Secure Facilities and Spaces

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

September 2019

Intent

- **The intent of this presentation is to make participants aware of:**
  - **Materials and Equipment that require secure spaces**
  - **Types of secure spaces**
  - **Terminology**
  - **Basic physical security concepts**
  - **What to focus on**
  - **Design Considerations.**

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/DMs need 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 & Equipment
    - Top Secret
    - Secret
    - Confidential
  - **Communications Security (COMSEC) Material**
  - **Arms, Ammunitions, and Explosives (AA&E)**

This presentation will focus on 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 a GSA-approved security container equipped with a lock meeting FF-L-2740, provided the container is located within an area that has been determined to have security-in-depth.**
  - **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

- **Communications security (COMSEC) Materials.**
  - **Communications Security (COMSEC) material is used to protect U.S. Government and partner classified or sensitive unclassified communications or information from unauthorized persons.**
    - Encryption Equipment for Classified Networks
      - SIPRNet
      - JWICS
    - Classified Communications Equipment
      - Encrypted Radio/Satellite Equipment
- **Store COMSEC material separately from other classified material**

CMS-1, Department of The Navy (DON) COMSEC Policy and Procedures Manual

Levels of Classification

- **COMSEC Materials may be stored in:**
  - **In a GSA-approved security container equipped with a lock meeting FF-L-2740**
    - Security containers storing COMSEC material should not be in commonly used passageways or other spaces where access cannot be controlled.
  - **Fixed COMSEC Facility as described in CMS-1, ANNEX J**
- **COMSEC Keying Materials may be stored in:**
  - **In a GSA-approved security container equipped with a lock meeting FF-L-2740**
  - **Storage Vaults as Described in CMS-1, ANNEX I**

COMSEC Facilities approved by an Accrediting Official in accordance with SCIF or SAPF standards are assumed to comply with the standards contained in CMS-1.

Levels of Classification

- **A COMSEC facility is not an office area where only user-level COMSEC equipment are available for individual use. Examples are:**
  - **An office, cubical or set of cubicles each with its own user level COMSEC equipment. (i.e. SIPRNet or JWICS workstation)**
  - **Area with Secure Terminal Equipment (STE)**
  - **Secure Voice Over Internet Protocol (SVOIP)**
  - **Secure Communications Interoperability Protocol (SCIP) products for individual secure voice conversations,**
  - **Residence with a SIPRNet connection,**
  - **Single TACLANE or HAIPE device,**

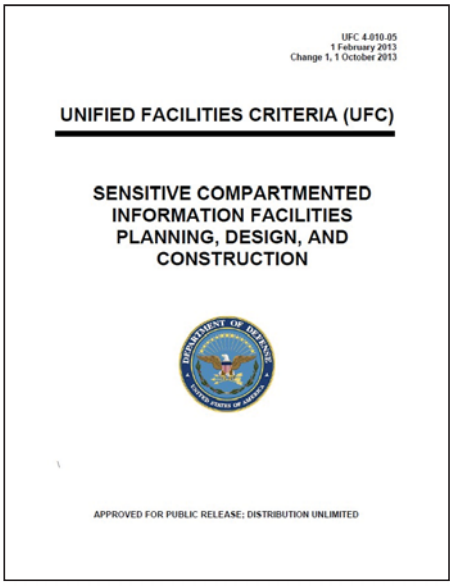
Levels of Classification

- **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)**

DoD Manual 5105.21, Sensitive Compartmented Information (SCI) Administrative Security Manuals Volume 1-3

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
  - Revision in progress



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

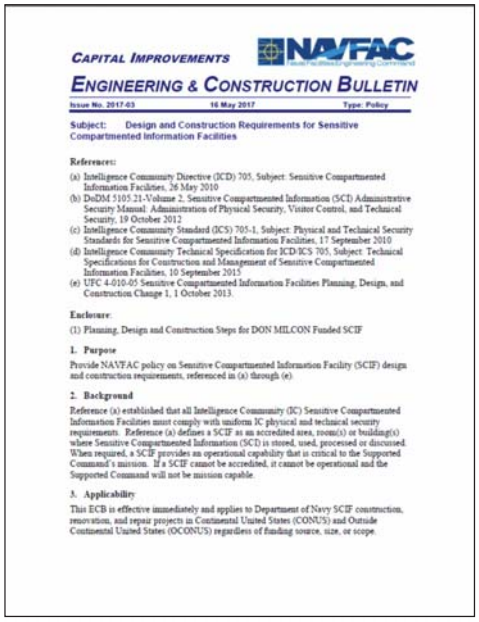
UNIFIED FACILITIES CRITERIA (UFC)

SENSITIVE COMPARTMENTED INFORMATION FACILITIES PLANNING, DESIGN, AND CONSTRUCTION

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

ECB 2017-03: Design and Construction Requirements for Sensitive Compartmented Information Facilities

- **PURPOSE:** Provide NAVFAC policy on Department of the Navy SCIF design and construction requirements, referenced in SCIF policy
- **PREPARING ACTIVITY:** NAVFAC
  - This document was coordinated with SSO Navy, NAVFAC Asset Management (AM), and U.S. Marine Corps. Points of contact:
  - NAVFAC CI: Richard Cofer
  - NAVFAC AM: Mr. Mike Bryan, NAVFAC HQ
  - USMC HQ: Mr. Brian Sanders, Headquarters Marine Corps
  - SSO Navy: Roland L. Lohr, SSO Navy, Head, Accreditation & Physical Security Division Intel Protection & Oversight
- **DOCUMENT STATUS:**
  - Published May 2017 on the NAVFAC Portal, Effective Immediately



CAPITAL IMPROVEMENTS NAVFAC

ENGINEERING & CONSTRUCTION BULLETIN

Issue No. 2017-03 16 May 2017 Type: Policy

Subject: Design and Construction Requirements for Sensitive Compartmented Information Facilities

References:
(a) Intelligence Community Directive (ICD) 705, Subject: Sensitive Compartmented Information Facilities, 26 May 2010
(b) DoDM 5105.21-Volume 2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security, 19 October 2012
(c) Intelligence Community Standard (ICS) 705-1, Subject: Physical and Technical Security Standards for Sensitive Compartmented Information Facilities, 17 September 2010
(d) Intelligence Community Technical Specification for ICD/ICS 705, Subject: Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, 10 September 2015
(e) UFC 4-010-05 Sensitive Compartmented Information Facilities Planning, Design, and Construction Change 1, 1 October 2013.

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

1. Purpose
Provide NAVFAC policy on Sensitive Compartmented Information Facility (SCIF) design and construction requirements, referenced in (a) through (e).

2. Background
Reference (a) established that all Intelligence Community (IC) Sensitive Compartmented Information Facilities 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 (SCI) 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.

3. Applicability
This ECB is effective immediately and applies to Department of Navy SCIF construction, renovation, and repair projects in Continental United States (CONUS) and Outside Continental United States (OCONUS) regardless of funding source, size, or scope.

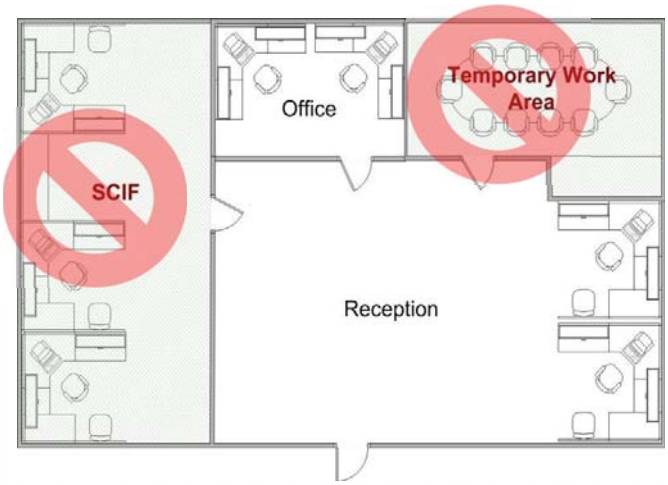
Levels of Classification

- **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)**

DoD Manual 5205.07, DoD Special Access Program (SAP) Security Manuals: Volume 1-3

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 SSM's approval, areas may be identified as "Controlled Space", "Secure Area" or "Controlled Area"**



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 FOIA. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended.**

DoDM 5200.01 Vol 4 DoD Information Security Program: Controlled Unclassified Information (CUI)

Protection of FOUO Information

- **During working hours:**
  - **During working hours, reasonable steps shall 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 shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.**

DoDM 5200.01 Vol 4 DoD Information Security Program: Controlled Unclassified Information (CUI)

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**
- **COMSEC Material**
  - **CMS-1, Department of The Navy (DON) COMSEC Policy and Procedures Manual**

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)**

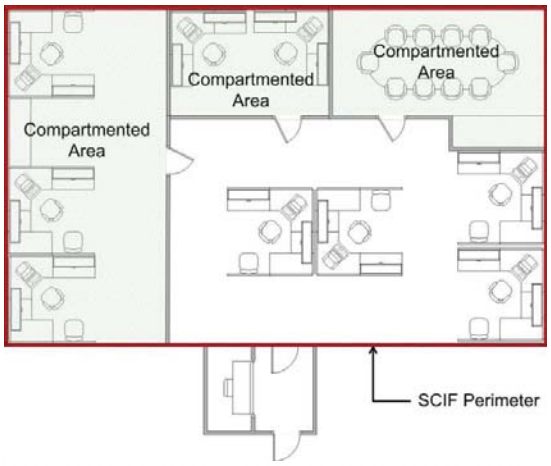
Terms to Know

- **Secure Room**
  - An open storage area constructed and authorized to allow open storage of classified information and materials.
- **Vault**
  - An area designed and constructed of reinforced concrete or steel lined construction to provide the maximum protection against forced entry and is equipped with a GSA-approved vault door and lock.
- **Modular Vault**
  - GSA-approved modular vaults meeting Federal Specification AAV-2737.
- **Specialized Security Container**
  - GSA-approved field safes and special purpose one and two-drawer light-weight security containers that are intended for storage of classified information in situations where normal storage is not feasible.

SECNAV M-5510.36 Department of the Navy Information Security Program

Terms to Know

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



IC Tech Spec-for ICD/ICS 705

Terms to Know

- **RED/BLACK LAN**
  - **Red Equipment:** A term applied to equipment that processes unencrypted NSI that requires protection during electrical/electronic processing.
  - **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.
  - **BLACK.** Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed.

CNSSAM TEMPEST 1-13 RED/BLACK Installation Guide (U/FOUO)

Terms to Know

- **Protected Distribution System (PDS)**
  - **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.**

CNSSI No.7003 PROTECTED DISTRIBUTION SYSTEMS (PDS)

Terms to Know

- **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.

CNSSI No.7003 PROTECTED DISTRIBUTION SYSTEMS (PDS)

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)**
  - An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria appointed by a U.S. Government department or agency to fulfill CTTA responsibilities.
  - The CTTA has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures

CNSSAM TEMPEST 1-13 RED/BLACK Installation Guide (U/FOUO)

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.

CNSSAM TEMPEST 1-13 RED/BLACK Installation Guide (U/FOUO)

Protection System Concepts

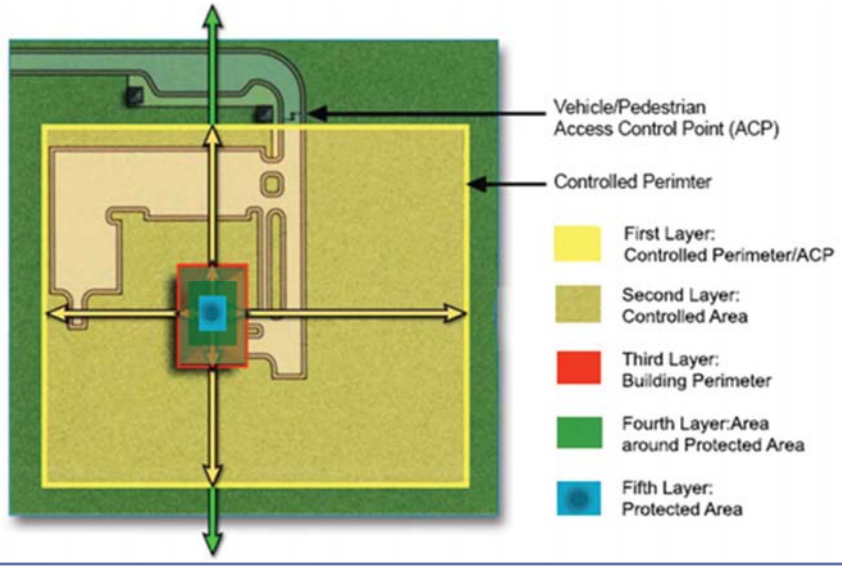
- **SECURITY IN DEPTH (SID)**
  - **A combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force.**
    - The layers in SID are designed to 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**
  - **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

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

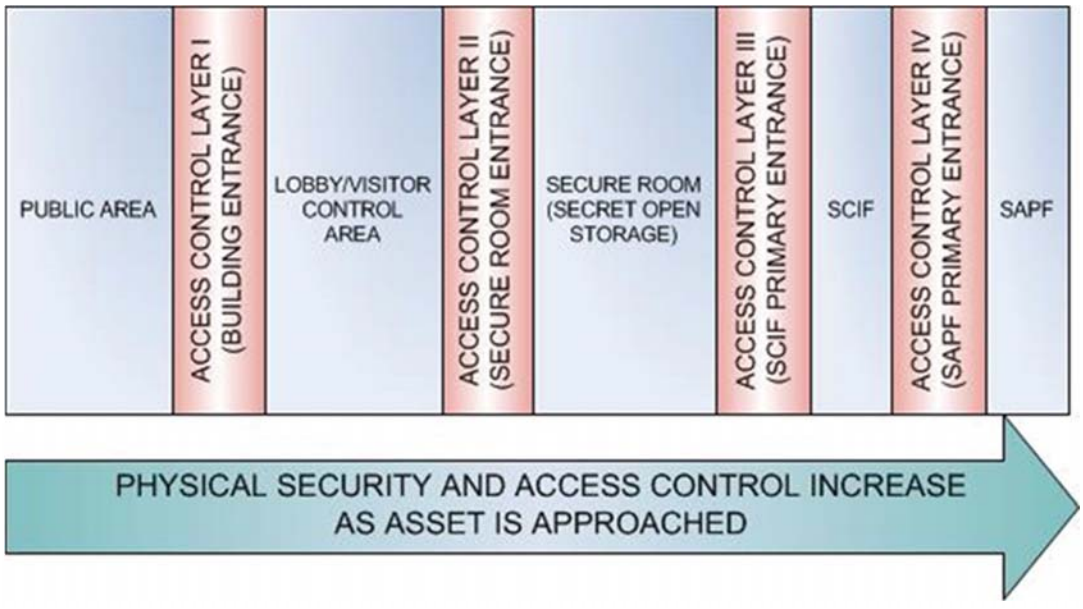


Protection System Concepts

- **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



Typical Site Protection Measures

Design Considerations

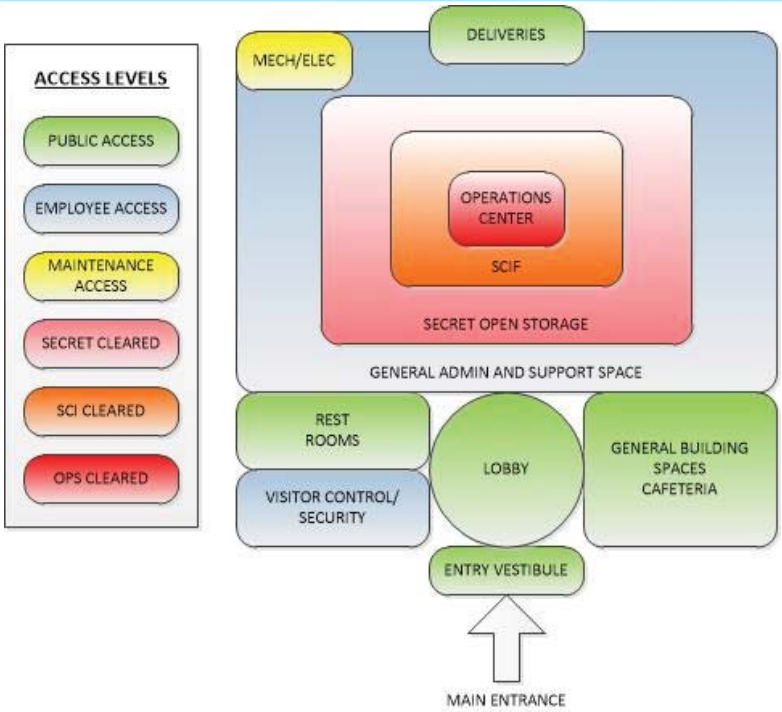
- **Utilize the building layout to enhance security**
  - **Understand the various secure spaces within the facility**
    - Understand the security levels and associated construction requirements (Secret, Top Secret, COMSEC, SAP, or SCI)
    - Understand the required separations, adjacencies and compartmented areas
    - Access control procedures and personal storage requirements

Design Considerations

- **Understand visitor access and escort requirements**
  - Visitors
  - Foreign Nationals
  - Maintenance personnel
  - Custodial Staff
- **Know who else is in the building**
  - Foreign Nationals

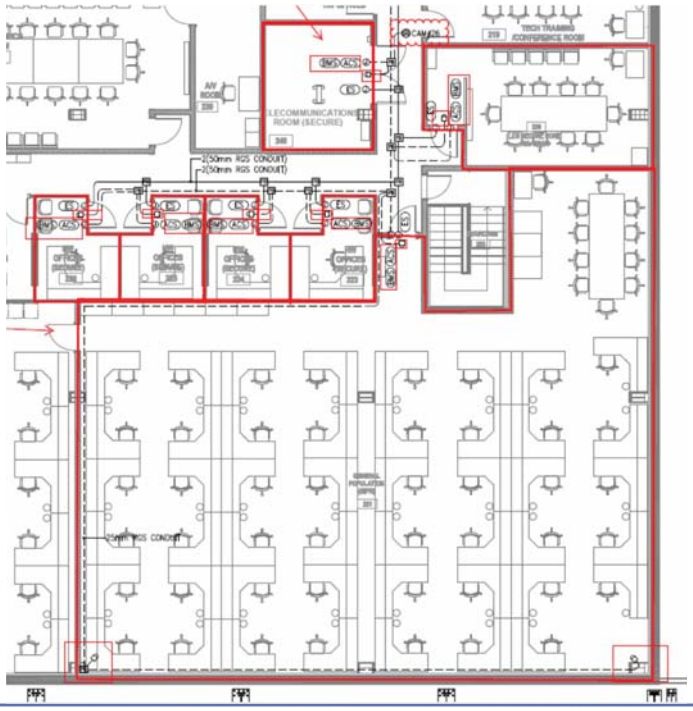
- **How does custodial staff clean restrooms or break rooms if they are within the secure perimeter?**
- **What happens down the road when HVAC repairs are required in an operational Secure Room, SCIF or SAPF?**

Design Considerations



Design Considerations

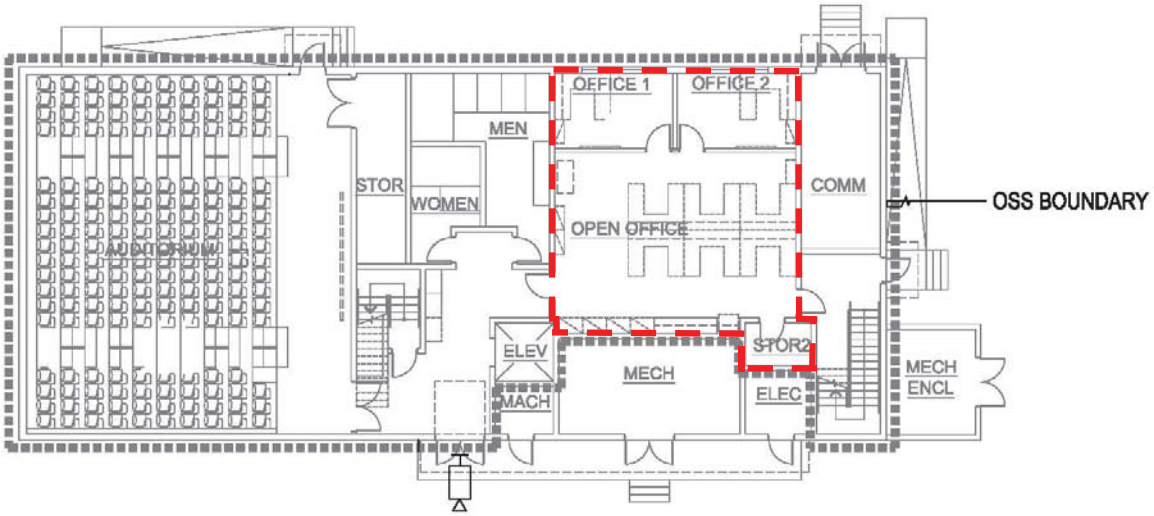
Design Considerations



Why seven (7) separate secure rooms?

Could this have been consolidated?

Design Considerations



Why is COMM RM a separate OSS Space with a separate entrance?

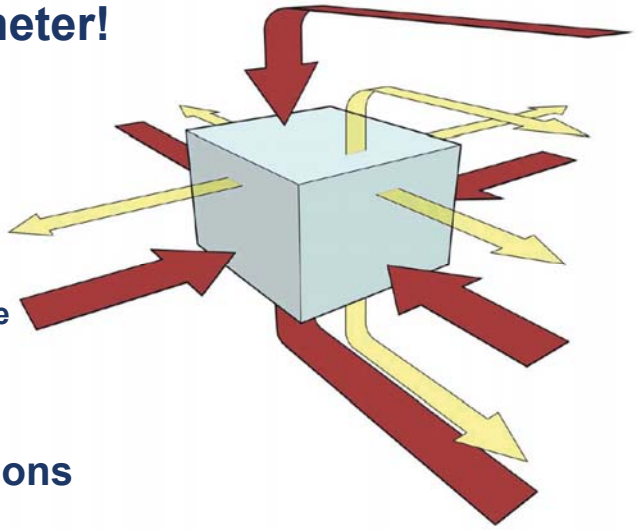
Why is the auditorium and core space include in the OSS?

Specific Design Strategy

- **PERIMETER CONSTRUCTION.**
  - **The perimeters and the penetrations to those perimeters are the primary focus of a facility design. Depending on the asset being protected, design may include mitigation for:**
    - **Forced Entry**
    - **Covert Entry**
    - **Visual Surveillance**
    - **Acoustic Eavesdropping**
    - **Electronic emanations**

Specific Design Strategy

- **Designers Must Take a Six Sided Approach When Developing Designs.**
  - **Focus on the Perimeter!**
    - **Walls**
    - **Floors**
    - **Ceilings**
    - **Doors**
      - **One Primary Entrance**
    - **Windows**
      - **None preferred**
    - **Perimeter Penetrations**



Remember

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

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?