Secure Facilities and Spaces

Presented by: Richard Cofer, P.E.

Naval Facilities Engineering Command Atlantic
Capital Improvements Business Line
Engineering Criteria and Programs

November 2016

Intent

- **The intent of this presentation is to make designers aware of:**
  - **Types of secure spaces**
  - **Terminology associated with secure spaces**
  - **Understand some basic physical security concepts**
  - **Understand baseline requirements**
  - **How layout can enhance the security of the secure spaces.**

Secure Facilities and Spaces

- **Secure Facilities and Spaces are designed and operated to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.**

Secure Facilities and Spaces

Secure Facilities and Spaces are typically found in:

- Command Headquarters
- Operation Centers
- Admin Facilities
- Communication Centers
- Training Facilities
- Hangars

Project Development

- **The requirements for a secure facility or space must be established during project planning.**
  - **Establish an interdisciplinary planning team with local considerations to include the following:**
    - Planning
    - Supported Command
    - Supported Command's Security Manager
    - Communications
    - Security: Installation/Region N3
    - Engineering

- **PM/DM needs to proactively engage Security Manager to coordinate project requirements and design**

Project Development

- **The planning team must:**
  - **Determine what assets require protection**
  - **Understand related DoD/Service policy/regulations**
  - **Understand the objectives of the system**
  - **Understand the user's operational requirements**
  - **Understand the operational and sustainment cost**
  - **Determine the protective measures and related costs and incorporate them into the project's scope and budget.**
  - **Determine funding source(s) for electronic security systems**

So What Generates the Requirement?

- **The asset being protected:**
  - **Classified Information**
    - Sensitive Compartmented Information (SCI)
    - Special Access Program (SAP) Information
    - Top Secret
    - Secret
    - Confidential
  - **Classified Communication Systems**
  - **Arms, Ammunitions, and Explosives (AA&E)**
- **This presentation will focus on the Classified Information and Communications Systems**

Levels of Classification

- **Top Secret Information:**
  - **Top Secret is be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.**
- **Top Secret information must be stored:**
  - **In a GSA-approved security container with one of the following supplemental controls:**
    - An employee cleared to at least the Secret level shall inspect the security container once every 2 hours.
    - The location that houses the security container is protected by an intrusion detection system (IDS) with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

Levels of Classification

- **Top Secret information must be stored (continued):**
  - **In an open storage area (also called a secure room) equipped with an IDS with the personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth, or within 5 minutes of alarm annunciation if it has not**
  - **In a vault, or GSA-approved modular vault, meeting the requirements of Federal Standard (FED-STD) 832**

Levels of Classification

- **Secret Information.**
  - **Secret is applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.**
- **Secret information must be stored:**
  - **In the same manner Top Secret information**
  - **In a GSA-approved security container or vault built to FED-STD 832 specifications, without supplementary controls**
  - **In an open storage, provided the senior agency official determines in writing that security-in-depth exists, and one of the following supplemental controls is utilized:**
    - An employee cleared to the Secret level shall inspect every 4 hours.
    - An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

Levels of Classification

- **Confidential Information.**
  - **Confidential. Confidential is applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.**
- **Confidential information must be stored**
  - **In the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.**

Levels of Classification

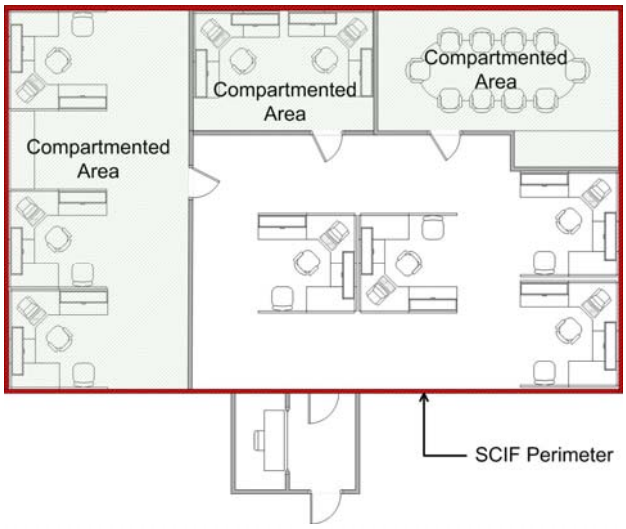
- **Sensitive Compartmented Information (SCI).**
  - **A SCI is classified Secret or Top Secret information that is derived from intelligence sources, methods or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.**
- **SCI can only be stored, used, processed, or discussed in a Sensitive Compartmented Information Facility (SCIF)**

Levels of Classification

- **Special Access Program (SAP):**
  - **A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.**
- **SAP Information can only be stored, used, processed, or discussed in a Special Access Program Facility (SAPF)**

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.



Unclassified Information

- **Controlled Unclassified Information (CUI).**
  - **Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.**
- **For Official Use Only (FOUO).**
  - **A protective marking to be applied to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the Freedom of Information Act (FOIA).**

Protection of FOUO Information

- **During working hours:**
  - **Reasonable steps must be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO information unattended where unauthorized personnel are present).**
- **After working hours:**
  - **FOUO information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided or is deemed inadequate, the information must be stored in locked desks, file cabinets, bookcases, locked rooms, etc.**

Terms to Know

- **Classified Information Systems:**
  - **CENTRIXS: Combined Enterprise Intelligence Exchange System (Confidential)**
  - **SIPRNET: Secret Internet Protocol Router Network**
  - **JWICS: Joint Worldwide Intelligence Communications System (Top Secret/SCI)**

Terms to Know

- **PDS: Protected Distribution System**
  - **A signal distribution system (raceway, conduit or duct) containing unencrypted National Security Information (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.**

Terms to Know

- **Secure Room (Open storage area)**
  - **Secure Room. An area constructed in accordance with the requirements of the DoDM 5200.01 Volume 3 Appendix to Enclosure 3 and authorized by the senior agency official for open storage of classified information.**
- **Controlled Access Area (CAA)**
  - **A physical area such as a building or room under physical control and where only personnel cleared to the level of the information being processed are authorized unrestricted access.**
- **Restricted Access Area (RAA)**
  - **A physical area such as a building or room where only personnel cleared to the level of the information being processed are authorized unrestricted access, but does not meet all of the physical security requirements of a CAA.**

Terms to Know

- **TEMPEST**
  - **TEMPEST refers to the investigation, study, and control of Compromising Emanations of National Security Information (NSI) from telecommunications and information processing systems.**
  - **TEMPEST countermeasures are required when the facility contains equipment that will be processing National Security Information (NSI). Example: CENTRIXS, SIPRNET or JWICS**
- **Certified TEMPEST Technical Authority (CTTA)**
  - **The CTTA has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures**

Terms to Know

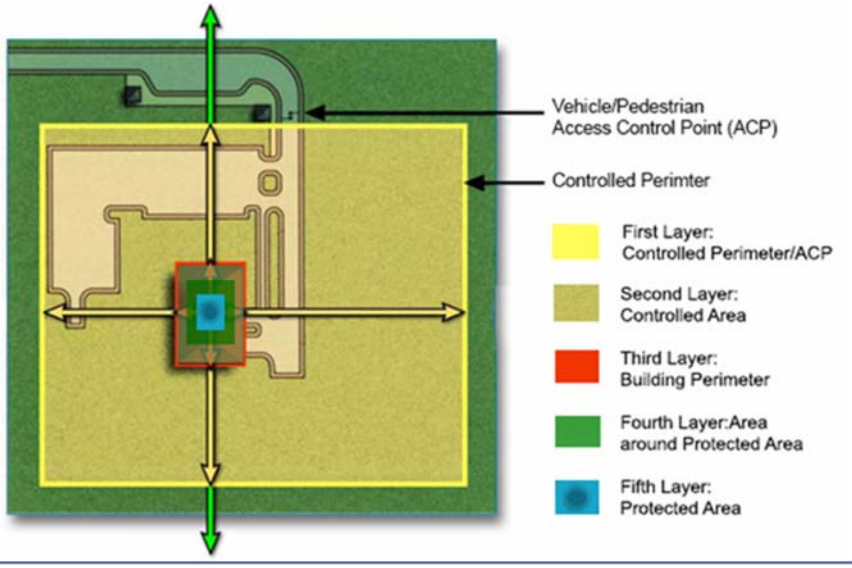
- **Inspectable space:**
  - **Inspectable Space is the three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.**
- **If required TEMPEST countermeasures are omitted, the facility will not be accredited and the Supported Command will not be mission capable.**

Protection System Concepts

- **SECURITY IN DEPTH (SID)**
  - **A combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force.**
    - The layers in SID are designed to screen personnel and materials to allow access to authorized personnel.
    - The complementary security controls are made up of different types of procedures, boundaries, Electronic Security System (ESS), and response forces so that the aggressor's tools and techniques required to bypass one layer of the system are not the same for successive layers.

Protection System Concepts

- **SID Layers**
  - **The first layer of defense is typically an Installation's perimeter including the Access Control Points (ACPs).**



Protection System Concepts

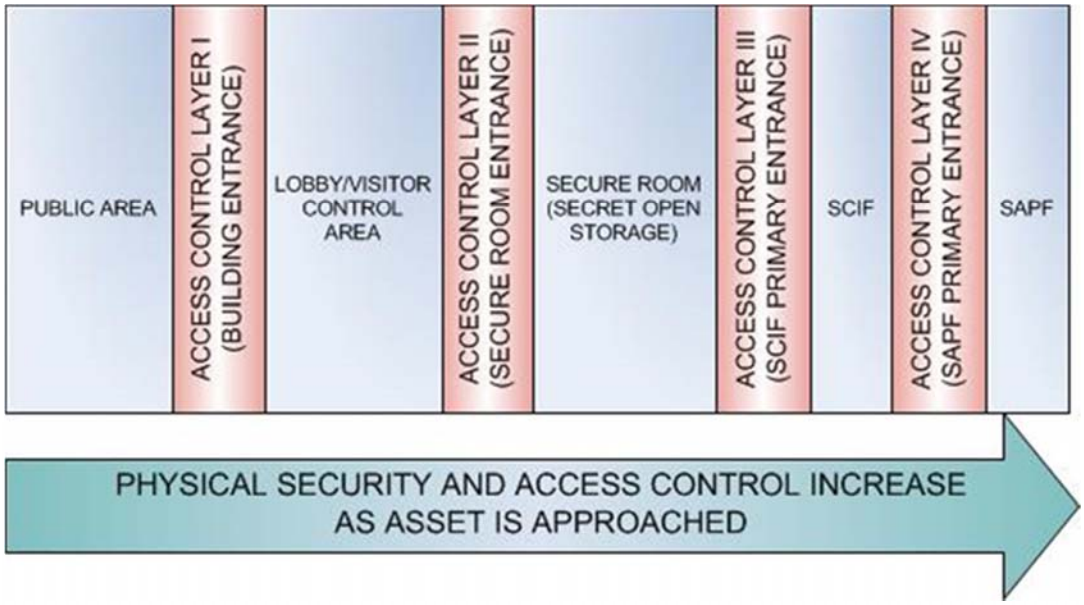
- **SID Layers**
  - **To determine protection measures for a specific project, security professionals must assess the SID in place and determine if additional layers are required. Here are some examples of how or where SID can be implemented:**
    - On a Military installation or compound with a dedicated response force of U.S. citizens or U.S. persons.
    - Within a controlled or restricted area.
    - Within a building or fenced compound that employs access control.
    - Within the building away from exterior walls, on an upper floor or in the basement.
    - In a protected area where the space adjacent to or surrounding the protected area is controlled and protected by alarm.

Protection System Concepts

- **Zoning**
  - **Zoning is the concept of grouping functional areas by security or access levels to enhance security.**
  - **Having multiple zones within a facility that require personnel to transition through increasingly secure access control layers (zones) can enhance the security of the higher security zones/areas**
  - **Zones may include**
    - Public access (public/visitor areas, service areas)
    - Controlled access area, Restricted access area, secret open storage, top secret open storage, SCIF, SAPF and the compartmented areas within.

Protection System Concepts

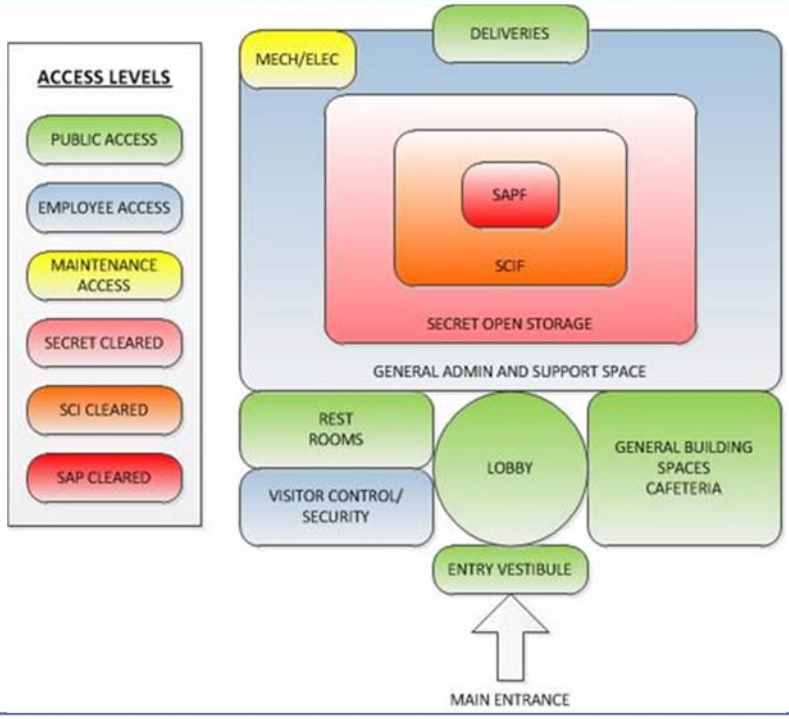
Zoning/SID Layers



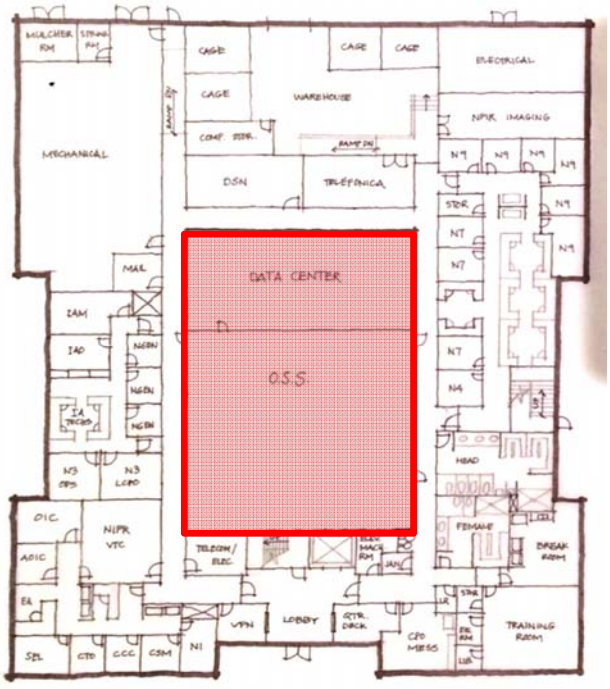
Design Considerations

- **Utilize the building layout to enhance security**
  - **Understand the various secure spaces within the facility**
    - Understand the security levels and associated construction requirements (Secret, Top Secret, SAP, or SCI)
    - Understand the required separations, adjacencies and compartmented areas
    - Access control procedures and personal storage requirements
  - **Understand visitor access and escort requirements**
    - Visitors
    - Foreign Nationals
    - Maintenance personnel
    - Custodial Staff
  - **Know who else is in the building**
    - Foreign Nationals

Design Considerations

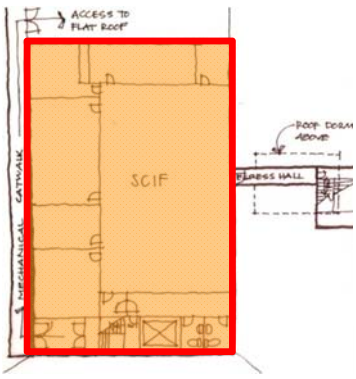


Design Considerations



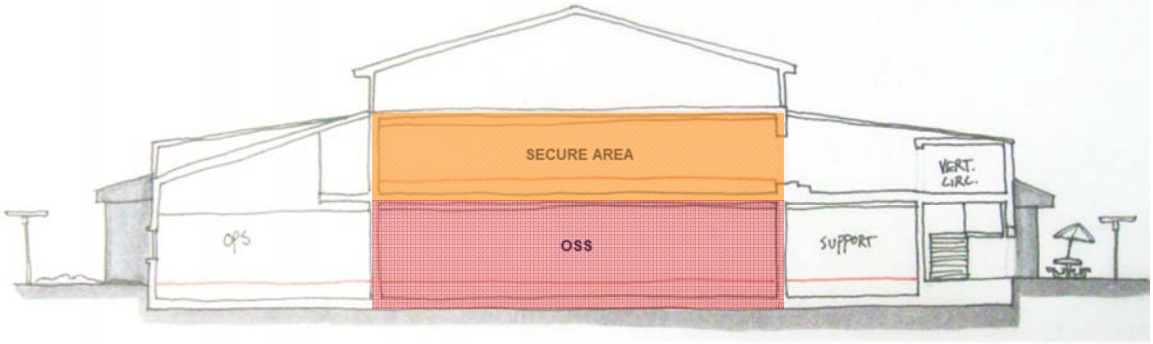
OPEN SECRET STORAGE

SCIF



SECOND FLOOR SECURE AREA LOCATED DIRECTLY OVER THE OSS SPACE/DATA CENTER.

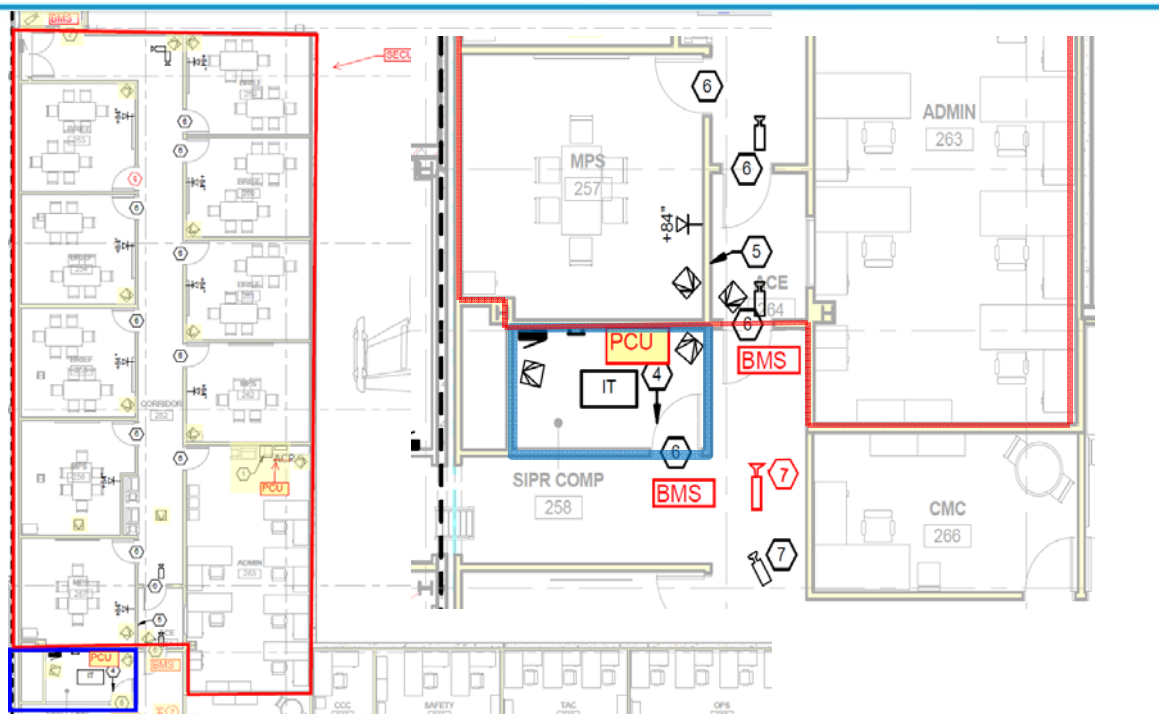
Design Considerations



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

BUILDING SECTION

Design Considerations



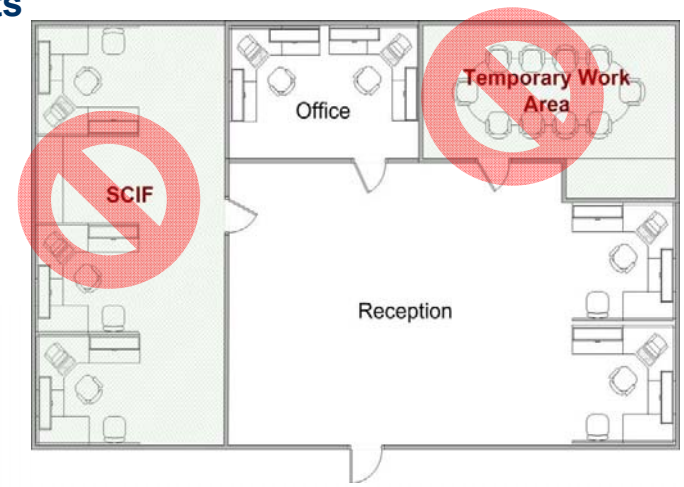
When is a SCIF or SAPF needed?

- **A SCIF or SAPF is established when there is a clear operational requirement that is crucial to the command's mission.**
- **To be operational, a SCIF or SAPF must be Accredited.**
  - **Accreditation is the formal approval that a space meets the prescribed physical, technical, and operational standards.**

If a SCIF or SAPF cannot be accredited, it cannot be operational… and the command is not mission capable!

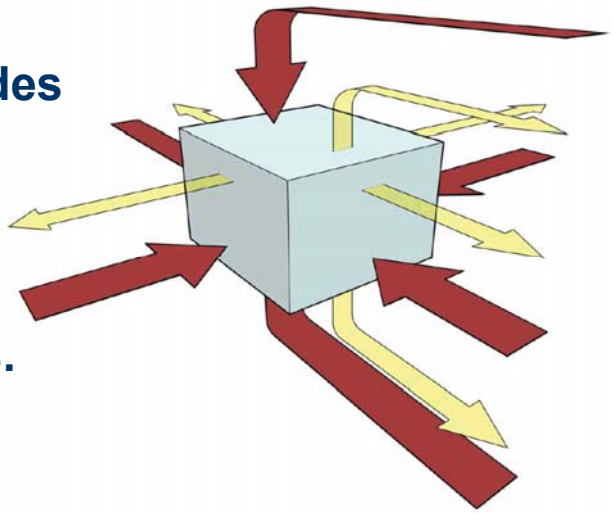
Information Security for SCIF and SAPF

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



Specific Design Strategy

- **DESIGNERS MUST TAKE A SIX-SIDED APPROACH WHEN DEVELOPING DESIGNS.**
  - **The perimeter includes all walls , floors, ceilings, doors, windows and penetrations in the perimeter such as ductwork and pipes.**



Specific Design Strategy

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

Specific Design Strategy

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

Specific Design Strategy

- **Walls:**
  - **Perimeter walls, floor and ceiling must be permanently and solidly constructed and attached to each other. Walls must go from true floor to true ceiling.**
  - **Seal partition continuously with acoustical foam or sealant (both sides) and finished to match wall wherever it abuts another element such as the floor, ceiling, wall, column, or mullion.**
  - **Uniformly finish wall from true floor to true ceiling.**

Specific Design Strategy

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

Specific Design Strategy

Specific Design Strategy

- **Wall A (Standard Wall) - Sound Group 3 (STC 45 or better)**
  - **3-5/8” 16 gauge metal or 2 x 4 wood studs**
  - **16 gauge continuous track (top & bottom) w/ anchors at 32” o.c. maximum) – bed in continuous bead of acoustical sealant..**
  - **Three layers ⅝ inch-thick gypsum wallboard (GWB), one layer on the uncontrolled side of the SCIF and two on the controlled side of the SCIF. The interior two layers of wallboard shall be mounted so that the seams do not align (i.e., stagger joints)..**
  - **Acoustic fill 3 ½ “ (89mm) sound attenuation material, fastened to prevent sliding down and leaving void at the top..**

Specific Design Strategy

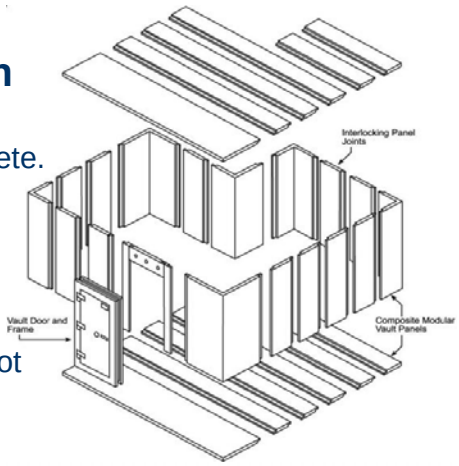
- **Wall B (Enhanced Wall) Expanded Metal Sound Group 3 (STC 45 or better):**
  - **Same as Wall A except:**
    - **¾” mesh, # 9 (10 gauge) expanded metal shall be affixed to the interior side of perimeter wall studs.**
    - **Expanded metal shall be spot-welded to the studs every six inches along the length of each vertical stud and at the ceiling and floor.**

Specific Design Strategy

- **Wall C (Enhanced Wall) Perimeter walls with Fire Rated Plywood:**
  - **Wall assembly the same as Wall B except:**
  - **1/2" Fire Retardant Plywood affixed 8' vertical by 4' horizontal to 16 gauge studs using glue and #10 steel tapping screws at 12 on center (o.c.)**
  - **GWB shall be mounted to plywood with screws avoiding contact with studs to mitigate any possible acoustic flanking path.**

Specific Design Strategy

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



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

Possible TEMPEST Countermeasures

- **RF mitigation shall be provided at the direction of the CTTA when the facility utilizes electronic processing and does not provide adequate RF attenuation at the inspectable space boundary.**
  - **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**

Possible TEMPEST Countermeasures

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

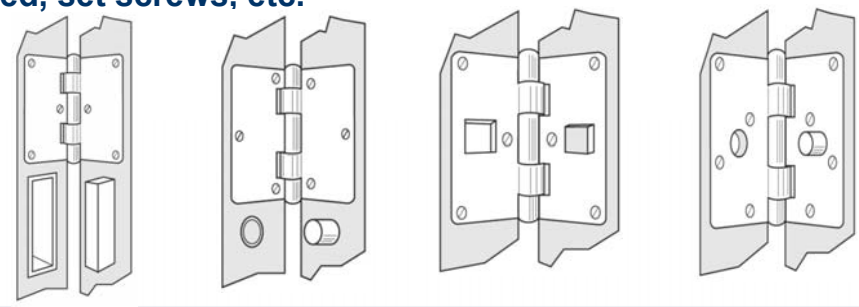
Specific Design Strategy

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

Specific Design Strategy

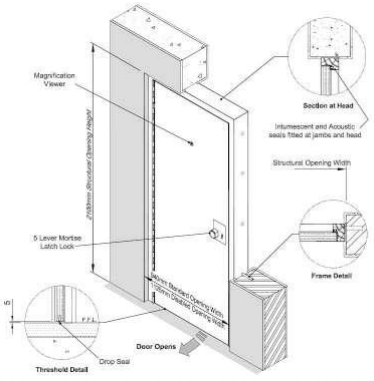
Specific Design Strategy

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



Specific Design Strategy

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



Secure Area Entrance

Is this a SCIF or SAPF?

Secure Area Entrance

Specific Design Strategy

- **WINDOWS:**
  - **No windows are preferred. Therefore, minimize or eliminate windows in the secure spaces, especially on the ground floor.**
  - **Windows must be non-opening.**
  - **Windows must provide visual and acoustic protection**
    - Windows, which might reasonably afford visual observation of classified activities within the facility with; SSM approval, must be made opaque or equipped with blinds, drapes, or other coverings.

Specific Design Strategy

- **WINDOWS Continued:**
  - **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) must:**
    - Meet the standards of the perimeter
    - Be protected against forced entry.
    - Be alarmed
  - **Provide RF protection when required.**

Specific Design Strategy

- **Example of Windows in a Historical building converted to a SCIF.**
- **Windows designed for:**
  - Historical
  - Antiterrorism Standards
  - Acoustic Eavesdropping
  - Forced Entry (Bars)
  - Visual surveillance (Blinds)

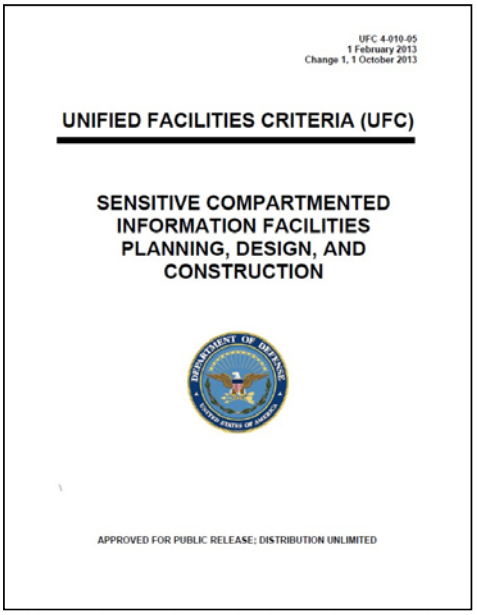
Approved by Cultural Resources and Site Security Officer!

Policy Documents

- **SCIF:**
  - **DoD Manual 5105.21, Volume 2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security**
    - Intelligence Community Standard (ICS) 705-1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities.
  - **UFC 4-010-05 Sensitive Compartmented Information Facilities Planning, Design, and Construction**
- **SAPF:**
  - **DoD Manual 5205.07, Volume 3, DoD Special Access Program (SAP) Security Manual: Physical Security**
    - Intelligence Community Standard (ICS) 705-1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities.
- **Secret/Top Secret Open Storage:**
  - **SECNAV M-5510.36 Department of the Navy Information Security Program**

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 SCIF policy requirements and ensure appropriate implementation.
- **PREPARING ACTIVITY:** NAVFAC
  - Point of contact: Richard Cofer
  - Author: 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
    - Updates due to :
      - Publication of DoDM 5105.21
      - Update of IC Tech Spec-for ICD/ICS 705
      - Lessons Learned
      - Clarification on TEMPEST mitigation.


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

Priorities??

Priorities??

Restricted Area Sign

Responsibility/Take Away

- **As a design and construction agent for the Department of Defense, it is imperative that we understand how to design and construct secure facilities and spaces for the protection of classified information.**
- **Remember, these requirements affect project:**
  - **Planning**
  - **RFP Development**
  - **Design**
  - **Construction**


QUESTIONS