must go from true floor to true ceiling.
- Seal partition continuously with acoustical sealant (both sides) and finished to match wall wherever it abuts another element such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

Specific Design Strategy: Perimeter

- **Painting of wall assembly**
  - In some cases, the SSM may require the paint above the false ceiling to be a different color.
- **Existing walls**
  - When an existing wall is constructed with substantial material (e.g., brick, concrete, cinderblock, etc.) equal to meet the perimeter wall construction standards, the existing wall may be utilized to satisfy the IC Tech Spec-for ICD/ICS 705.
- **CTTA recommended countermeasures (foil backed GWB or layer of approved Ultra Radiant R-Foil)**
  - Foil backed GWB may be problematic
  - Installed in accordance with *Best Practices Guideline for Architectural Radio Frequency Shielding (FOUO)*.

Specific Design Strategy: Perimeter

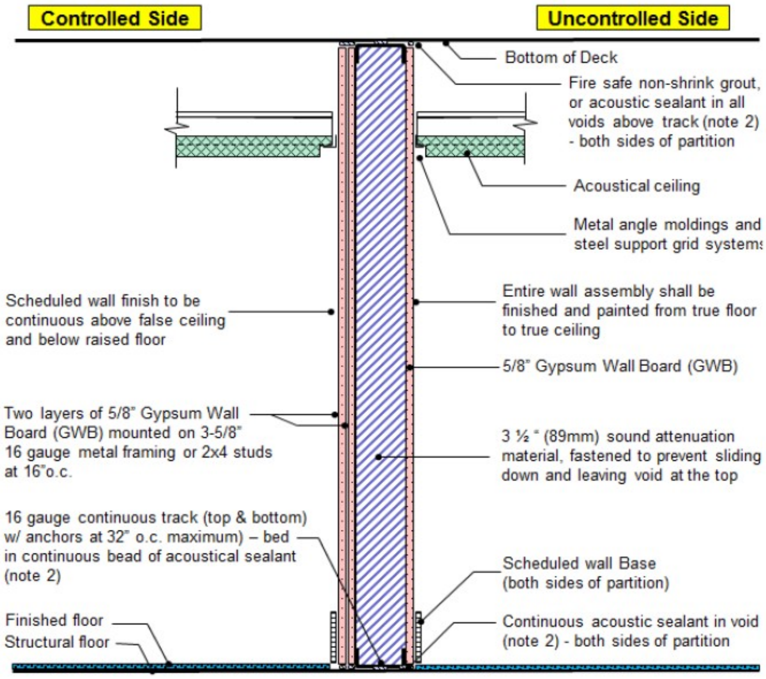
- **Wall A (Standard Wall) - Sound Group 3 (STC 45 or better)**
  - 3-5/8” metal or 2 x 4 wood studs.
  - Continuous runners (same gauge as studs) attached to true floor and true ceiling.
  - Three layers of 5/8 inch foiled back Type X gypsum, one layer on the outside and two on the inside of the SCIF wall. When R-foil or foil back gypsum is employed, it shall be placed inside the secure area 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 Suggested Construction for Standard Wall

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.
- 16 gauge continuous track (top & bottom) w/ anchors at 32" o.c. maximum) – bed in continuous bead of acoustical sealant.
- Any utilities required on the perimeter wall shall be surface mounted.



Controlled Side

Uncontrolled Side

Bottom of Deck

Fire safe non-shrink grout, or acoustic sealant in all voids above track (note 2) - both sides of partition

Acoustical ceiling

Metal angle moldings and steel support grid systems

Scheduled wall finish to be continuous above false ceiling and below raised floor

Entire wall assembly shall be finished and painted from true floor to true ceiling

5/8" Gypsum Wall Board (GWB)

Two layers of 5/8" Gypsum Wall Board (GWB) mounted on 3-5/8" 16 gauge metal framing or 2x4 studs at 16"o.c.

3 ½ " (89mm) sound attenuation material, fastened to prevent sliding down and leaving void at the top

16 gauge continuous track (top & bottom) w/ anchors at 32" o.c. maximum) – bed in continuous bead of acoustical sealant (note 2)

Scheduled wall Base (both sides of partition)

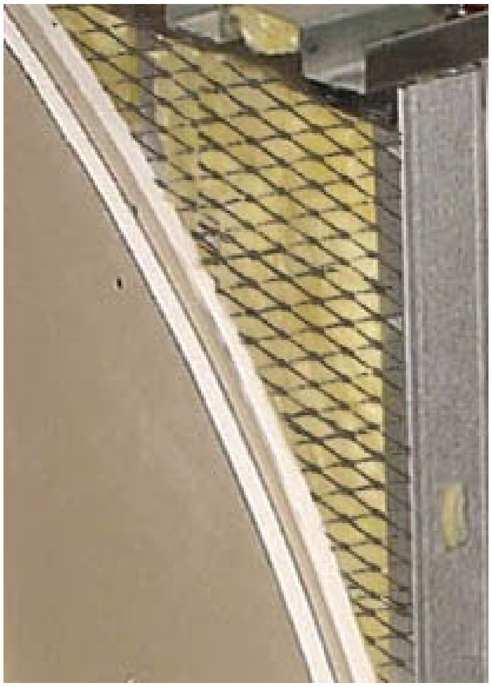
Finished floor

Structural floor

Continuous acoustic sealant in void (note 2) - both sides of partition

Specific Design Strategy: Perimeter

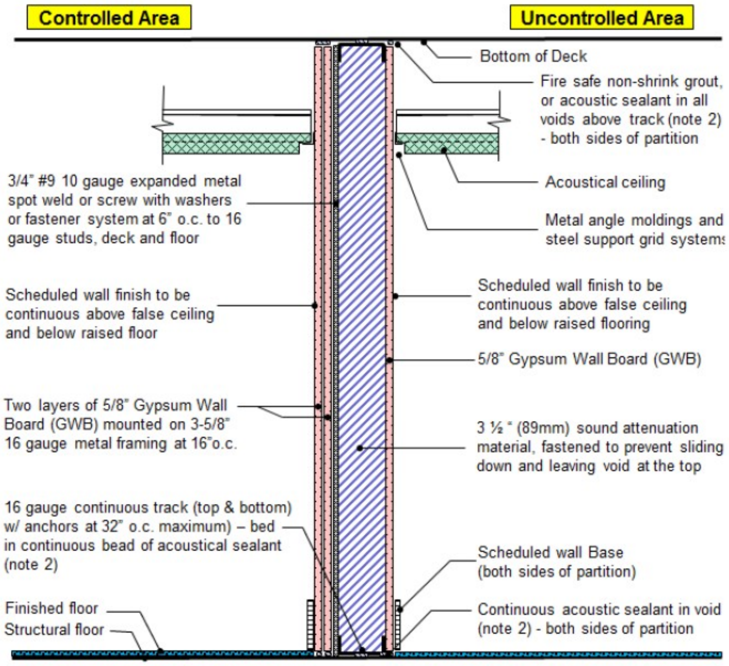
- **Wall B (Enhanced Wall) Expanded Metal Sound Group 3 (STC 45 or better):**
  - Same as Wall A except:
    - Metal studs and runners shall be 16 gauge.
    - Wood or Metal Studs shall be 16" on center.
    - Provide ¾" #9 (10 gauge) case hardened expanded metal affixed to the interior side of SCIF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



Wall B Suggested Construction for Expanded Metal

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

- CTTA recommended countermeasures (foil bracketed wallboard or R-foil shall be installed in accordance with Best Practices for Architectural Frequency (RF) Shielding.
- Any utilities required on wall shall be surface mounted.


Controlled Area
Uncontrolled Area
Bottom of Deck
Fire safe non-shrink grout, or acoustic sealant in all voids above track (note 2) - both sides of partition
Acoustical ceiling
Metal angle moldings and steel support grid systems
3/4" #9 10 gauge expanded metal spot weld or screw with washers or fastener system at 6" o.c. to 16 gauge studs, deck and floor
Scheduled wall finish to be continuous above false ceiling and below raised floor
Scheduled wall finish to be continuous above false ceiling and below raised flooring
5/8" Gypsum Wall Board (GWB)
Two layers of 5/8" Gypsum Wall Board (GWB) mounted on 3-5/8" 16 gauge metal framing at 16"o.c.
3 ½ " (89mm) sound attenuation material, fastened to prevent sliding down and leaving void at the top
16 gauge continuous track (top & bottom) w/ anchors at 32" o.c. maximum) – bed in continuous bead of acoustical sealant (note 2)
Scheduled wall Base (both sides of partition)
Finished floor
Structural floor
Continuous acoustic sealant in void (note 2) - both sides of partition

Specific Design Strategy: Perimeter

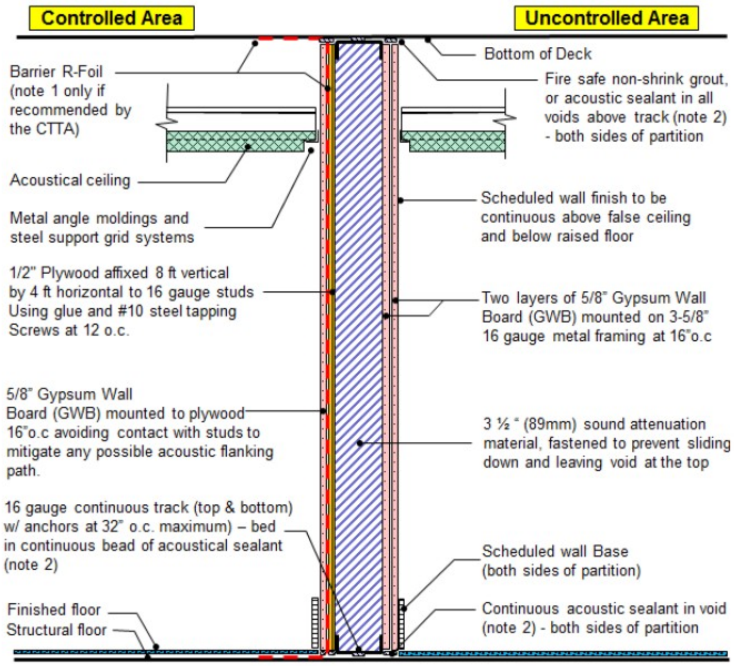
- Wall C (Enhanced Wall) Perimeter walls with Fire Rated Plywood:
  - Wall assembly the same as Wall B except:
  - One layer of 5/8" thick "fire retardant" plywood shall be substituted for expanded metal and first interior layer of gypsum board on the interior side of the SCIF wall assembly.
  - The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

- Wall C with Fire Rated Plywood is sometimes preferred over Expanded Metal for enhanced walls to mitigate against surreptitious entry.

Wall C Suggested Construction for Plywood (Fire Rated)

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

- CTTA recommended countermeasures (foil backed wallboard or R-foil shall be installed in accordance with Best Practices for Architectural Frequency (RF) Shielding.
- Any utilities required on wall shall be surface mounted.


Controlled Area
Uncontrolled Area
Bottom of Deck
Barrier R-Foil (note 1 only if recommended by the CTTA)
Fire safe non-shrink grout, or acoustic sealant in all voids above track (note 2) - both sides of partition
Acoustical ceiling
Metal angle moldings and steel support grid systems
Scheduled wall finish to be continuous above false ceiling and below raised floor
1/2" Plywood affixed 8 ft vertical by 4 ft horizontal to 16 gauge studs Using glue and #10 steel tapping Screws at 12 o.c.
Two layers of 5/8" Gypsum Wall Board (GWB) mounted on 3-5/8" 16 gauge metal framing at 16"o.c
5/8" Gypsum Wall Board (GWB) mounted to plywood 16"o.c avoiding contact with studs to mitigate any possible acoustic flanking path.
3 ½ " (89mm) sound attenuation material, fastened to prevent sliding down and leaving void at the top
16 gauge continuous track (top & bottom) w/ anchors at 32" o.c. maximum) – bed in continuous bead of acoustical sealant (note 2)
Scheduled wall Base (both sides of partition)
Finished floor
Structural floor
Continuous acoustic sealant in void (note 2) - both sides of partition

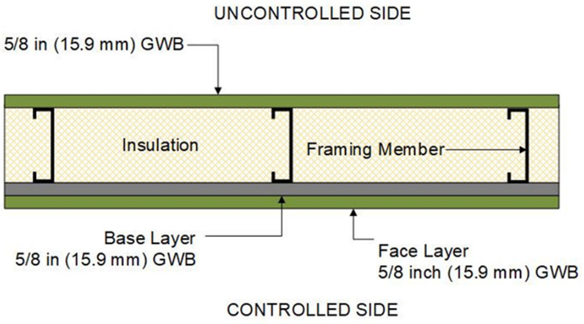
Specific Design Strategy: Perimeter

- IC Tech Spec-for ICD/ICS 705 indicates Standard STC 45 wall requires three layers of 5/8 inch (15.9 mm) gypsum wallboard (GWB). One layer on the uncontrolled side (outside) of the protected area and two layers on the controlled side (interior) of the protected area to meet STC 45, STC 50 wall requires four layers. Two layers on the outside and two layers on the inside.
  - Stagger joints on the opposite sides of a partition so they are not on the same stud.
  - Install the GWB so that the joints of the face layer are offset from the joints of the base layer.
  - Joints in the face layer that are parallel to the framing members must fall over the framing members and offset from the base layer.
    - Exception: When using adhesive between the layers, joints in the face layer do not have to occur over the framing member.

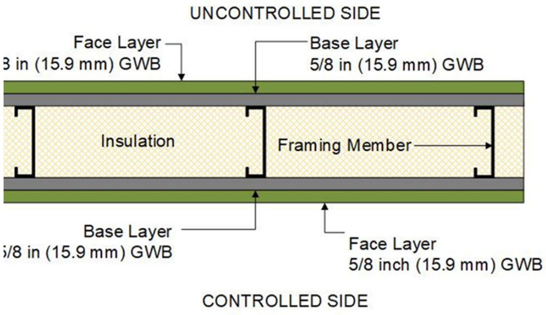
Specific Design Strategy: Perimeter

- **Wall Assembly**
  - **Use fibrous insulation to improve the sound isolating performance of the system.**
    - Do not over pack the insulation. Over-packing the cavity may decrease the performance.
    - The use of spray foam or other hardening insulations may decrease the sound performance.

STC 45 Assembly

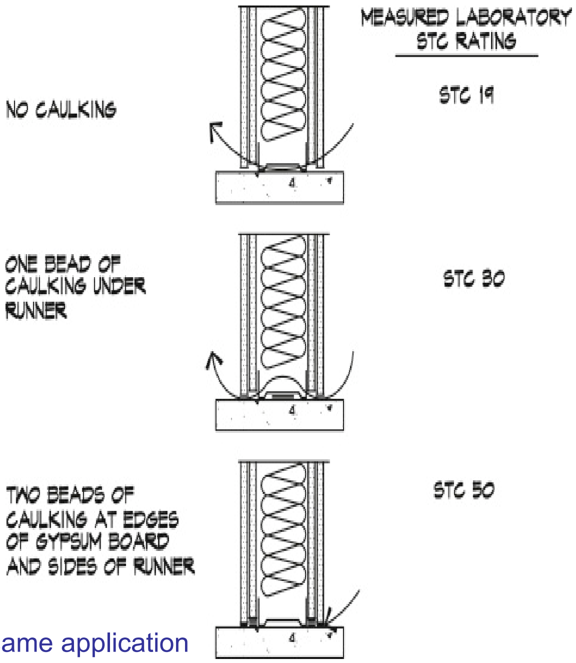


STC 50 Assembly



Specific Design Strategy: Perimeter

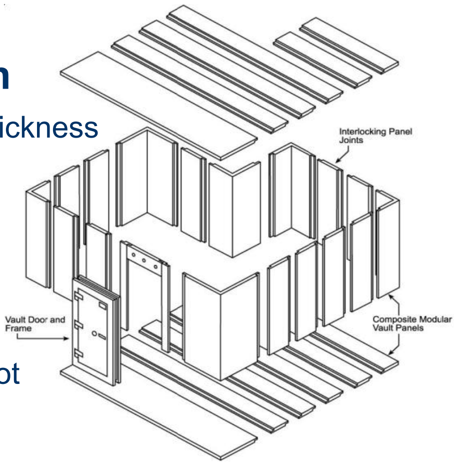
- **Gypsum board panels are lifted into using a spacer under their bottom edge, so there is a small gap at the bottom.**
- **Sealing openings is critical to acoustical performance. Seal gaps with a non-hardening caulk so the acoustical rating of the wall is maintained**
  - Minimum – Continuous sealant each side of track
  - Better – Continuous sealant each side of track and bottom of track
  - Best – Continuous sealant bottom of track, multiple sealant beads (one on each side of track and at finish wall board)


MEASURED LABORATORY STC RATING
NO CAULKING
STC 19
ONE BEAD OF CAULKING UNDER RUNNER
STC 30
TWO BEADS OF CAULKING AT EDGES OF GYPSUM BOARD AND SIDES OF RUNNER
STC 50

Continuous sealant shown at sill, but same application occurs at top of partition / underside of decking/slab

Specific Design Strategy: Vault Construction

- **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**



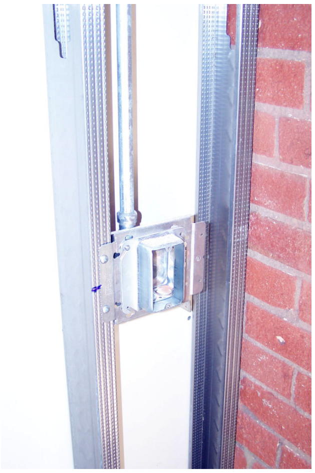
Minimum Wall Construction and Alarm

	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.

Specific Design Strategy: Utilities

- Utilities such as power, Telecommunications, signal, or plumbing on the perimeter wall treated for acoustic or RF must be surface mounted or provide a furred out wall 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.



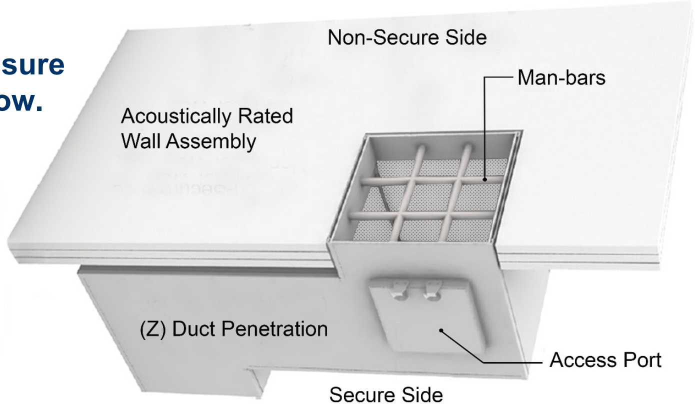
Specific Design Strategy: Utilities

Specific Design Strategy: Utilities

- Vents, ducts, conduits, pipes, or anything that penetrate the perimeter present a vulnerability that needs to be addressed.
- Penetrations of the perimeter must 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 perimeter wall (inside wall).

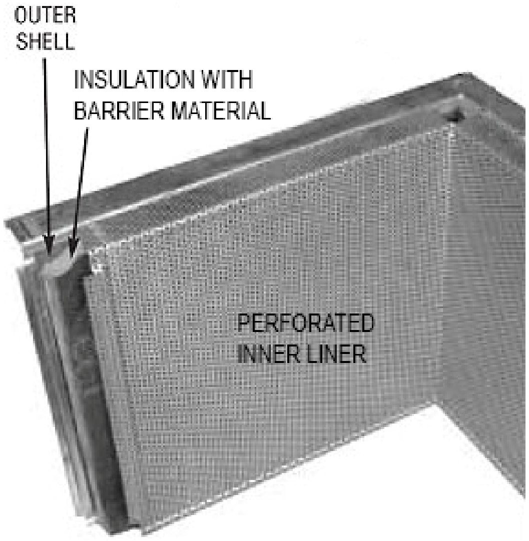
Specific Design Strategy: Utilities

- Vents and Ducts
  - All vents and ducts must be protected to meet the acoustic requirements
  - To ensure acoustic performance of the perimeter is not compromised, provide sound baffles (duct silencers) or (Z) Duct Penetrations.
  - IC Tech Spec – for ICD/ICS 705 provides an example of a (Z) Duct Penetration.
  - Coordinate selection with Mechanical Engineer to insure fan sizing for proper air flow.



Specific Design Strategy: Utilities

- Vents and Ducts
  - Beware, IC Tech Spec – for ICD/ICS 705 indicates acoustically lined duct. Per UFC 3-410-01, acoustical duct liner is not allowed.
  - In lieu of acoustical duct liner, provide double wall acoustic duct.
  - For contamination protection, include a barrier material between the perforated liner and the insulation designed to prevent air quality issues caused by bacteria and other contaminates that can embed in the insulation.

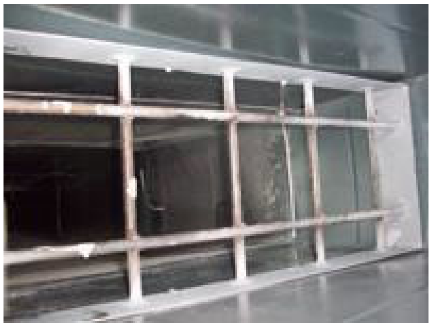


Specific Design Strategy: Utilities

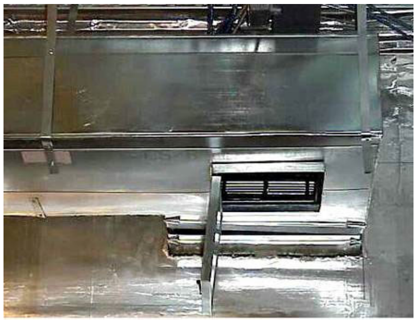
- VENT, PIPE, AND DUCT OPENINGS :
  - All vents or duct openings exceeding 96 square inches that penetrate the perimeter shall be protected with permanently affixed bars, grills, metal sound baffles or waveguides.
    - If one dimension of the penetration measures less than 6 inches, bars or grills are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

Specific Design Strategy: Utilities

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



MANBARS



INSPECTION PORT

Specific Design Strategy: Utilities

- Utilities (power & signal) should enter the perimeter at a single point.
  - All utility penetrations must be sealed to mitigate acoustic emanations and covert entry.
  - Spare conduits are allowed for future expansion provided the expansion conduit is filled with acoustic fill and capped.
- Utilities servicing areas other than SCIF/SAPF shall not transit the perimeter unless mitigation is provided.

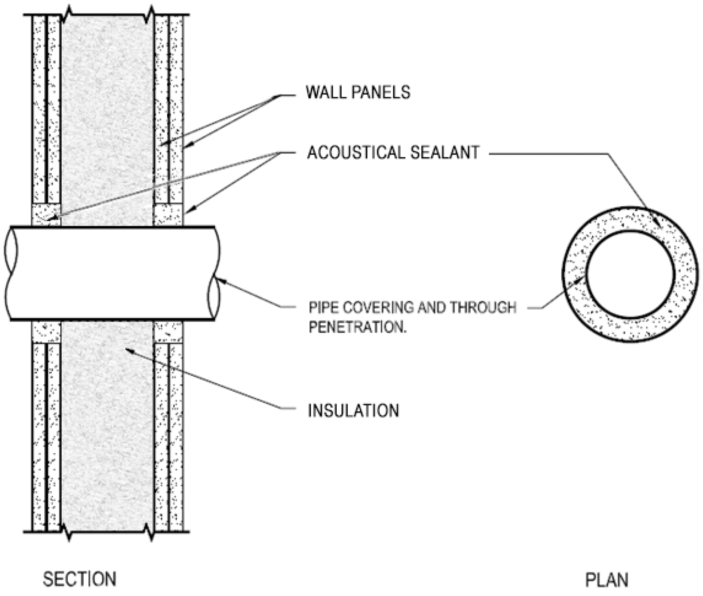
Specific Design Strategy: Utilities

- Metallic penetrations through the perimeter may be considered carriers of compromising emanations (CE) and require TEMPEST countermeasures. Unless directed otherwise by the CTTA:
  - Metallic conduit: install dielectric union adjacent to the pipe penetration through the perimeter wall (inside wall), or ground the conduit using a no. 4 wire (0.2043-diameter copper wire) to the building grounding system.
  - Metallic sprinkler (fire suppression) pipes: ground using a no. 4 wire (0.2043-diameter copper wire) to the building grounding system.
  - Mechanical system refrigerant lines: ground the line using a no. 4 wire (0.2043-diameter copper wire) to the building grounding system.

Specific Design Strategy: Utilities

- **Acoustic Sealing for Pipe Penetration**
  - **Same principle for Conduit**

- Apply 1/4" minimum round bead of sealant (5/8" maximum) to seal perimeter of sound-rated partition.
- Seal sound-rated partitions on both sides.

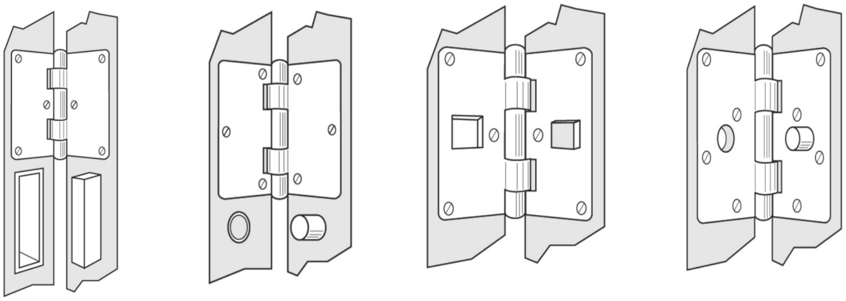


Specific Design Strategy: Doors

- **PERIMETER DOORS:**
  - **Doors and frame assemblies must meet acoustic requirements (vestibule of two doors may be used) unless declared a non-discussion area.**
    - This is problematic for roll up and double doors.
  - **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: Doors

- **PERIMETER DOORS: Shall be equipped with an automatic heavy duty door closer with controls to prevent unauthorized entry.**
  - **Perimeter doors with day access controls shall be dead bolted at night or meet the primary entrance door requirements.**
  - **Hinge pins on perimeter 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: Doors

- **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**

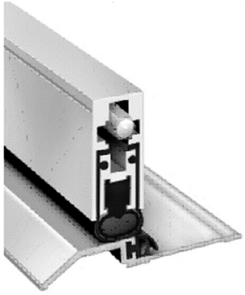
Specific Design Strategy: Doors

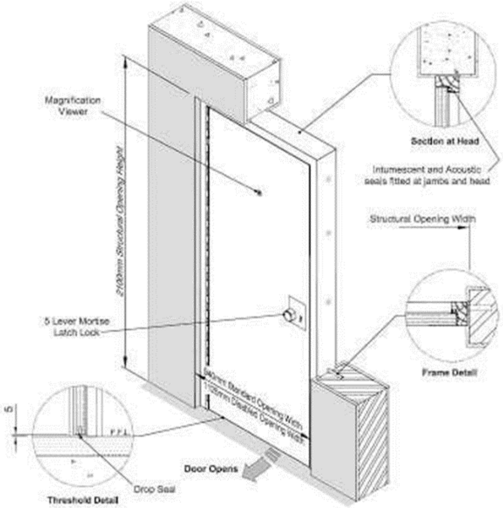
- **1 ¾ inch thick solid core wood or composite doors will not meet STC 45 rating.**
  - **1 ¾" Solid core door – factory sealed**
    - Best STC obtainable = 38 STC
  - **1 ¾" Solid core door – field assembly**
    - Best STC obtainable = 35 STC
  - **2" Solid core door – factory sealed**
    - Best 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.**

Specific Design Strategy: Doors

- **In order to obtain a true STC 45 or 50 rated door specify an acoustical doors assembly using UFGS 08 34 73 *Sound Control Door Assemblies* to include door, seals, hinges, and threshold.**
  - UFGS 08 34 73 requires third party laboratory testing in accordance with ASTM E-90 and field testing in accordance with ASTM E336



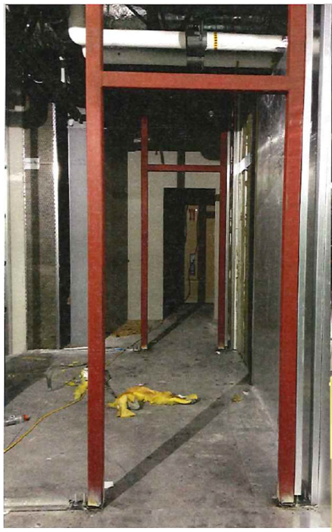

Magnification Viewer
2100mm Structural Opening Height
Section at Head
Intumescent and Acoustic seals fitted at jambs and head
Structural Opening Width
5 Lever Mortise Latch Lock
Frame Detail
940mm Standard Opening Width
1105mm Disabled Opening Width
5
F F L
Door Opens
Drop Seal
Threshold Detail

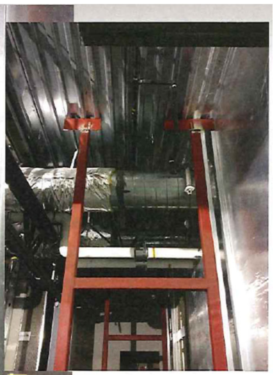
Specific Design Strategy: Doors

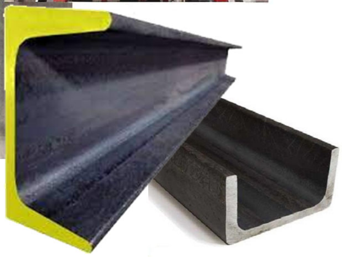
- **To ensure the sound rated assemblies meet the minimum STC requirement when installed.**
  - **Provide sound rated assemblies that are factory tested in accordance with ASTM E90 that are no less than:**
    - STC 50 when STC 45 is required
    - STC 55 when STC 50 is required.
  - **ASTM E336, Standard Test Method for Measurement of Airborne Sound Attenuation between Rooms in Buildings allows for a -5 STC. i.e. if a field test indicates 40 STC for a 45 STC rated assembly, it would pass the ASTM E336 testing criteria.**

Specific Design Strategy: Doors

- Acoustical rated door assemblies are much heavier than typical doors and require additional structural support.
  - Coordinate design of structural support with a Structural Engineer.
  - Install in door assembly in accordance with UFGS 08 34 73 and manufacturer's instructions.







For acoustics
Use Structural C or U Channel in lieu of tubing

Specific Design Strategy: Doors

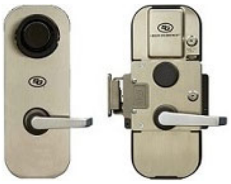
[redacted]

Specific Design Strategy: Primary Entrance

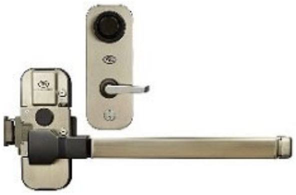
- Typically, one primary entrance where visitor control is conducted.
  - Should incorporate a vestibule to preclude visual observation and enhance acoustic protection.
  - Equipped with an approved automated access control device.
  - Equipped with a GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L- 2890 and combination lock meeting Federal Specification FF-L 2740A. Note: FF-L-2890 requires FF-L 2740A combination lock for primary and secondary entrance.
- Elevators cannot meet the primary entrance or perimeter door requirements.

Specific Design Strategy: Door Hardware

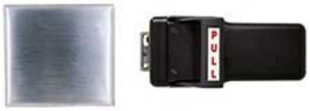
- There are several types of FF-L-2890 hardware!
  - Need to know
    - Is the hardware for Primary, Secondary or Exit Only?
    - Will the door hardware need to have capability for use with access control, or will access control be stand-alone?
  - Provide a key override in the event of a malfunction or loss of power to the automated access control device.



Type I, Primary Door
ADA Compliant
Stand-alone access control



Type IV, ADA Compliant
panic hardware
Integrated access control



Type IX, ADA Compliant
Exit Only (Deadbolt)

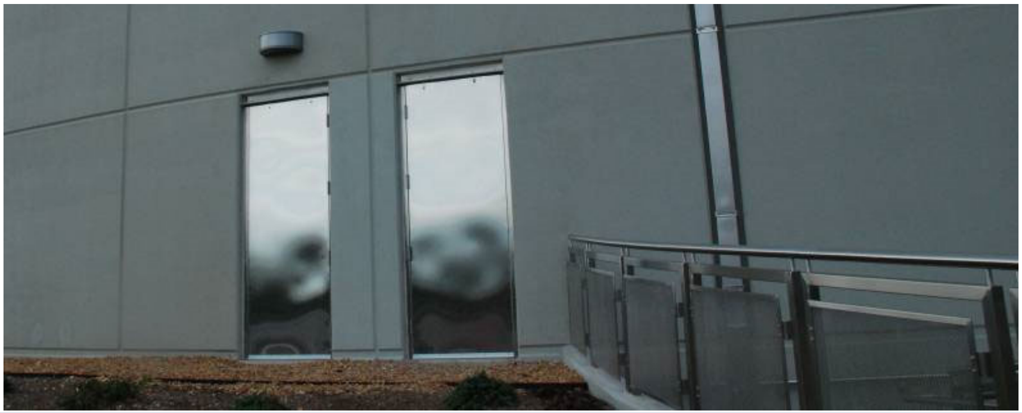
For information refer to DoD Lock Program for types

Specific Design Strategy: Doors

- ROLL-UP DOORS: Can only be located in an area 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 either door to prevent observation through the opening between the doors.
  - Alarm each door (have a balanced magnetic switch).
  - Install a GSA approved lock on the moving door.

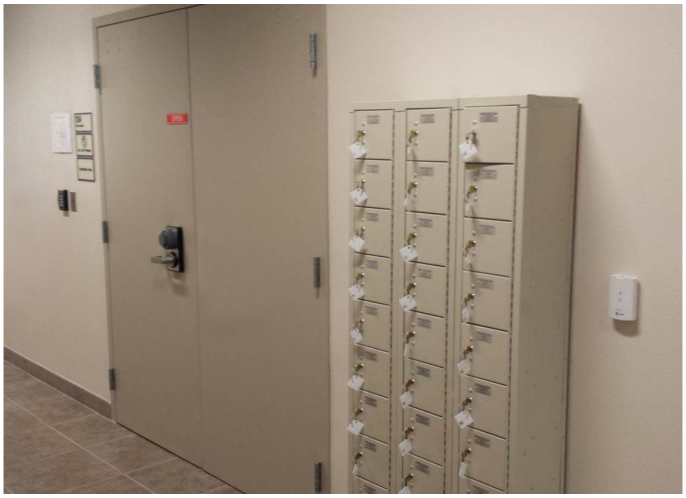
Specific Design Strategy: Doors

- EMERGENCY EXIT DOORS: Must meet perimeter door requirements and:
  - Have no exterior hardware.
  - Secured with deadlocking panic hardware (FED Spec FF-L-2890).
  - Alarmed 24/7 and equipped with a local annunciation.
  - Delayed-egress may be permitted with NFPA 101 compliance.



Specific Design Strategy: Storage

- Storage at Primary Entrance
  - No Personal Electronic Devices (PED) allowed within Secure area.
  - PED cabinets cannot be located within 10 ft. (3 m) of equipment processing unencrypted NSI.



Specific Design Strategy: Windows

- Every effort should be made to minimize windows, especially on the ground floor. When used, windows must be:
  - Non-opening
  - Provide visual protection
  - Provide acoustic protection
  - Include TEMPEST requirements when recommended by CTTA.
- 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 perimeter.
  - Be protected against forced entry.
  - Be alarmed.

Specific Design Strategy: Daylighting

- Secure facilities are not inherently exempt from the high-performance building requirements of UFC 1-200-02.
  - If provided, daylighting must be coordinated with supported command and the SSM.
  - There are spaces that cannot have daylit due to operational considerations.
- When providing daylighting, design fenestration to be non-opening, provide visual and acoustic protection and include TEMPEST requirements when recommended by CTTA.

Specific Design Strategy: Daylighting

- Promote access to daylight in lobbies, perimeter stairwells, breakrooms and other common spaces.

Specific Design Strategy: Daylighting

- For visual protection, design must eliminate line of sight into secure areas via angles or with translucent glazing, curtain walls, clerestories, skylights, glass unit masonry, fiberglass panels or other lightweight plastics.

Specific Design Strategy: Daylighting

- Daylighting Penetrations less than 18 feet (5.5 meters)
  - Daylighting penetrations that are less than 18 feet (5.5 meters) (measured from the bottom of the penetration) above the ground or from the nearest platform; such as lower roof, canopy or mechanical equipment, which affords access to the penetration must:
    - Meet the standards of the perimeter
    - Protected against forced entry
    - Be alarmed
  - If one dimension of the penetration measures less than 6 inch (150 mm), forced entry protection and alarm is not required.

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, place lights to ensure visual observation by SCIF personnel and place controls inside the SCIF at each door including emergency exit doors.

Specific Design Strategy: Telecommunications

- **Telecommunication Cabling System:**
  - Coordinate requirements with Supported Command, SSM and service provider.
  - Cabling, patch panels, connector blocks, work area outlets, and cable connectors must be color coded to distinguish classification level or cabling must be clearly marked to indicate their classification level.
  - Cabling must enter at a single location and be identified and labeled with its purpose and destination at the point of entry.
  - Backbone and horizontal cabling may differ depending on network classification, service provider, and TEMPEST requirement.

Specific Design Strategy: Fire Alarm and Mass Notification System (MNS)

- The introduction of electronic systems that have components outside the secure area should be avoided. Speakers or other transducers, which are part of a system that is not wholly contained in the secure area, are sometimes required for Life Safety 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 must penetrate the SCIF perimeter at one point.
  - In systems that require notification only, the system must have a high gain buffer amplifier.
  - In systems that require two-way communication, the system must have electronic isolation. Occupants must be alerted when the system is activated.
  - When required, provide all electronic isolation components within the perimeter as near to the point of penetration as possible.

General Design Strategy: Electronic Security System (ESS)

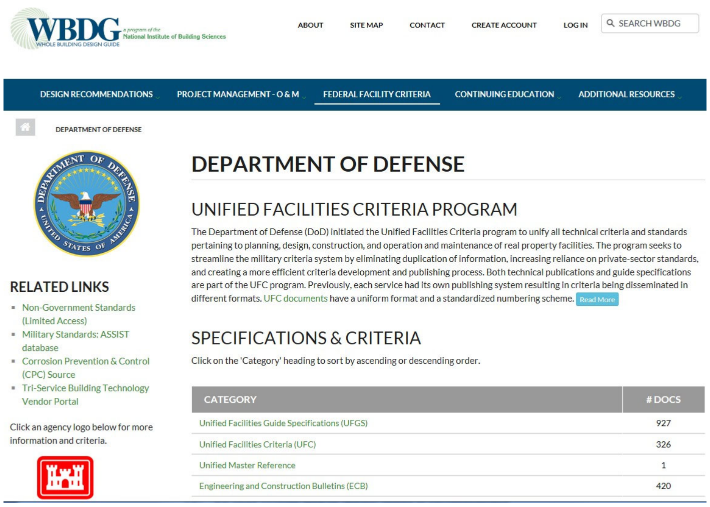
- Requirements for IDS for the protection of SCI are contained in IC Tech Spec-for ICD/ICS 705.
- Design criteria for IDS is contained in Unified Facilities Criteria (UFC) 4-021-02, *Electronic Security Systems* available on the Whole Building Design Guide website.
- Guidance on coordination for Electronic Security System (ESS) equipment procurement and installation is contained in BMS B-1.3, *Operational Outfitting Considerations* Available on the NAVFAC Portal.

Specific Design Strategy: ESS

- **IDS installation, related components, and monitoring stations shall comply with Underwriters Laboratories (UL) 2050 Extent 3 standards.**
  - **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 materials are restricted and only distributed to those demonstrating relevant national industrial security involvement.**

Specific Design Strategy: ESS

- **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).**
  - **“Non-Government Standards (Limited Access)” link is on the DoD page under Related Links on Whole Building Design Guide Website:**


WBDG
WHOLE BUILDING DESIGN GUIDE
a program of the National Institute of Building Sciences
ABOUT
SITE MAP
CONTACT
CREATE ACCOUNT
LOG IN
SEARCH WBDG
DESIGN RECOMMENDATIONS
PROJECT MANAGEMENT - O & M
FEDERAL FACILITY CRITERIA
CONTINUING EDUCATION
ADDITIONAL RESOURCES
DEPARTMENT OF DEFENSE
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
Read More

DEPARTMENT OF DEFENSE

UNIFIED FACILITIES CRITERIA PROGRAM

The Department of Defense (DoD) initiated the Unified Facilities Criteria program to unify all technical criteria and standards pertaining to planning, design, construction, and operation and maintenance of real property facilities. The program seeks to streamline the military criteria system by eliminating duplication of information, increasing reliance on private-sector standards, and creating a more efficient criteria development and publishing process. Both technical publications and guide specifications are part of the UFC program. Previously, each service had its own publishing system resulting in criteria being disseminated in different formats. UFC documents have a uniform format and a standardized numbering scheme.

RELATED LINKS

- Non-Government Standards (Limited Access)
- Military Standards: ASSIST database
- Corrosion Prevention & Control (CPC) Source
- Tri-Service Building Technology Vendor Portal

Click an agency logo below for more information and criteria.

SPECIFICATIONS & CRITERIA

Click on the 'Category' heading to sort by ascending or descending order.

CATEGORY	# DOCS
Unified Facilities Guide Specifications (UFGS)	927
Unified Facilities Criteria (UFC)	326
Unified Master Reference	1
Engineering and Construction Bulletins (ECB)	420

Specific Design Strategy: ESS

- Extent Number 3 protection shall consist of any of the following methods. An alarm system can utilize a single method or any combination of methods:
  - Perimeter Only – Full protection of all accessible openings.
  - Motion Detection – Contact protection of all accessible doors leading from the premises and a system of intrusion detection in all sections of each enclosed area that has exterior openings so as to detect movement.
  - Sound Detection – Contact protection of all accessible movable openings leading from the premises and a sound detection system in all sections of each enclosed area that has exterior openings
  - Channels – Contact protection of all movable accessible openings leading from the premises and a system of invisible beams or motion detectors arranged so that the minimum length of the beams or motion detection is equal to the longest dimension of each enclosed area that has an exterior opening. The channels shall be arranged to provide the most effective coverage of the premises. A channel of protection along one wall, with or without openings, does not meet the intent of this requirement.

Specific Design Strategy: ESS

- Intrusion Detection System Requirements:
  - Protect all Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, unless continuously occupied.
    - These adjacent areas do not need IDS protection if the AO determines that a facility’s security programs consist of layered and complementary controls sufficient to deter and detect unauthorized entry and movement.
  - IDS shall be separate from, and independent of, fire, smoke, radon, water, and other systems.
  - Doors without access control systems and that are not under constant visual observation shall be continuously monitored by the IDS.
  - Emergency exit doors shall be alarmed and monitored 24 hours a day.
  - Perimeter doors shall be protected by an HSS and a motion sensor.

Specific Design Strategy: ESS

- **Intrusion Detection System Requirements**
  - **If a monitoring station is responsible for more than one IDS, there must be an audible and visible annunciation for each IDS.**
  - **If the IDS incorporates an access control system (ACS), notifications from the access control system must 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: ESS

- **Intrusion Detection System Sensors**
  - **Motion Detection Sensors**
    - UL 639 listed
    - Dual-Technology Sensors may be used when authorized and each technology transmits alarm conditions independent of the other technology.
  - **Point Sensors**
    - UL 634 High Security Switches (HSS) level II.
      - Level II rated switches include Balanced Magnetic Switches (BMS) that pass additional performance testing.

Specific Design Strategy: ESS

- **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 4-021-01, Electronic Security Systems for more on system design including tamper protection.**

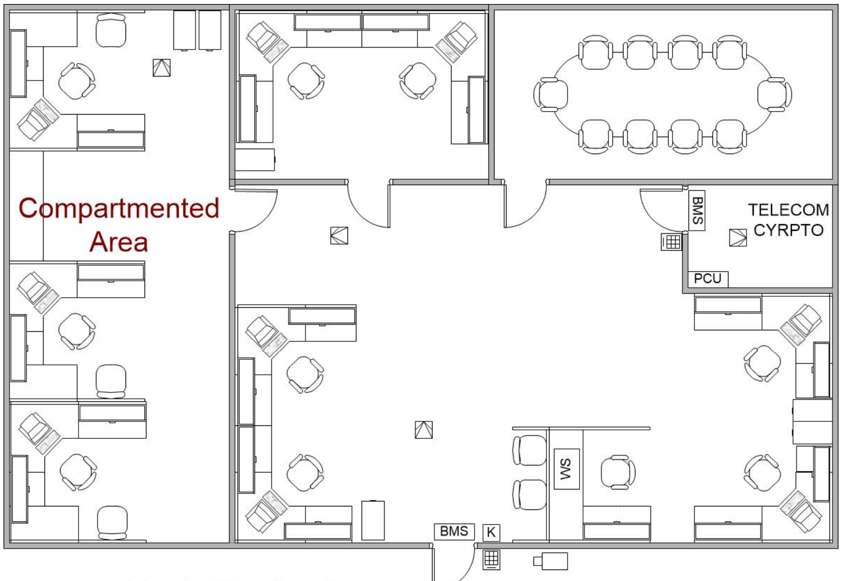
Specific Design Strategy: ESS

- **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 batteries, uninterruptible power supply (UPS), 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: ESS

- Access Control Systems
  - Access is restricted to authorized personnel.
  - Access control is accomplished by visual recognition or through use of an automated access control system
    - Automated access control systems must use at least two technologies (badge, PIN, or biometric)
      - Default is a CAC compatible card reader compatible with Keypad
  - Access control methods must be approved by the Accrediting Official (AO).

Specific Design Strategy: ESS



K Arm/Disarm Keypad

PCU Processing Control Unit

BMS High Security Level 2 Balance Magnetic Switch

⊠ Motion Detector

▦ Cardreader w/Keypad

▭ Camera (Optional)

WS ACS Admin Workstation (Maybe at Alternate Location)

Specific Design Strategy: ESS

- **Based on the regulatory requirements, the standard practice is:**
  - **Focus ESS protection at the perimeter of the secure spaces.**
  - **Every perimeter door will have a Level II high security switch and a motion sensor.**
  - **Any window below 18' will be protected with a level II high security switch (if operable) and a be protected with a motion sensor.**
  - **In addition, strategically place motion sensors to protect the interior areas through which reasonable access could be gained, including walls common to areas can be protected by a motion sensor.**
    - This does not mean 100% coverage.
    - Protection can be accomplished by placement directly over the protected assets or in hallways or other restricted passage ways leading to classified/sensitive assets

Specific Design Strategy: ESS

- **IDS Equipment Installation, Testing, and Training**
  - **IDS installation plans shall be restricted as documented in the CSP.**
  - **IDS Approval**.
    - The AO will approve IDS proposals and plans prior to installation as part of the construction approval process.
    - Final system acceptance testing shall be included as part of the accreditation package.

Specific Design Strategy: ESS

- **IDS Equipment Installation, Testing, and Training**
  - **For Installations inside the United States:**
    - Performed by U.S. companies using U.S. citizens with a trustworthiness determination.
      - Trustworthiness determination per DoDM 5100.01
  - **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.

Specific Design Strategy: 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 facility contains equipment that will be processing national security information (NSI).**

- **Certified TEMPEST Technical Authority (CTTA) has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures.**

Specific Design Strategy: TEMPEST

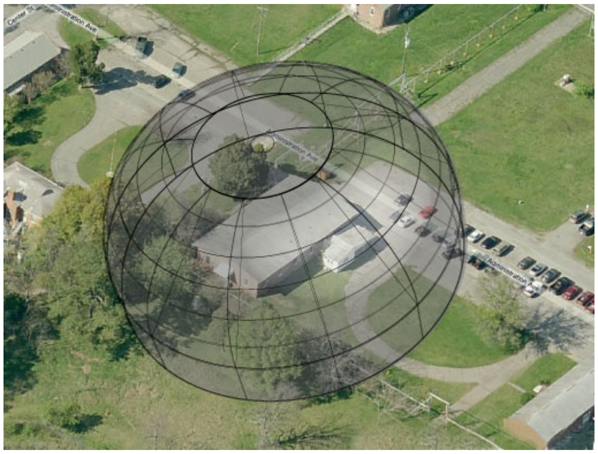
- Failure to consult the CTTA could result in installation of unnecessary and/or expensive countermeasures or the omission of needed countermeasures.
- Request the SSM get the CTTA involved during the planning phase!
  – SSM must submit the TEMPEST Addendum (TEMPEST Checklist) with the FCC.
  – TEMPEST Countermeasures are documented in the TEMPEST Countermeasure review (TCR) and approved by the AO.

Specific Design Strategy: TEMPEST

- To initiate a TEMPEST Countermeasure Review (TCR), the SSM will submit a TEMPEST Addendum to the FFC.
- In conducting TEMPEST countermeasure review, the CTTA will 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
- DOR/PM will need to provide the SSM site plans and building floorplans to assist CTTA in the evaluation of inspectable space.

Specific Design Strategy: TEMPEST

- The CTTA shall determine the Inspectable Space for a facility.
  - 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.
  - Typically, this is the building or Secure perimeter



Specific Design Strategy: TEMPEST

- RED/BLACK concept:
  - 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.
  - DoDM 5105.21 Vol 2 references National Security Telecommunications Information System Security Advisory Manual 2-95 & 2-95A, “RED/BLACK Installation Guidance for Red/Black guidelines.
  - Project specific requirement will be documented in the TCR.

Specific Design Strategy: TEMPEST

- **When Shielding is required:**
  - **Provide foil backed GWB or R-Foil in accordance with *Best Practices Guideline for Architectural Radio Frequency Shielding*.**
  - **Foil backed GWB may be problematic.**
  - **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 space between the first and second layer of gypsum board.**

  - **Don't forget ceiling, floor, penetrations, and connections. Remember, six-sided approach!**
  - **Completely shielded floor may not be required for slab on grade.**

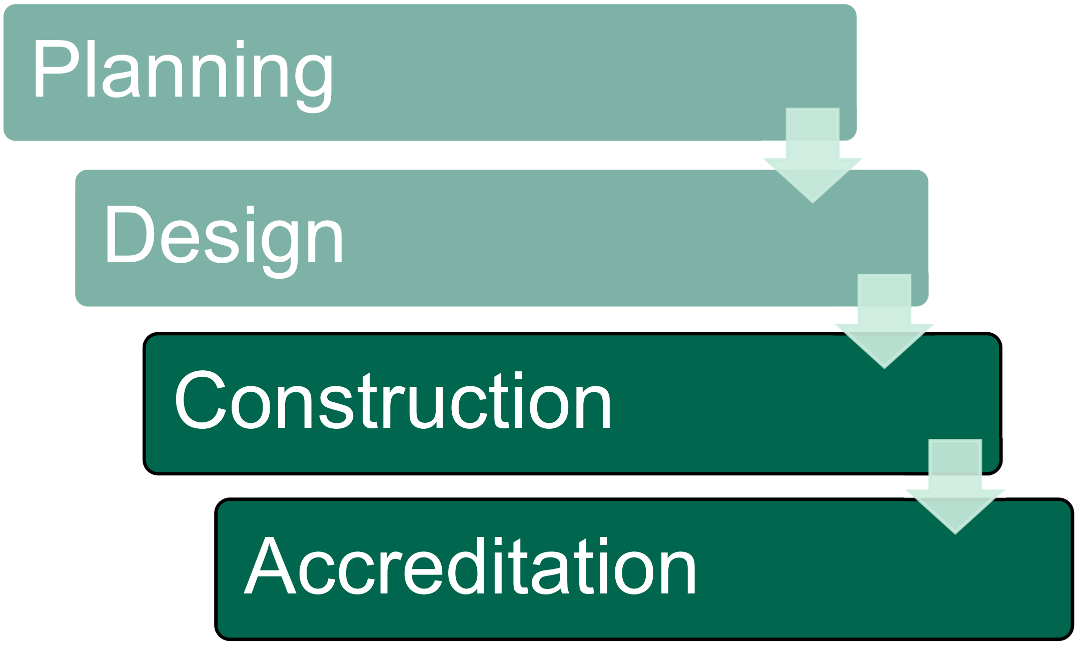
Specific Design Strategy: TEMPEST

- **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.

Design Approval

- In accordance with Tech Spec of ICD 705 prior to construction:
  - Final Design must be submitted to the SSM and approved by AO.
  - CSP must be approved by AO.

Project Phases



Planning

Design

Construction

Accreditation

Construction Security Plan (CSP)

- Documents the security requirements for each project.
- Prepared by Site Security Manager (SSM) (not construction contractor or NAVFAC).
- Specific security requirements in the CSP intended for the construction contractor must be incorporated into the construction contract documents prior to award.
- CM should receive copy of CSP at contract award (may be CUI).
- Any changes to an approved CSP must be submitted to the AO for approval.
  - The CM must communicate to the SSM when changes to the CSP may result in a changed condition to the contract (additional time and/or money). Would be considered a Customer Requested Change.

Construction Security Plan (CSP)

- For DBB projects:
  - Do not award a construction contract without AO approved CSP.
- For DB projects:
  - Do not start onsite construction activities (excluding mobilization, demolition, clearing and grubbing) without AO approved CSP.

Site Security Manager

- **Primary Point of Contact for security requirments:**
  - **Validates construction personnel requirements for work including:**
    - General secure area Construction
    - Finish work- Outfitting (such as Furniture, Fixtures and Equipment (FF&E) and ESS)
  - **Validates material purchasing, inspection, shipping, and secure storage area (SSA) requirements including FF&E and ESS.**
  - **Validates area site access controls for personnel, materials, and vehicles**
  - **Coordinates all changes to CSP with Construction Manager for cost and schedule implications.**
  - **Submits changes to CSP to AO for approval.**
    - Changes to CSP are not valid until approved by AO.

Construction Personnel

- **Within the U.S. and its territories.**
  - **SCIF/SAPF construction and design shall be performed by U.S. companies using U.S. citizens or U.S. persons with AO approval.**
  - **Intrusion Detection System (IDS) installation and testing shall be performed by U.S. companies using U.S. citizens with a trustworthiness determination.**
- **Outside U.S. and its territories**
  - **General SCIF/SAPF construction shall be performed by U.S. companies using U.S. citizens.**
  - **SCIF/SAPF finish work shall be performed U.S. Top Secret-cleared or Secret-cleared personnel**
- **These are documented in the CSP.**

Construction Security

- **Refer to contract and project CSP for workers vetting, Access Control, Material Procurement, Material Control access control and inspection procedures.**
- **SSMs have 24-hour unrestricted access to on-site construction offices and areas to conduct security inspections.**
- **Contractor must provide a list of personnel working on or within the SCIF/SAPF.**
  - **SSM will verify information provided on construction personnel.**
  - **Denied workers will not be allowed to enter SCIF/SAPF.**
- **Construction site security and access control must include effective entry and exit screening and search procedures. A single entry point should be established to aid in this process.**
  - **Physical security barriers shall be erected to deny unauthorized access to the controlled areas.**
  - **Cell phones may be prohibited.**

Secure Storage of Construction Materials

- Materials specifically destined for SCIF/SAPF construction may have to be delivered and stored in a Secure Storage Area (SSA).
- Some materials specifically destined for SCIF/SAPF construction may have to be delivered prior to use to allow time for the SSM to inspect materials.
- Only personnel vetted by the SSM will have access to the stored materials.

Construction: Site Security

- Construction Surveillance Technicians (CSTs) report to the SSM, their responsibilities include:
  - Supplement site access controls, implement screening and inspection procedures, as well as monitor construction and personnel, when required by the AO.
  - Observe and report suspicious incidents or materials:
    - In low and medium technical threat countries, begin surveillance of non-cleared workers at the start of SCIF/SAPF construction or the installation of major utilities, whichever comes first.
    - In high and critical technical threat countries, begin surveillance of non-cleared workers at the start of: construction of public access or administrative areas adjacent to the SCIF/SAPF; SCIF/SAPF construction; or the installation of major utilities, whichever comes first.

Construction: Site Security

- Cleared American Guards (CAGs) report to SSM or CST. Their responsibilities include:
  - Performs access-control functions at vehicle and pedestrian entrances to the site except as otherwise noted in the CSP.
  - Screens all non-cleared workers, vehicles, and equipment entering or exiting the site.
  - Denies introduction of prohibited materials, such as explosives, weapons, electronic devices, or other items as specified by the AO or designee.
  - Conducts random inspections of site areas to ensure no prohibited materials have been brought on to the site.

Construction: Site Security

- Intelligence Community and the Tech Spec for ICD/ICS 705 do not require Cleared American Guards (CAGs) or Construction Security Technicians (CSTs) for projects within the United States, its territories, or possessions.
- Construction security surveillance such as CSTs and CAGs, may be client funded using appropriations available for operations or with resource sponsor's approval, funded by MILCON. Refer to NAVFACINST 4700.1, 7045.1 and CRB Guidelines.
- NAVFAC does not contract for CAGs and CSTS.
  - NAVFAC does not have contracting authority to contract for non-NAVFAC contractor support positions.

Construction Manager

- If any updates are made to the CSP, inform supported command and SSM of the scope or budget implications.
- Conduct Design-Build (DB) Post Award Kickoff (PAK) or Design-Bid-Build (DBB) Pre-Construction Conference (PreCon). SSM must attend.
- Forward approved construction submittals to SSM for inclusion in FFC.
- Conduct the initial NAVFAC Red Zone (NRZ) meeting. Include inspections and acceptance testing in the critical activities.
  - Coordinate preliminary walkthrough with the SSM prior to substantial completion of space.
  - Conduct periodic inspections of area to document and validate construction requirements.
  - Conduct final inspections and acceptance testing with the SSM in accordance with the NRZ critical activities.

Construction: Quality Management

Required SCIF/SAPF Inspections (Per UFGS 01 45 00.00 20)

- Periodic Inspections
- Preliminary Inspection
- Acceptance Testing and Sound Attenuation
- Acceptance Testing and for Electronic Security Systems
- Final Inspection

Accreditation Cycle

- **ISC 705-2 provides accreditation policy requirements.**
  - **inspections and evaluations are performed by the AO, or designee (SSM), prior to initial accreditation.**
  - **The accreditation includes a review of documents relating to 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.**

Accreditation Cycle

- No Surprises!
- Coordinate Periodic Inspections, Preliminary Inspection
- Acceptance Testing, and Final Inspection with SSM.
  - Conduct inspections to validate and document:
  - Perimeter wall
  - Acoustical construction (batting and seals)
  - R-foil or aluminum foil backed gypsum installation (TEMPEST requirement)
  - Gypsum wallboard installation
  - True Floor to True Ceiling
  - Top and bottom sealed (both sides) with acoustical foam or sealant finished to match wall

Accreditation Cycle

- Inspections (continued:
  - Walls finished and painted from true floor to true ceiling
  - Perimeter Door Installation
  - 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

Accreditation Cycle

- **Assemble required documents for accreditation process. (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

Accreditation Cycle

- **Drawings (continued):**
  - **Fire Protection**
    - Sprinkler piping including penetration details
    - Fire Alarm system
    - Mass Notification System
  - **Mechanical**
    - HVAC plans, sections and details of SCIF penetrations, ductwork details sheets
    - Plumbing floor plans, detail for perimeter 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 perimeter penetrations

Accreditation Cycle

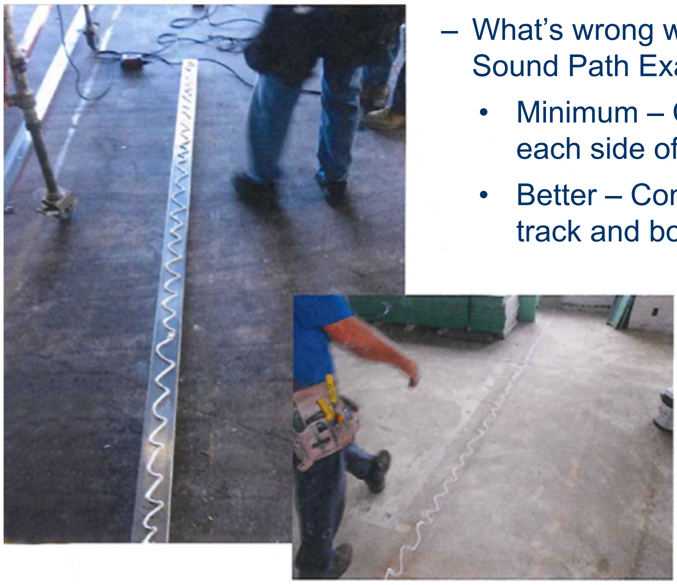
– **Submittals**
  - Doors
  - Door Hardware (locks, closers, and hinges)
  - Acoustical assemblies
  - Electronic Security Systems
  - Sound masking equipment
  - As-Built drawings (May be Controlled Unclassified Information (CUI))

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 should focus on the perimeter and capture:**
  - **Wall construction**
    - Top and bottom sealed (both sides) with acoustical foam or sealant finished to match wall
    - Acoustic installation (batting and seals)
    - R-foil or aluminum foil backed gypsum installation (TEMPEST)
  - **Wall finishes**
    - Finished and painted from true floor to true ceiling
  - **Perimeter penetrations**
  - **Duct construction including inspection ports and acoustic baffle**
  - **Man-bar construction**

Construction: Lessons Learned

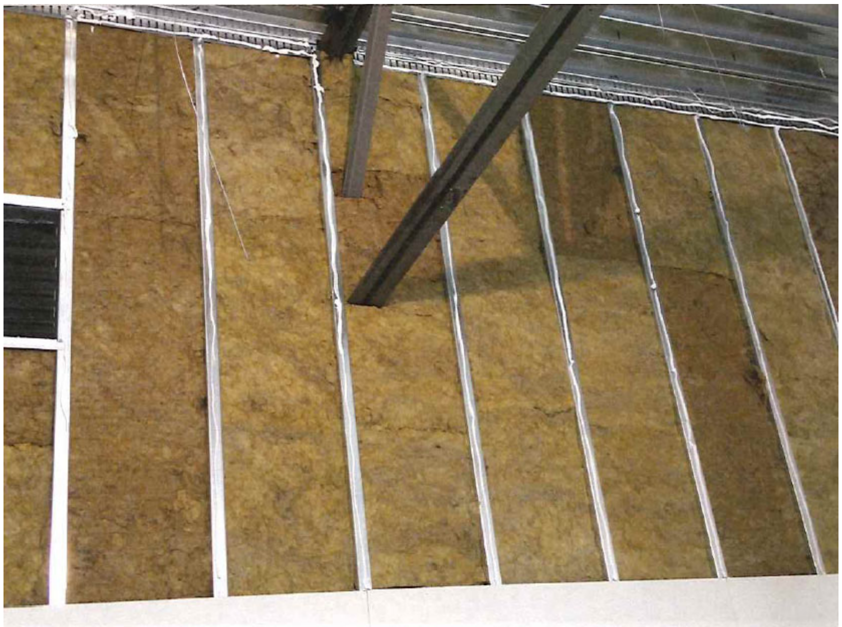
- **Top and bottom of walls are sealed (both sides) with acoustical sealant**



- What’s wrong with this Picture? Remember the Sound Path Example.
  - Minimum – Continuous bead of sealant on each side of track
  - Better – Continuous sealant each side of track and bottom of track

Construction: Lessons Learned

- **Acoustic insulation is securely fastened**

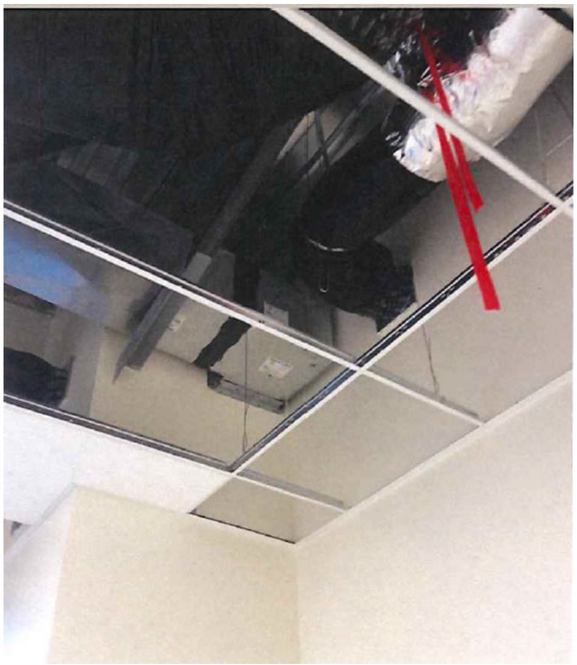


Construction: Lessons Learned

- Joints are tight with no gaps.
- Joints staggered on the opposite sides of a partition so they are not on the same stud.
- Joints of the face layer are offset from the joints of the base layer.
- Joints in the face layer that are parallel to the framing members must fall over the framing members and offset from the base layer.

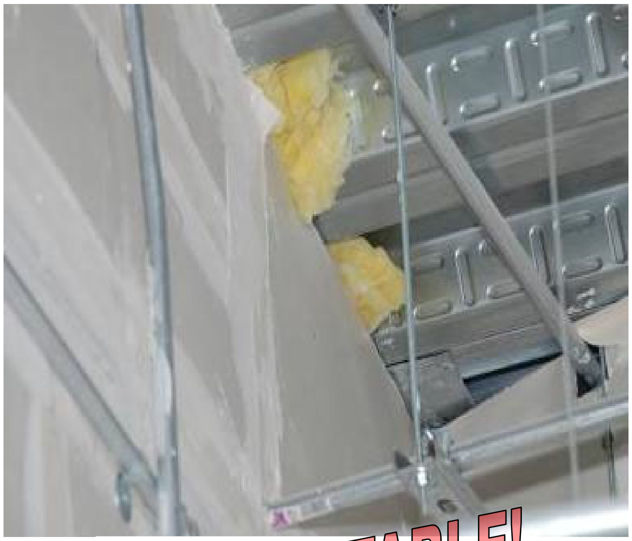
Construction: Lessons Learned

- Wall goes from floor slab (true floor) to underside of floor or roof deck (true ceiling)
- Wall uniformly finished and painted from true floor to true ceiling



Construction: Lessons Learned

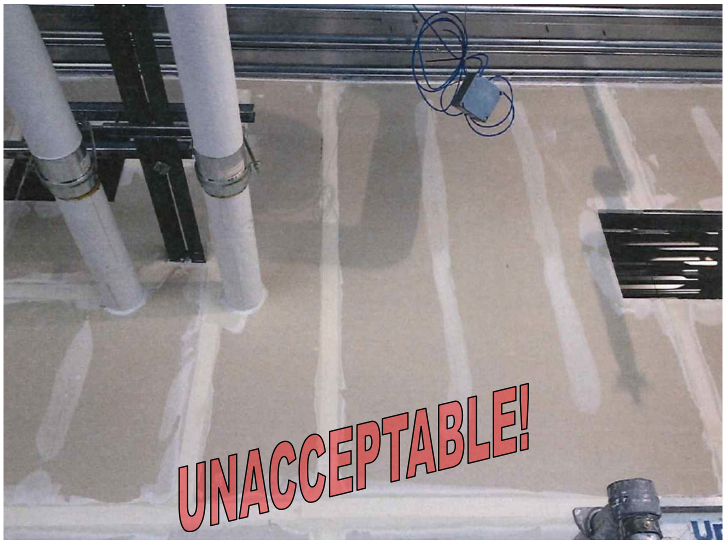
- **True floor to true ceiling?**
- **Uniformly painted and finished from true floor to true ceiling?**
- **Acoustically rated?**
  - 3 layers GWB?
  - Acoustically sealed on both sides?



UNACCEPTABLE!

Construction: Lessons Learned

- **Penetrations acoustically sealed on both sides?**
- **Wall uniformly finished and painted from true floor to true ceiling?**

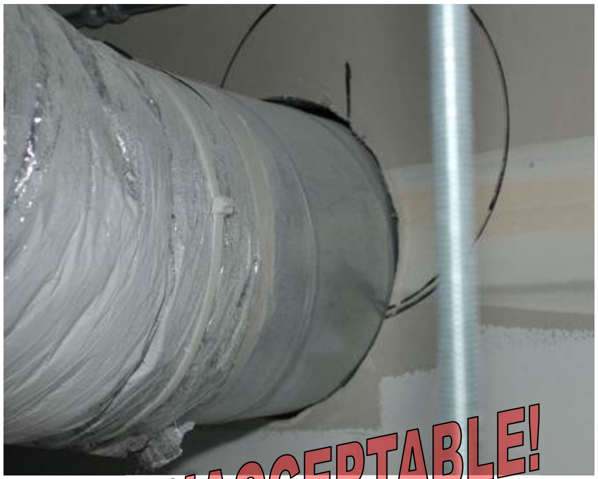


UNACCEPTABLE!

- **Still needs to be uniformly finished and painted from true floor to true ceiling.**

Construction: Lessons Learned

- Wall uniformly painted and finished from true floor to true ceiling?
- Penetration acoustically sealed on both sides?

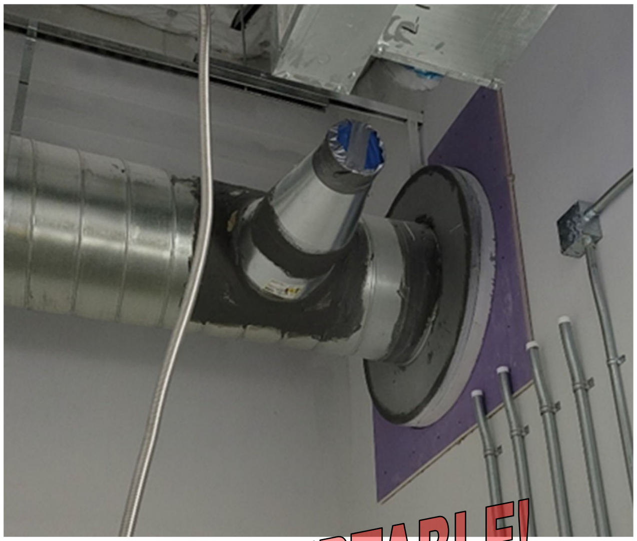


UNACCEPTABLE!

Construction: Lessons Learned

- Wall uniformly painted and finished from true floor to true ceiling?
- Gap between finished and unfinished GWB?
- Penetration acoustically sealed on both sides?

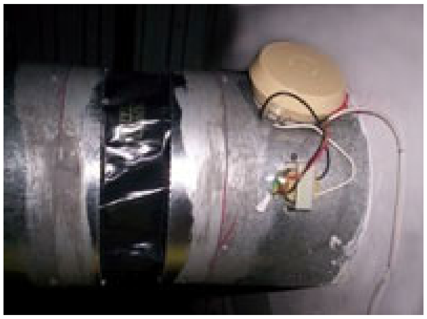
- Must be finished and painted and the penetrations must be sealed and finished.



UNACCEPTABLE!

Construction: Lessons Learned

- **Acoustic Protection**
  - **When normal construction and baffling measures have been determined to be inadequate for meeting Sound Group 3 or 4, sound masking may be provided.**
  - **Not Good: classified as personal property.**
    - A sound masking system may utilize a noise generator as a noise source, an amplifier, and speakers or transducers located on the perimeter.
    - When required, provide sound masking devices at penetrations to the perimeter such as doors and duct penetrations.



TRANSDUCER

Take Away

- **As a construction agent for the Department of Defense, NAVFAC must understand the requirements and ensure that the SCIFs and SAPFs we plan, design, and construct meet the policy based facility requirements for accreditation.**
  - **If a space cannot be accredited, it cannot be operational… and the supported command is "not mission capable!"**
- **Be Proactive: Find out who is the designated Site Security Manager (SSM)**
  - **Get them involved early in the project planning**
  - **Keep them involved through construction.**
- **Communication is the keystone to a successful project and accreditation.**

Take Away

- Get the preliminary CSP during the planning phase.
  - Know the construction security, material purchase/storage and personnel requirements
- Get the final “approved” CSP during design phase
- Focus on perimeter and its penetrations when designing
- Focus on the perimeter and its penetrations when reviewing the design
- Focus on the perimeter and the penetrations to the perimeter when constructing
- TEMPEST, TEMPEST, TEMPEST

Acronyms

AO – Accrediting Official

BOD – Beneficial Occupancy Date

CM – Construction Manager

CSP – Construction Security Plan

CST – Construction Surveillance Technician

CTTA – Certified TEMPEST Technical Authority

DB – Design Build

DBB – Design Bid Build

DM – Design Manager

ET – Engineering Technician

FFC – Fixed Facility Checklist

ICD – Intelligence Community Directive

ICS – Intelligence Community Standard

PM – Project Manager

QC – Quality Control

RFP – Request for Proposal

SAPF – Special Access Program Facility

SCI – Sensitive Compartmented Information

SCIF – Sensitive Compartmented Information Facility

SSA – Secured Storage Area

SSM – Site Security Manager

UFC – Unified Facilities Criteria

UFGS – Unified Facilities Guide Specification

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.

Definitions

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.

Secure Working Area:

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

Security Environment Threat List (SETL): Classified List managed by the Office of Intelligence and Threat Analysis (ITA). The SETL reflects four categories of security threat, including political violence and crime for U.S. missions overseas.

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.

Definitions

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

Special Access Program Facility (SAPF).

- An accredited area, room, group of rooms, building, or installation where SAP materials may be stored, used, discussed, manufactured, or electronically processed. When required, SAPF provide an operational capability that is critical to the supported command’s mission

TEMPEST:

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

Vault:

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