Sensitive Compartmented Information Facilities (SCIF)
Special Access Program Facilities (SAPF)

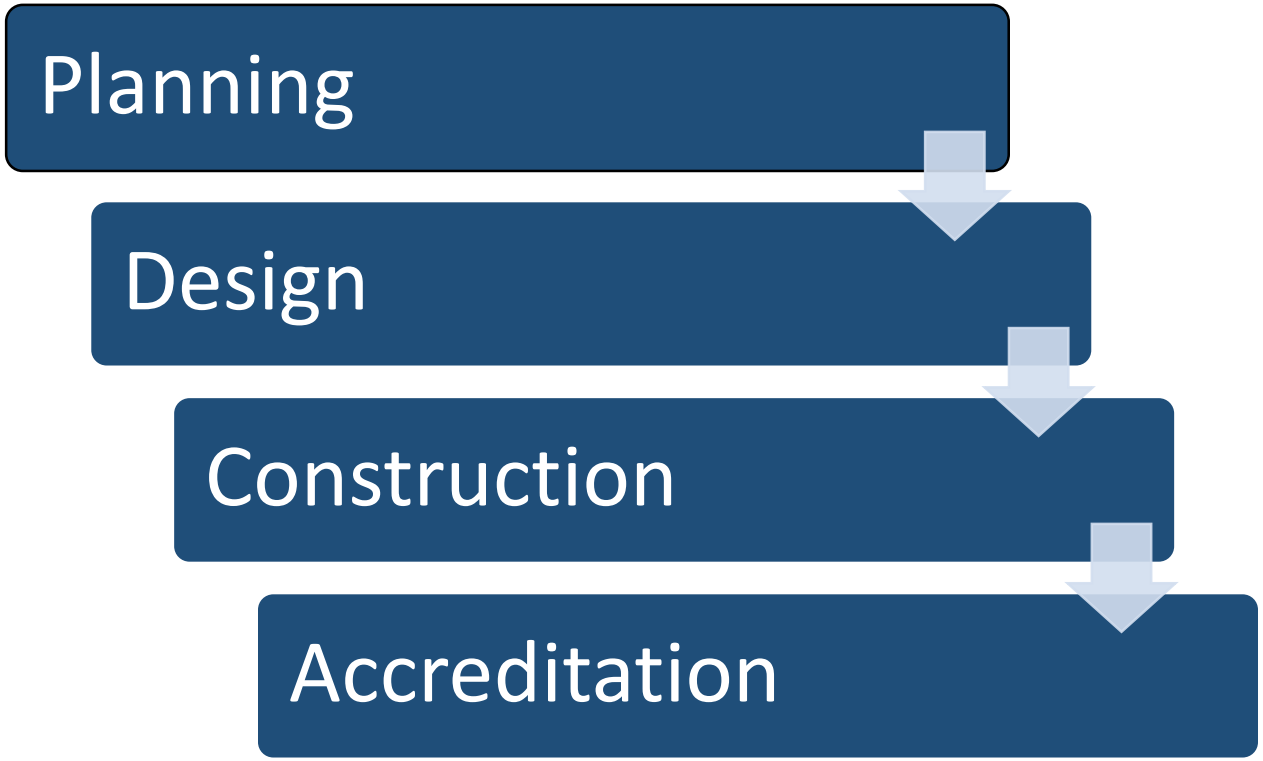
Presented to
NAVFAC FAR EAST

John Lynch, P.E. and Julie Heup, P.E.
Planning, Design and Construction Criteria (PDCC)
Engineering Criteria and Programs

October 2024

Welcome

This presentation will provide an introduction to SCIF & SAPF Policy and Criteria and discuss the four phases of a project:



NAVFAC Naval Facilities Engineering Systems Command

Sensitive Compartmented Information

Sensitive Compartmented Information (SCI) is 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 National Intelligence.

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

NAVFAC Naval Facilities Engineering Systems Command

Sensitive Compartmented Information Facility (SCIF)

SCIF is an accredited area(s), room(s) or building(s) where Sensitive Compartmented Information (SCI) is stored, used, processed or discussed. SCIF is only required for SCI and not required for Confidential, Secret or Top Secret information.

–Typically found in:

- Command Headquarters
- Operation Centers
- Communication Centers

NAVFAC Naval Facilities Engineering Systems Command

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:

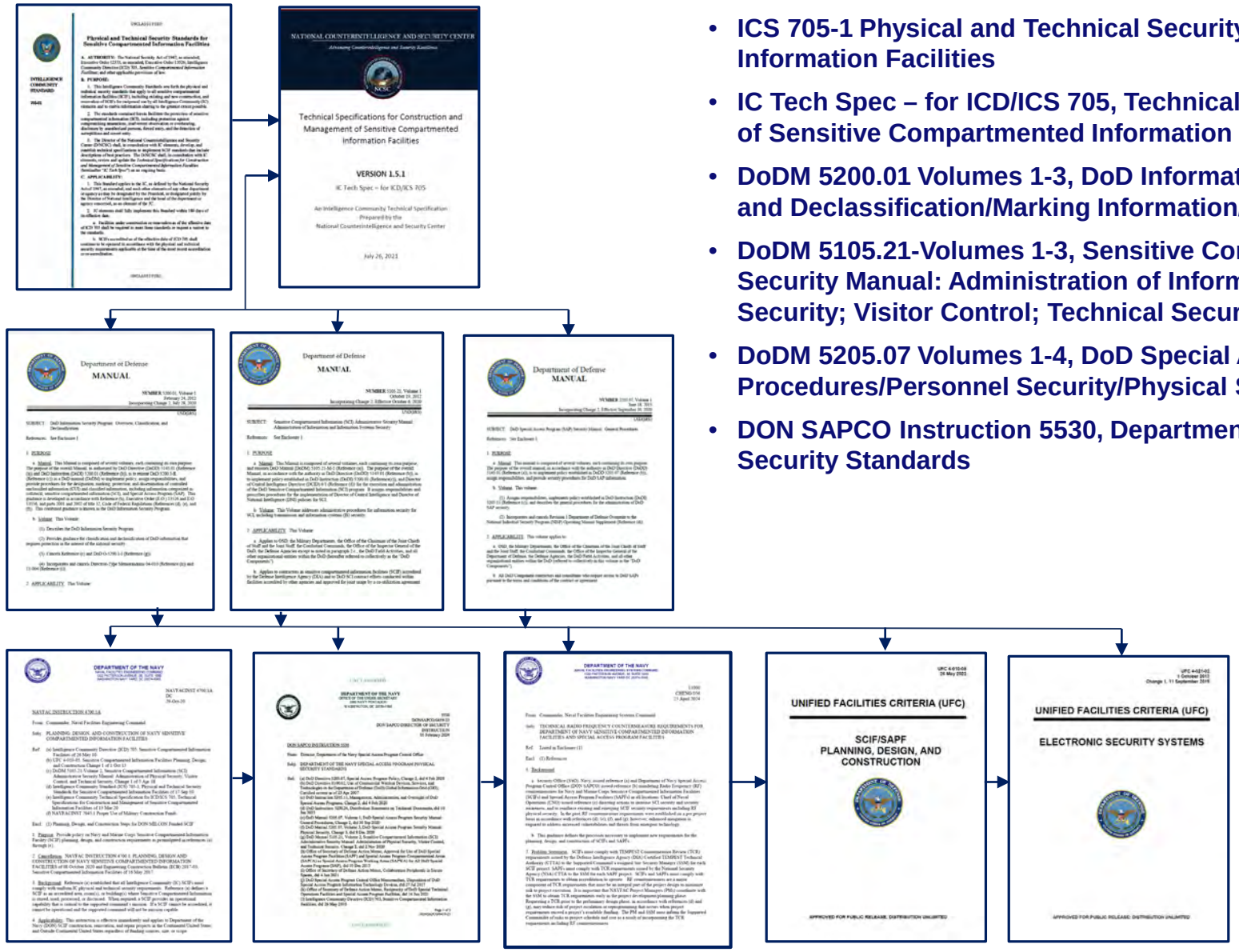
- Hangers
- Trainers

NAVFAC Naval Facilities Engineering Systems Command

SCIF/SAPF References

- **UFC 4-010-05:** *SCIF/SAPF Planning, Design and Construction, 26 May 2023*
- **NAVFACINST 4700.1A:** *Planning, Design and Construction of Navy Sensitive Compartmented Information Facilities, 15 Dec 2020*
- **NAVFAC CHENG/056 ltr**: *Technical Radio Frequency Countermeasure Requirements for DON SCIF/SAPF, 25 Apr 2024*
- **DON SAPCO Instruction 5530**: *DON Special Access Program Physical Security Standards, 5 Feb 2024*
- **SSO Navy Message, Naval Intelligence Security Policy (NISP) Directive: 001-23:** *Mandatory Radio Frequency Countermeasure Requirements for all New DON Sensitive Compartmented Information Facilities, 30 Jan 23*
- **NAVADMIN 169/23:** *U.S. Navy Special Security Officer Sensitive Compartmented Information (SCI) Policy and SCI Facility Operations, 23 Jul 23*
- **ICD/ICS 705 Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities:** *26 Jul 2021, Published by the Directory of National Intelligence (DNI)* **(There are other associated Intelligence Community Directives/Standards (ICD/ICS))**
- **DoDM 5200.01 Volume 1-3:** *DoD Information Security Protection (INFOSEC) 28 Jul 2020*
- **DoDM 5105.21 Volume 1-3:** *Sensitive Compartmented Information (SCI) Administrative Security Manuals (SCIF) 2020 - Implements DNI policies for protection of SCI and additional requirements*
- **DoDM 5205.07 Volume 1-4:** *DoD Special Access Program (SAP) Security Manuals (SAPF) 2020 - Establishes the construction of a SAPF will conform to the equivalent SCIF requirements, as defined in IC Tech Spec-for ICD/ICS 705*
- **DoDI 5200.48:** *Controlled Unclassified Information (CUI) 6 Mar 2020*
- **UFGS 13 49 20:** *Radio Frequency Shielding (Under Development)*
- **UFGS 13 49 30:** *High-Altitude Electromagnetic Pulse (HEMP) Shielding*
- **UFGS 01 14 00** *WORK RESTRICTIONS*
- **UFGS 01 45 00** *QUALITY CONTROL*

Policies for SCIF and SAPF



- ICS 705-1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
- IC Tech Spec – for ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities
- DoDM 5200.01 Volumes 1-3, DoD Information Security Program: Overview, Classification, and Declassification/Marking Information/Protection of Classified Information
- DoDM 5105.21-Volumes 1-3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security/Physical Security; Visitor Control; Technical Security/Industrial Security; Special Activities
- DoDM 5205.07 Volumes 1-4, DoD Special Access Program (SAP) Security Manual: General Procedures/Personnel Security/Physical Security/Marking
- DON SAPCO Instruction 5530, Department of the Navy Special Access Program Physical Security Standards

- UFC 4-010-05 SCIF/SAPF Planning, Design and Construction
- NAVFACINST 4700.1A Planning, Design and Construction SCIF
- NAVFACENGSYSCOM Serial Letter 11000, CHENG/056, Technical Radio Frequency Countermeasure Requirements for DON Sensitive Compartmented Information Facilities and Special Access Program Facilities (SCIF/SAPF)
- UFC 4-021-02 Electronic Security Systems

NAVFAC
Naval Facilities Engineering Systems Command

ACRONYMS

(Not all inclusive: See UFC/DONSAPCO/ICD/ICS/DODM for more complete lists)

AO – Accrediting Official

SAO – DONSAPCO Accrediting Official

BOD – Beneficial Occupancy Date

CAR – Concept Approval Request

CA – Concept Approval

CM – Construction Manager

CSA – Cognizant Security Authority

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

SIO – Senior Intelligence Officer

SSA – Secured Storage Area

SSM – Site Security Manager

SSO – Special Security Officer

TCR – TEMPEST Countermeasure Review

UFC – Unified Facilities Criteria

UFGS – Unified Facilities Guide Specification

NAVFAC Naval Facilities Engineering Systems Command

Definitions

(Not all inclusive: See UFC/DONSAPCO/ICD/ICS/DODM for more complete lists)

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

(Not all inclusive: See UFC/DONSAPCO/ICD/ICS/DODM for more complete lists)

Construction Security Technician (CST):

- A U.S. Top Secret cleared person specially trained in surveillance and the construction trade to deter technical penetrations and thwart implanted technical collection devices.

Fixed Facility Checklist (FFC):

- Checklist used by CSAs to determine whether construction requirements have been met.

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.

Special 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

(Not all inclusive: See UFC/DONSAPCO/ICD/ICS/DODM for more complete lists)

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.

TEMPEST Addendum:

- An addendum to the FFC that provides information to the CTTA to aid in the determination of what TEMPEST countermeasures, if any, need to be applied.

TEMPEST Counter Measure Review (TCR):

- The review conducted or validated by the Certified TEMPEST Technical Authority to document the recommended TEMPEST countermeasures for the project.

Vault:

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

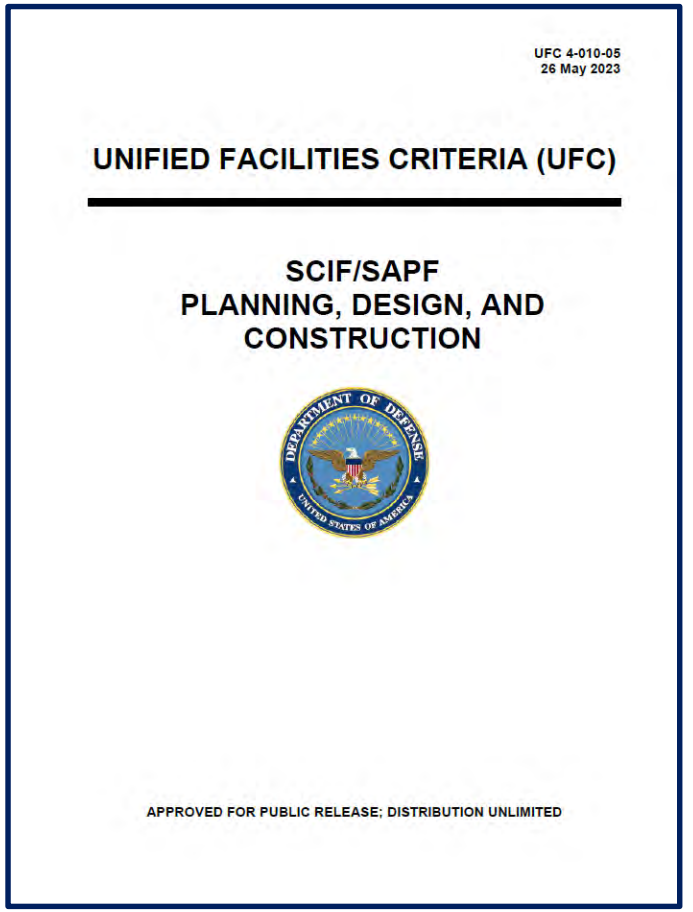
Waveguide:

- Devices installed at perimeter penetrations that are formed by metal tubing or ducting intended to attenuate wave energy.

NAVFAC Naval Facilities Engineering Systems Command

UFC 4-010-05 SCIF/SAPF PLANNING, DESIGN, AND CONSTRUCTION

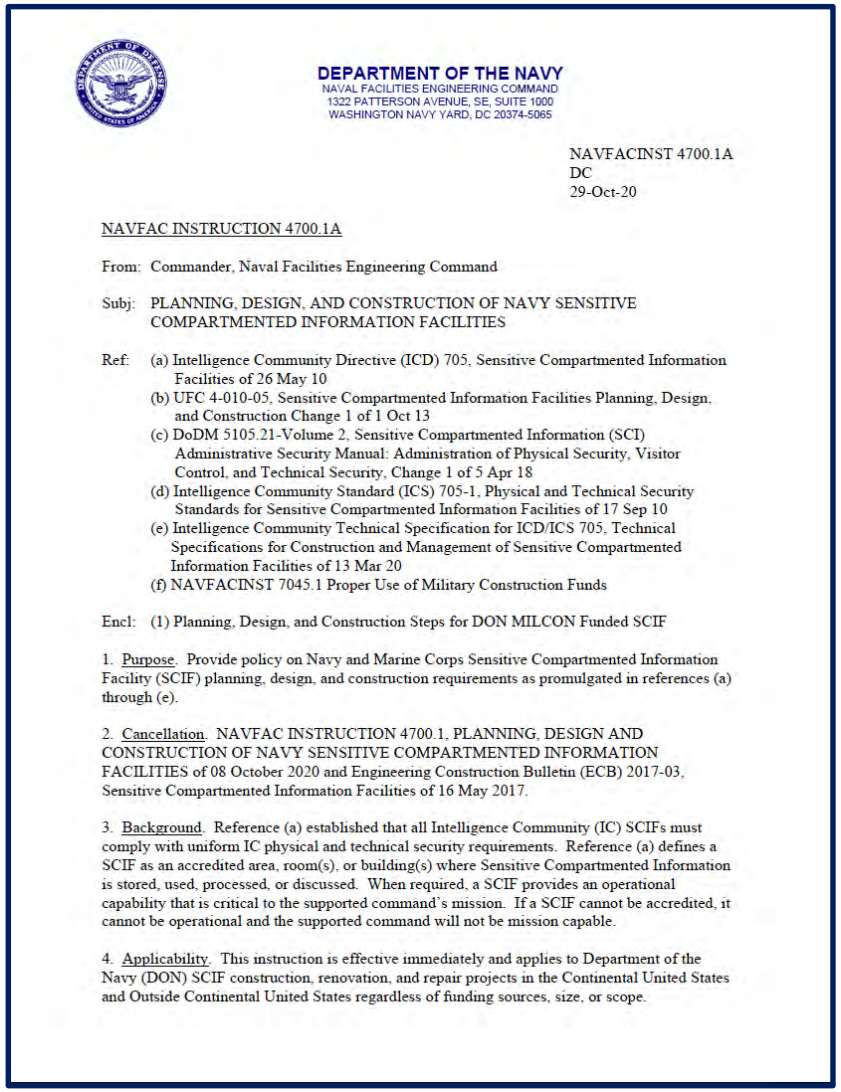
- **PURPOSE:** To provide unified criteria and make the planning, design and construction communities aware of policy requirements and ensure appropriate implementation.
- **PREPARING ACTIVITY:** NAVFAC
  - Point of contact: John Lynch
- **CURRENT DOCUMENT STATUS:**
  - Published May 2023, Available on the Whole Building Design Guide Website (www.wbdg.org)



NAVFAC Naval Facilities Engineering Systems Command

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 PDCC
  - 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
  - Version 4700.1**B** currently being developed and vetted.



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.

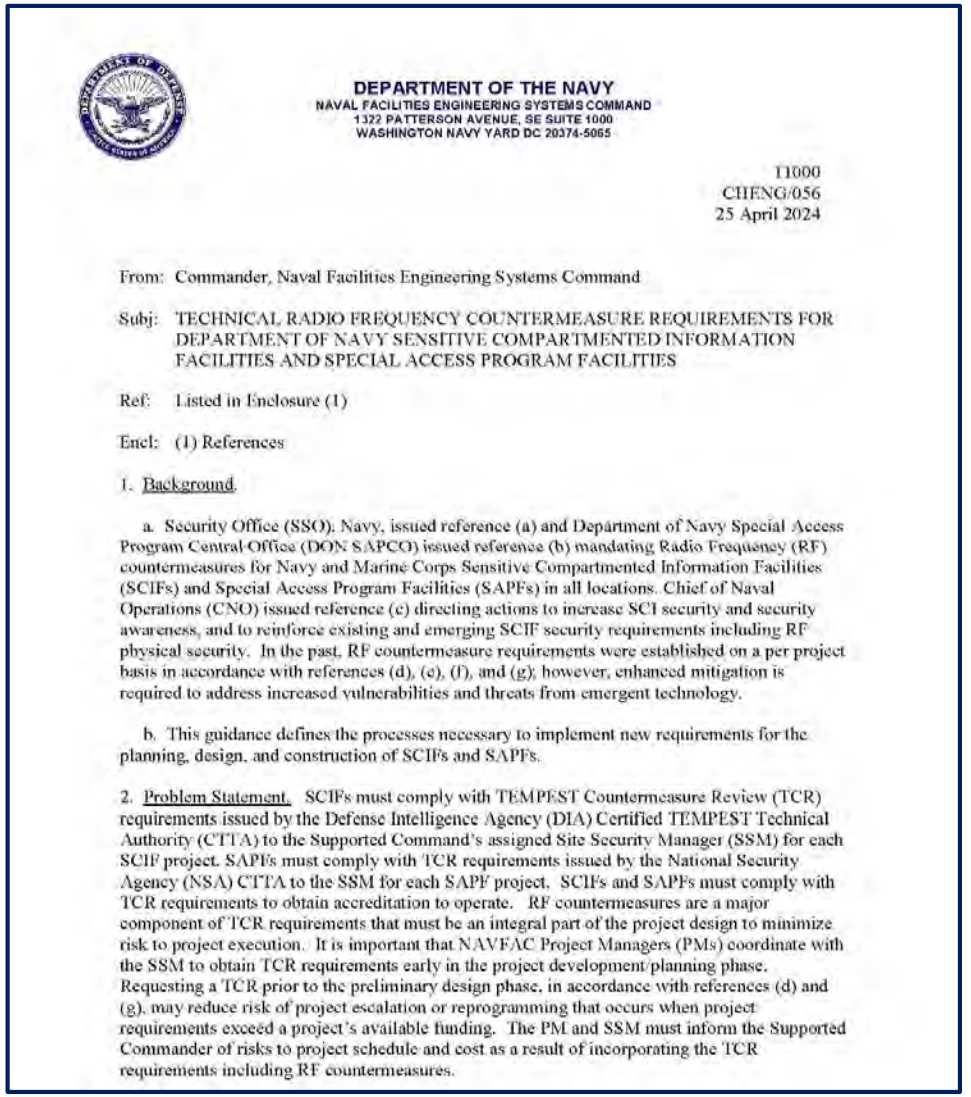
3. Background. Reference (a) established that all Intelligence Community (IC) SCIFs must comply with uniform IC physical and technical security requirements. Reference (a) defines a SCIF as an accredited area, room(s), or building(s) where Sensitive Compartmented Information is stored, used, processed, 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.

NAVFAC 11000 CHENG/056

Technical RF Countermeasure Requirements for DoN SCIFs & SAPFs

- **PURPOSE:** Issued to improve execution and budgeting of SCIF/SAPF projects to meet mission needs of Supported Commands.
  - Defines processes necessary to implement new requirements for the planning, design, and construction of SCIFs and SAPFs.
  - Encourages NAVFAC to coordinate with the Supported Command's SSM to obtain TCR requirements early in the project development/planning phase.
  - Requires NAVFAC to implement TCR requirements including RF countermeasures in construction documents for all current and future Navy and Marine Corps projects that include SCIFs/SAPFs.
  - Outlines process steps for NAVFAC staff to coordinate with the Supported Command's SSM based on execution stage of project.
- **PREPARING ACTIVITY: NAVFAC PDCC**
- **PUBLISHED: 25 April 2024**



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

11000
CHENG/056
25 April 2024

From: Commander, Naval Facilities Engineering Systems Command

Subj: TECHNICAL RADIO FREQUENCY COUNTERMEASURE REQUIREMENTS FOR DEPARTMENT OF NAVY SENSITIVE COMPARTMENTED INFORMATION FACILITIES AND SPECIAL ACCESS PROGRAM FACILITIES

Ref: Listed in Enclosure (1)

Encl: (1) References

1. Background.

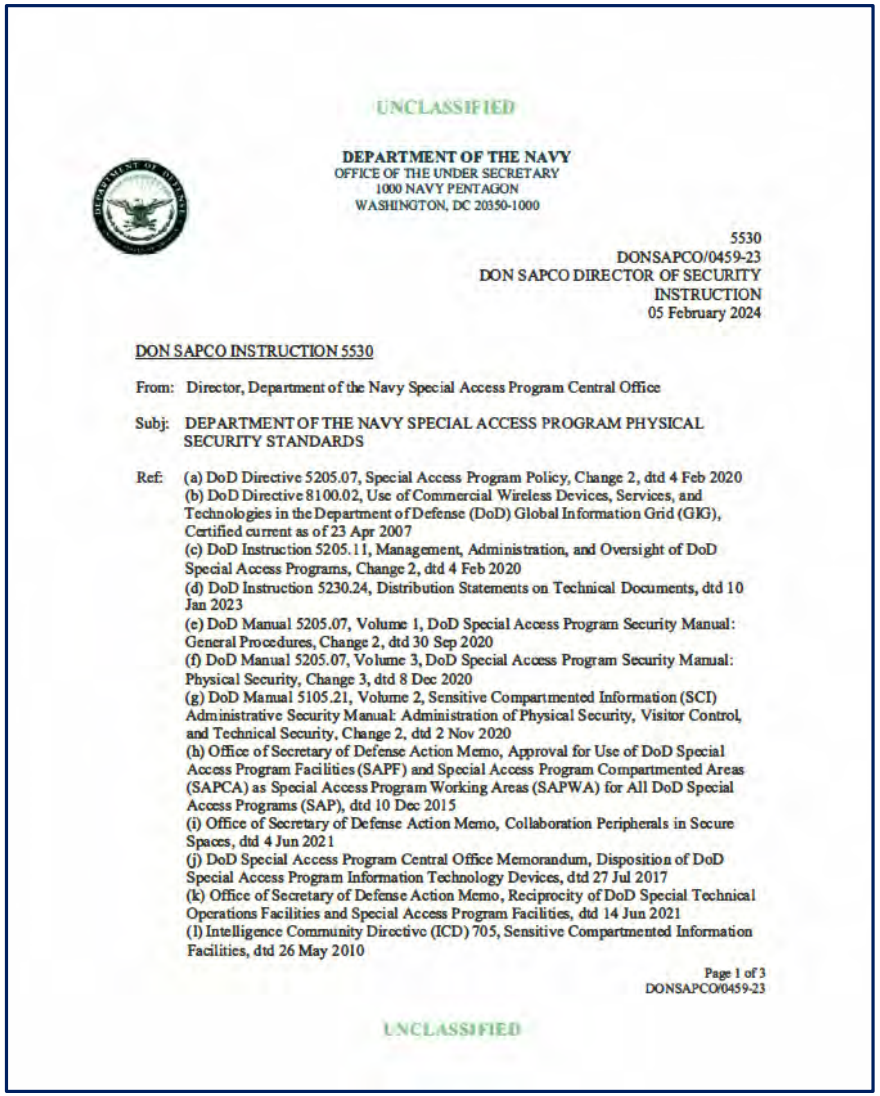
a. Security Office (SSO), Navy, issued reference (a) and Department of Navy Special Access Program Central Office (DON SAPCO) issued reference (b) mandating Radio Frequency (RF) countermeasures for Navy and Marine Corps Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program Facilities (SAPFs) in all locations. Chief of Naval Operations (CNO) issued reference (c) directing actions to increase SCI security and security awareness, and to reinforce existing and emerging SCIF security requirements including RF physical security. In the past, RF countermeasure requirements were established on a per project basis in accordance with references (d), (e), (f), and (g); however, enhanced mitigation is required to address increased vulnerabilities and threats from emergent technology.

b. This guidance defines the processes necessary to implement new requirements for the planning, design, and construction of SCIFs and SAPFs.

2. Problem Statement. SCIFs must comply with TEMPEST Countermeasure Review (TCR) requirements issued by the Defense Intelligence Agency (DIA) Certified TEMPEST Technical Authority (CTTA) to the Supported Command's assigned Site Security Manager (SSM) for each SCIF project. SAPFs must comply with TCR requirements issued by the National Security Agency (NSA) CTTA to the SSM for each SAPF project. SCIFs and SAPFs must comply with TCR requirements to obtain accreditation to operate. RF countermeasures are a major component of TCR requirements that must be an integral part of the project design to minimize risk to project execution. It is important that NAVFAC Project Managers (PMs) coordinate with the SSM to obtain TCR requirements early in the project development/planning phase. Requesting a TCR prior to the preliminary design phase, in accordance with references (d) and (g), may reduce risk of project escalation or reprogramming that occurs when project requirements exceed a project's available funding. The PM and SSM must inform the Supported Commander of risks to project schedule and cost as a result of incorporating the TCR requirements including RF countermeasures.

DON SAPCO Instruction 5530
DON Special Access Program Physical Security Standards

- **PURPOSE:** Provides supplemental guidance to DoD Manual (SAP Physical Security) and ICD/ICS 705 (Tech Spec for SCIFs)
    - Implements and ensures consistency of physical security standards across the DON SAP enterprise
- **APPLICABILITY:** Applies to DON SAP Facilities (SAPFs) accredited to receive, generate, process, use, discuss, store, manufacture, or test SAP classified information.
- **PREPARING ACTIVITY:** DON SAPCO (Director for Special Access Program Central Office)
- **PUBLISHED: 25 April 2024**



UNCLASSIFIED

DEPARTMENT OF THE NAVY
OFFICE OF THE UNDER SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

5530
DONSAPCO/0459-23
DON SAPCO DIRECTOR OF SECURITY
INSTRUCTION
05 February 2024

DON SAPCO INSTRUCTION 5530

From: Director, Department of the Navy Special Access Program Central Office

Subj: DEPARTMENT OF THE NAVY SPECIAL ACCESS PROGRAM PHYSICAL SECURITY STANDARDS

Ref: (a) DoD Directive 5205.07, Special Access Program Policy, Change 2, dtd 4 Feb 2020
(b) DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), Certified current as of 23 Apr 2007
(c) DoD Instruction 5205.11, Management, Administration, and Oversight of DoD Special Access Programs, Change 2, dtd 4 Feb 2020
(d) DoD Instruction 5230.24, Distribution Statements on Technical Documents, dtd 10 Jan 2023
(e) DoD Manual 5205.07, Volume 1, DoD Special Access Program Security Manual: General Procedures, Change 2, dtd 30 Sep 2020
(f) DoD Manual 5205.07, Volume 3, DoD Special Access Program Security Manual: Physical Security, Change 3, dtd 8 Dec 2020
(g) DoD Manual 5105.21, Volume 2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security, Change 2, dtd 2 Nov 2020
(h) Office of Secretary of Defense Action Memo, Approval for Use of DoD Special Access Program Facilities (SAPF) and Special Access Program Compartmented Areas (SAPCA) as Special Access Program Working Areas (SAPWA) for All DoD Special Access Programs (SAP), dtd 10 Dec 2015
(i) Office of Secretary of Defense Action Memo, Collaboration Peripherals in Secure Spaces, dtd 4 Jun 2021
(j) DoD Special Access Program Central Office Memorandum, Disposition of DoD Special Access Program Information Technology Devices, dtd 27 Jul 2017
(k) Office of Secretary of Defense Action Memo, Reciprocity of DoD Special Technical Operations Facilities and Special Access Program Facilities, dtd 14 Jun 2021
(l) Intelligence Community Directive (ICD) 705, Sensitive Compartmented Information Facilities, dtd 26 May 2010

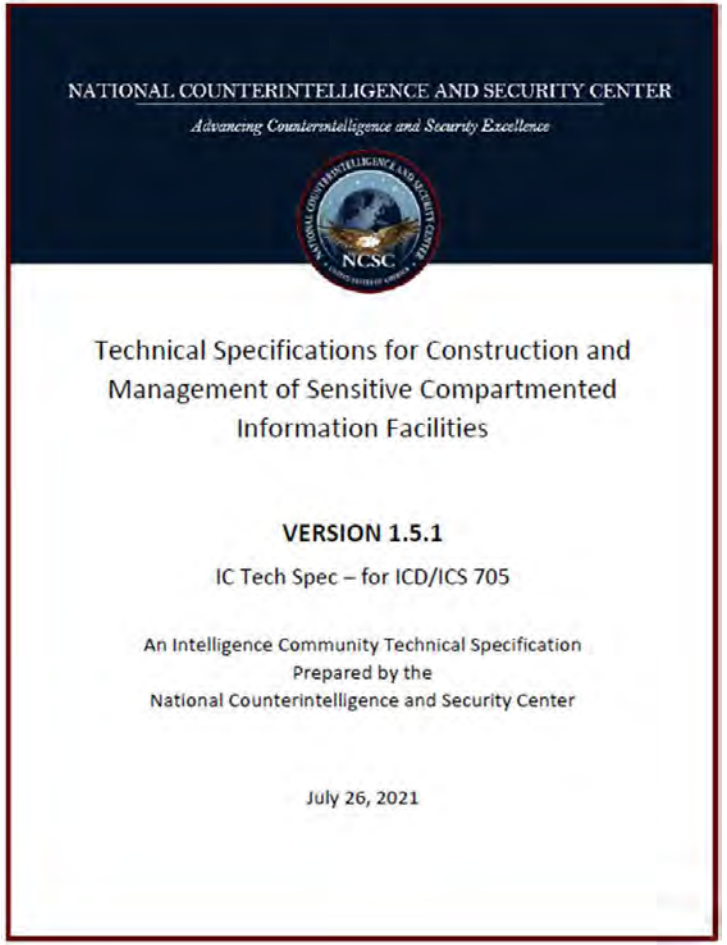
Page 1 of 3
DONSAPCO/0459-23

UNCLASSIFIED

NAVFAC Naval Facilities Engineering Systems Command

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities

- **PURPOSE: ICD/ICS 705-Tech Spec**
  - Sets forth the physical and technical security specifications and best practices for meeting standards of Intelligence Community Standard (ICS) 705-01 (Physical and Technical Standards for Sensitive Compartmented Information Facilities).
- **PREPARING ACTIVITY:**
  - OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
  - National Counterintelligence and Security Center
- **CURRENT DOCUMENT :**
  - July 26, 2021, v 1.5.1


NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Advancing Counterintelligence and Security Excellence

NCSC

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities

VERSION 1.5.1

IC Tech Spec – for ICD/ICS 705

An Intelligence Community Technical Specification
Prepared by the
National Counterintelligence and Security Center

July 26, 2021

NAVFAC Naval Facilities Engineering Systems Command

Classifications of Facilities

- **There are Six Classifications, we typically deal with three.**
  - **Closed Storage:**
    - An accredited facility where SCI or SAP material is required to be stored in GSA-approved storage containers when not in use.
      - This includes documents, computer hard drives, and storage media.
  - **Open Storage:**
    - An accredited facility in which SCI or SAP information may be openly stored or processed without using a GSA-approved storage container.
  - **Continuous Operation:**
    - An accredited facility staffed and operated 24/7.

DOD M 5105.21 Vol 2: Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security

NAVFAC Naval Facilities Engineering Systems Command

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)

NAVFAC Naval Facilities Engineering Systems Command

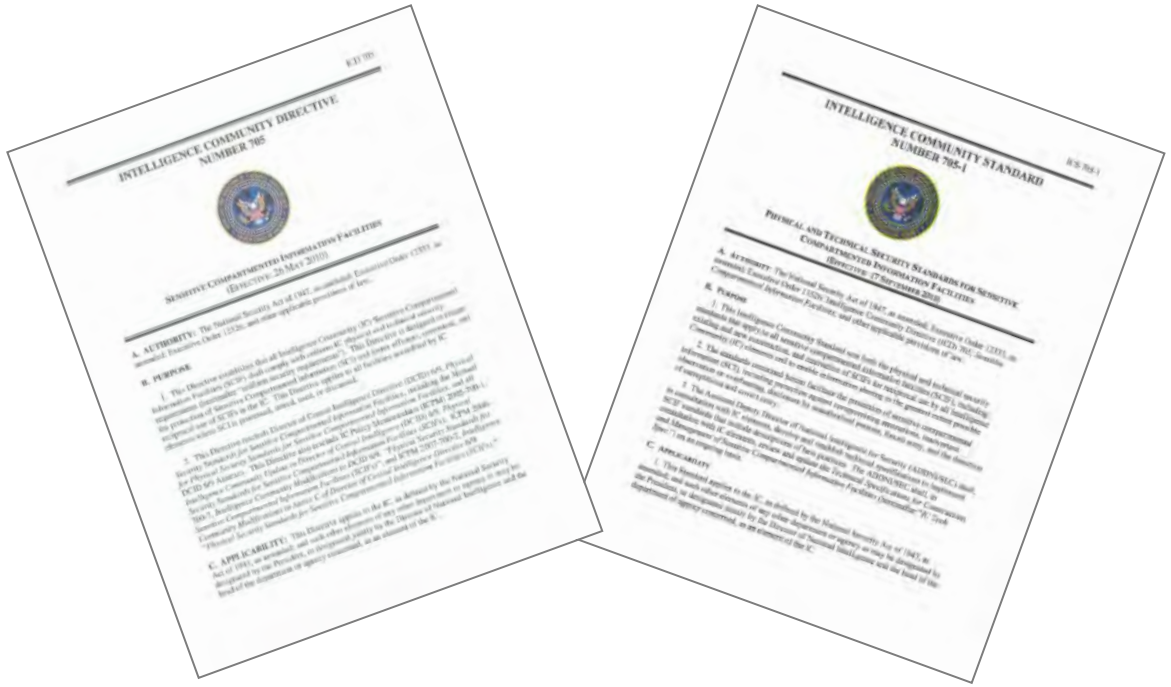
Accreditation (The Ultimate Goal !!)

- **Accreditation is a formal process to ensure that a facility has been designed, constructed, inspected, and certified to operate in accordance with the provisions of ICD 705.**
- **Refer to DoDM 5105.21, Vol 2 and DoDM 5205.07 Vol 3, DONSAPCO INST 5300 for the DoD/DoN policy on 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.**

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC Responsibilities

- As one of the design and construction agents for the Department of Defense, it is **imperative** that NAVFAC understands the requirements contained in the UFC, NAVFAC policies, DON policy, DoD Manuals and the Intelligence Community Directives and Standards (ICD/ICS) and include them in project requirements.
- Documents affect :
  - Planning
  - SAES or RFP Development
  - Design
  - Construction



SCIF/SAPF CONSTRUCTION IS A TEAM EFFORT!

NAVFAC
Naval Facilities Engineering Systems Command

Supported Command

- **THIS IS WHERE IT ALL STARTS!!**
- **Supported Command's Senior Intelligence Officer/Special Security Officer**
  - Initiates Concept Approval Request
    - The concept approval is **the first critical element** in the establishment of a SCIF.
    - Concept approvals certifies that a clear operational requirement exists for the SCIF and there is no existing SCIF to support the requirement.
  - Signs the Concept Approval Request (CAR), making sure to factor in NAVADMIN 169/23 and NISPD-09-22 (RF Countermeasures) into the planning process.
  - Route the complete CAR package and the RF shielding acknowledgement memo to SSO Navy/DONSAPCO via Regional Cognizant Security Authority (RCSA/RSSO/DONSAPCO) for approval or disapproval.
  - **Appoints/Identifies Site Security Manger (SSM)**
  - The Supported Command SSO or Site Security Manger (SSM) will draft the Construction Security Plan (CSP), Pre-Construction Fixed Facility Checklist (Pre-CON FFC), Pre Construction Checklist (Pre-CON Checklist), and TEMPEST Checklist and submit to AO via RSSO/SSO/PSO for approval.

NAVFAC Naval Facilities Engineering Systems Command

THE NAVFAC PROJECT TEAM

NAVFAC
Naval Facilities Engineering Systems Command

SCIF and SAPF NAVFAC Project Team

- **Facility/Project Planner**
  - Reviews CRB Guidelines – RF countermeasures/ESS
  - Reviews NAVFACINST 4700.1
  - Reviews UFC 4-010-05
  - Responsible for developing, planning, design and gathering project requirements
  - Working with the supported command Senior Intelligence Officer (SIO) and ensures the supported command has concept approval for SCIF/SAPF prior to finalizing planning documents (DD 1391/BFR)
  - Ensures supported command (SIO) has appointed a Site Security Manager (SSM) and identified the Accrediting Official (AO)
  - Ensures SSM has completed Construction Security Plan (CSP), preliminary Fixed Facility Checklist (FFC) and TEMPEST Checklist.
  - Incorporates security requirements established by the CSP and the TEMPEST Countermeasure Review (TCR) into the project scope and budget

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF NAVFAC Project Team

- **Project Manager (PM)**
  - Reviews CRB Guidelines – RF countermeasures/ESS
  - Reviews NAVFACINST 4700.1
  - Reviews UFC 4-010-05
  - Responsible for planning, design, construction and gathering project requirements
  - Working with the NAVFAC Facility Planner, ensures supported command has concept approval for SCIF/SAPF prior to finalizing planning documents
  - Ensures supported command has appointed an SSM and identified the AO
  - Ensures SSM has completed CSP, preliminary FFC and TEMPEST Checklist/Tempest Countermeasure Review (TCR).
  - Four Questions need to be asked (and answered in the affirmative) when supported commands states a need for SCIF/SAPF:
    1. Do you have Concept Approval?
    2. Who is the assigned SSM?
    3. Can I have a copy of the CSP? What is the status of the CSP?
    4. What are the TEMPEST requirements?”

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF NAVFAC Project Team

- **Design Manager (DM)**
  - Reviews NAVFACINST 4700.1
  - Reviews Chapters 1, 3, 4 and Appendix A of UFC 4-010-05
  - Responsible for leading / overseeing the design effort ensuring SCIF/SAPF requirements are appropriately included
  - Provides related design support during construction

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF NAVFAC Project Team

- **Construction Manager (CM)**
  - Reviews NAVFACINST 4700.1
  - Reviews Chapters 1, 4, and Appendix A of UFC 4-010-05
  - Reviews RFP or Plans and Specifications for SCIF/SAPF requirements
  - Have SSM attend the post award kickoff (PAK) or pre-construction conference (PRECON).
  - Discuss procedures for inspection and accreditation procedures including site security requirements and quality control inspections
  - Receives approved CSP from SSM
  - Regularly communicates with the SSM
  - Forwards approved technical submittals to SSM for information and inclusion in the FFC for accreditation.
  - Ensures construction and inspections are performed in accordance with the final design and contract specifications
  - Assists SSM/AO during the final inspection and accreditation/acceptance process

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF NAVFAC Project Team

- **Engineering Technician (ET)**
  - Reviews Chapters 1, 4, and Appendix A of UFC 4-010-05
  - Reviews RFP or Plans and Specifications for SCIF/SAPF requirements
  - Reviews Quality Control specifications for inspection requirements for SCIF/SAPF
  - Performs Quality Assurance during construction
  - Coordinate and accompany SSM on periodic inspections
  - Ensures QC Manager is documenting periodic inspections
  - Participates in Acceptance Inspections

NAVFAC Naval Facilities Engineering Systems Command

SCIF/SAPF ACCREDITATION TEAM MEMBERS

NAVFAC
Naval Facilities Engineering Systems Command

SCIF and SAPF Construction
Security Surveillance

- **NAVFACINST 4700.1A - Construction Personnel - Surveillance**
  - The Accrediting Official (AO), Site Security Manager (SSM), and Certified TEMPEST Technical Authority (CTTA) **ARE NOT** employees of or contracted by Naval Facilities Engineering Command (NAVFAC), the Department of Defense (DoD) Construction Agent or the Construction Contractor and these entities **ARE NOT** funded by the project (Military Construction (MILCON) project cost).
  - For most projects within the United States, its territories or possessions, Cleared American Guards (CAGs) or Construction Surveillance Technicians (CSTs) are not required by Intelligence Community Standard (ICS) 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities and Intelligence Community Technical Specification for ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities
  - When required by the CSP, the CAGs, and CSTs may be government employees, military personnel, or the requesting command may use contract personnel.
  - NAVFAC **does not** have contracting authority to contract for non-NAVFAC contractor support positions. (NAVSUP)

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF Construction
Security Surveillance

- **NAVFACINST 4700.1A Construction Personnel – Surveillance - Funding**
  - For Military Construction, the proper use of funds for CAGs and CSTs must follow **NAVFACINST 7045.1 Proper Use of Military Construction Funds**.
  - To avoid potential issues with regard to conflicts of interest, Cleared American Guards (CAGs) and Construction Security Technicians (CSTs) **ARE NOT** employees of NAVFAC, the DoD Construction Agent, or the construction contractor.
  - Where security surveillance is funded by the project, the **Requesting Command** is responsible for identifying the requirements, providing scope and budget information during the project planning, coordinating and managing the execution and expense of the apportioned project funds to provide the required security surveillance.
  - Construction Security Surveillance, CAGs and CSTs for SCIF and SAPF should use appropriations available for O&M (such as O&M, RDT&E, or Working Capital Fund (WCF) resources).
  - For MILCON projects, where the project sponsor chooses to program project funds for these efforts, the requirements **must be clearly identified** in Block 12 of the DD1391, which allows for confirmation of inclusion without compromising security.
    - This choice comes with some risk if not budgeted sufficiently

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF Construction
Security Surveillance Team Members

- The guidelines to provide special security surveillance during construction activities are established in **ICD/ICS 705**
  - Cognizant Security Authority (CSA) – Special Security Officer (SSO) Navy
  - Accrediting Official (AO) or SAPF Accrediting Official (SAO)
  - Certified TEMPEST Technical Authority (CTTA)
  - Site Security Manager (SSM)
  - Construction Surveillance Technicians (CST)
  - Cleared American Guards (CAG)
- To avoid conflict of interest, above personnel cannot be employees of the construction contractor, employees of or contracted by the DoD construction agent
- The requirement for these positions is contained in the Construction Security Plan (CSP) which is developed for each project by the Site Security Manager (SSM) and approved by the Accrediting Official (AO).
- The roles and responsibilities of these positions are summarized in the following slides.
- **The AO and SSM are non-NAVFAC personnel.**
  - These positions have historically been supported by government or contracted personnel.

NAVFAC Naval Facilities Engineering Systems Command

SCIF Construction

Cognizant Security Authority – Navy Special Security Officer (SSO)

- **Special Security Officer (SSO)**
  - Responsible for the security management, implementation, and oversight of SCI security programs for the DON's SCI security program
  - Cognizant Security Authority (CSA) assigns AO.
    - **Defense Intelligence Agency (DIA)**
  - For Navy and USMC, the service CSA is Navy Special Security Officer (SSO Navy) (SECNAVINST 5510.30C/DOD M 5105.21 Vol 2)
  - Accepts Concept Approval Request (CAR) and approves/disapproves Concept Approval (CA)
  - Approval authority for SCIF security requirements and accreditation
  - Routes the Construction Security Plan (CSP), Fixed Facility Checklist (FFC), TEMPEST Checklist to DIA
  - SSO with assistance from SSM documents construction progress
  - Submits final accreditation package to DIA upon completion of SCIF construction.
  - Provides a Pre-Accreditation inspection
  - Final Physical and Tempest accreditation messages are issued by DIA

SCIF Construction

Regional Cognizant Security Authority (RCSA)

- **Regional Cognizant Security Authority (RCSA) (aka – Regional Special Security Officer- RSSO)**
  - Accepts and Reviews Concept Approval Request (CAR) and sends to SSO Navy for approval
  - Review and route the Construction Security Plan (CSP), Fixed Facility Checklist (FFC), TEMPEST Checklist to SSO Navy who will send to AO/DIA for approval
  - RCSA/RSSO with assistance from SSM documents construction progress
  - Provides a Pre-Accreditation inspection
  - Submits final accreditation package to SSO Navy and AO/DIA upon completion of SCIF construction.
  - Final Physical and Tempest accreditation messages are issued by DIA
  - Regional SSOs/RCSA
    - 9 Offices world-wide (Groton, Jacksonville, Whidbey, Pearl Harbor, San Diego, Norfolk, Minneapolis, Naples, Yokosuka)

NAVFAC Naval Facilities Engineering Systems Command

SCIF Construction
Accrediting Official

- **Accrediting Official (AO)**
  - **AO for DON SCIFs is Defense Intelligence Agency (DIA)**
  - Approves design concept – Concept Approval (CA)
  - Approval authority for SCIF security requirements and accreditation
  - Assigns SCIF ID
  - Approves Construction Security Plan (CSP)
  - Approves Fixed Facility Checklist (FFC)
  - Approves TEMPEST Countermeasure Review (TCR) and Recommendations
  - Approve Pre-Construction Checklist
  - Upon receipt of CA for SCIF, sends message requiring supported command to designate a site security manager (SSM).
  - Provides Accreditation to operate
  - **The AO is not a NAVFAC or construction contractor employee**

NAVFAC Naval Facilities Engineering Systems Command

SAPF Construction
Program Security Officer (PSO)

- **SAPF Program Security Officer (PSO)**
  - PSO is responsible for program security management and execution of all security policies and requirements for a specific SAP program (*Similar to the Senior Intelligence Officer (SIO) for SCIF*)
  - Works closely with SAO and CTTA to ensure security of all SAPF facilities
  - Endorse Concept Approval Request (CAR)
  - Review all facility documentation/checklists – FFC/TEMPEST/Pre-Con
  - Review TEMPEST Countermeasure Review (TCR)
  - NOT authorized (Unless they are also a SAO) to accredit facilities or give final approval of construction related decisions that impact accreditation.

NAVFAC Naval Facilities Engineering Systems Command

SAPF Construction
Accrediting Official

- **SAPF Accrediting Official (SAO)**
  - DON SAPCO Director of Security (DoS) appoints SAO.
  - Approval authority for SAPF security requirements and accreditation
  - Approves Design Concept and Final Design
  - Approves Construction Security Plan (CSP)
  - Approves Fixed Facility Checklist (FFC)
  - Approves TEMPEST Countermeasure Review (TCR) and Recommendations in coordination with DONSAPCO CTTA.
  - Upon receipt of Concept Approval (CA) for SAPF, sends message **requiring supported command to designate a site security manager (SSM)**
  - Provides Accreditation to operate.
  - **The AO is not a NAVFAC or construction contractor employee**

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF Construction

Certified TEMPEST Technical Authority

- **Certified TEMPEST Technical Authority (CTTA)**
  - Authority to establish TEMPEST Countermeasures for accreditation.
  - Each project with a SCIF/SAPF requires a TEMPEST countermeasures review (TCR), performed by the CTTA.
    - The SSM will request a TCR by submitting a TEMPEST addendum (TEMPEST Checklist) for review.
    - Project Manager (PM) to submit TEMPEST Design Summary to SSM prior to establishing proposed TEMPEST design parameters for project.
    - PM to ensure supported command submits TEMPEST Checklist to the Certified Tempest Technical Authority (CTTA) for TEMPEST Counter Measure Review (TCR).
    - Based on the results of the TCR, the CTTA will determine the most cost-effective countermeasures and will document these requirements in writing to CSA and AO.
  - SCIF CTTAs are at Defense Intelligence Agency (DIA) and certified by DIA
  - SAPF CTTAs are at DONSAPCO and certified by the National Security Agency (NSA)

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF Construction

Certified TEMPEST Technical Authority

In the past, RF countermeasure requirements were established on a per project basis in accordance with DoD and DNI policy however, enhanced mitigation is currently required to address increased vulnerabilities and threats from emergent technology.

So……

In January 2023 Special Security Officer (SSO), Navy, issued SSO Navy Message, Naval Intelligence Security Policy (NISP) Directive: 001-23, Mandatory Radio Frequency Countermeasure Requirements for all New Navy and Marine Corps Sensitive Compartmented Information Facilities (Re-iterated in NAVADMIN 169/23 SCIF Policy)

In February 2024 Department of Navy Special Access Program Central Office (DON SAPCO) issued DON SAPCO Instruction 5530, Department of the Navy Special Access Program Physical Security Standards mandating Radio Frequency (RF) countermeasures for Navy and Marine Corps Special Access Program Facilities (SAPFs) in all locations.

TEMPEST Countermeasure Reviews (TCRs) are now REQUIRED for each project.

NAVFAC Naval Facilities Engineering Systems Command

SCIF/SAPF CONSTRUCTION SECURITY SURVEILLANCE TEAM MEMBERS

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF
Construction Security Surveillance

- **Site Security Manager (SSM)**
  - **Appointed by the Supported Command** or AO upon receipt of Concept Approval (CA); **This appointment must be done at the planning phase**
  - Works with AO from planning through construction through accreditation
  - Can be U.S. Government Employee (not NAVFAC/ Department of Defense (DoD) Construction Agent), Military member, or contractor NOT associated construction contractor
  - Prepares and submits Construction Security Plan (CSP), Fixed Facility Checklist (FFC) and TEMPEST Checklist for AO approval and action
  - Forwards TEMPEST Countermeasure Review (TCR) from CTTA
  - Single point of contact and responsible for security aspects during design and during construction ensures procedures to control site access are implemented
  - Works with AO/SAO/CTTA as necessary when issues arise that may impact accreditation
  - Performs periodic inspections during construction
    - Inspections should be performed jointly with ET and QC Manager
  - Receives technical submittals associated with SCIF/SAPF from CM for information and inclusion in FFC for accreditation
  - May take photo/video record of construction progress
  - Has 24/7 access to the construction site.

NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF
Construction Security Surveillance

- **Construction Surveillance Technician (CST)**
  - **Normally not required for projects within the U.S. and its territories**
  - When required by the CSP/AO during the construction development phase, CSTs work with SSM and are specially trained in surveillance and the construction trade to monitor construction activities to deter technical penetrations and thwart implanted technical collection devices.
    - Outside US and not under Chief of Mission (COM), must possess a U.S. TOP SECRET clearance
    - CST not required when U.S. TOP SECRET-cleared contractors are used
  - CSTs supplement site access controls, implement screening and inspection procedures in accordance with the Construction Security Plan (CSP)
  - Specially trained in surveillance and the construction trade to deter technical penetrations and thwart implanted technical collection devices
  - Policy does not direct who must hire CSTs or CAGs (Clarification upcoming)
  - For SAPFs, CST are required if SSM has no construction experience
  - **Not a NAVFAC or construction contractor employee**
    - **May be government employees, military personnel, or the requesting command may use contract personnel.**

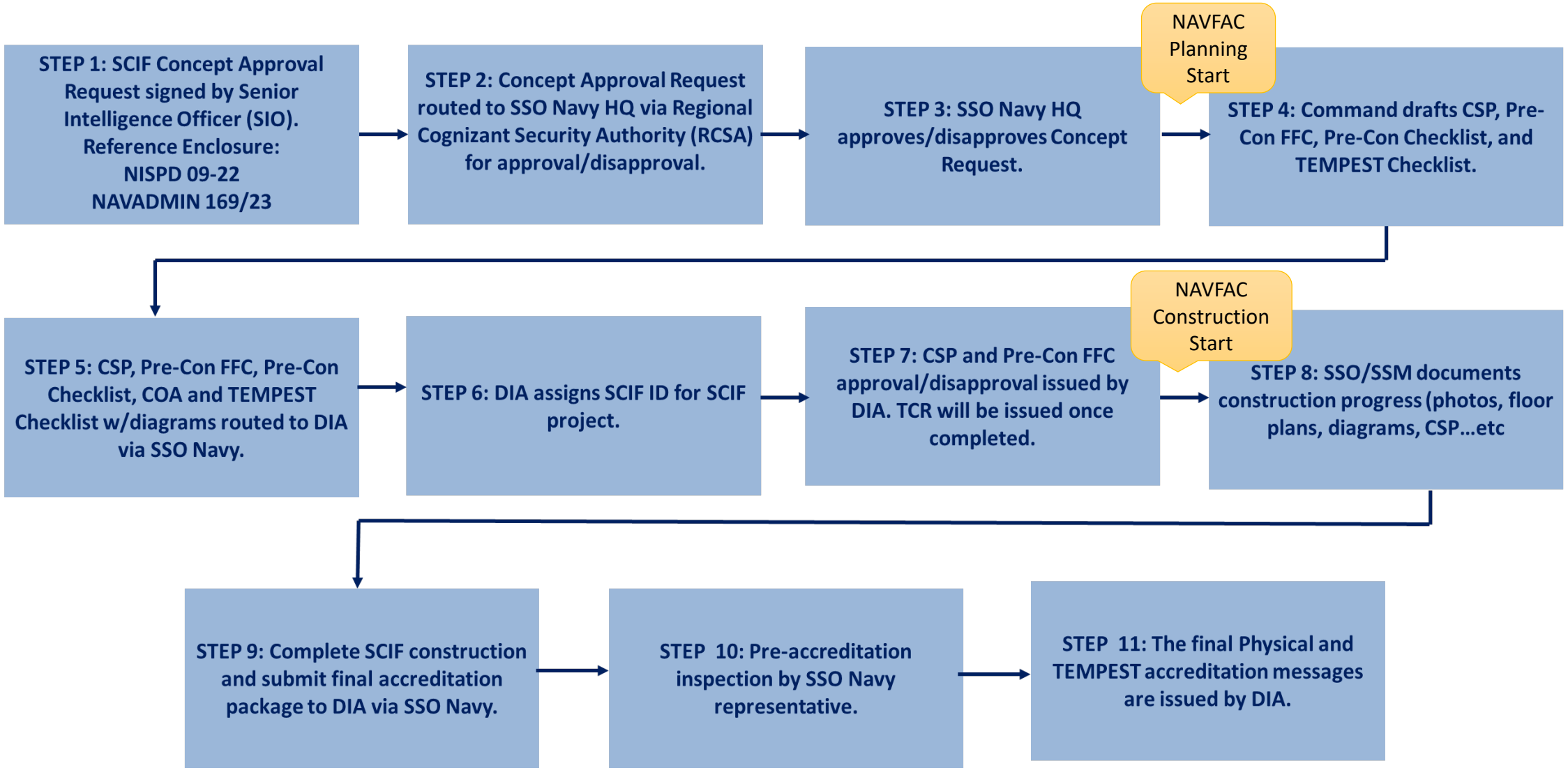
NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF
Construction Security Surveillance

- **Cleared America Guard (CAG)**
  - Normally not required for projects within the U.S. and its territories
  - Possess a U.S. SECRET clearance/TOP SECRET when under COM authority
  - When required by the CSP during the construction development phase, Works with SSM and CST
  - Performs access-control functions at all 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.
  - Conducts random inspections of site areas to ensure no prohibited materials have been brought on to the site.
  - Specially trained in surveillance and the construction trade to deter technical penetrations and thwart implanted technical collection devices
  - Policy does not direct who must hire CSTs or CAGs (This needs clarification)
  - Not a NAVFAC or construction contractor employee
    - May be government employees, military personnel, or the requesting command may use contract personnel.

NAVFAC Naval Facilities Engineering Systems Command

SCIF Accreditation Process



NAVFAC Naval Facilities Engineering Systems Command

SCIF Accreditation Process

Step 1: SCIF Planning begins and the Senior Intelligence Officer (SIO) signs the Concept Approval Request (CAR), making sure to factor in NAVADMIN 169/23 and NISPD-09-22 into the planning process.

Step 2: The complete CAR package and the RF shielding acknowledgement memo will be routed to SSO Navy HQ via Regional Cognizant Security Authority (RCSA) for approval or disapproval.

Step 3: SSO Navy HQ issues Concept Approval (COA) or issues disapproved CAR via M3 message traffic to local RCSA and assigned PLA.

Step 4: The command Special Security Officer **(SSO)** or Site Security Manger **(SSM)** will draft the Construction Security Plan **(CSP),** Pre-Construction Fixed Facility Checklist **(Pre-CON FFC),** Pre Construction Checklist **(Pre-CON Checklist),** and **TEMPEST Checklist.**

> ***Pre-Construction FFC:** Since all information will not be available when submitting the Pre-Con-FFC during the initial planning stage, you must provide as much information as possible. You must also provide additional information as it becomes available or as requested by RCSA/SSO Navy HQ.

Step 5: The SSO will submit the CSP, Pre-Con FFC, Pre-Con Checklist, COA, and TEMPEST Checklist with the associated diagrams to their local RCSA for review. The RCSA will review the SCIF package for accuracy and completeness before forwarding to DIA via SSO Navy HQ for approval.

Step 6: DIA will assign the SCIF ID for the project and the DIA CTTA team will begin drafting the TEMPEST Countermeasure Review (TCR).

NAVFAC Naval Facilities Engineering Systems Command

SCIF Accreditation Process

Step 7: The DIA SCIF Branch will issue the CSP/Pre-Con FFC approval or disapproval. The DIA CTTA Team will release the TCR. The Command will complete the TCR requirements and submit the TEMPEST form B to DIA via SSO Navy. (This may vary for ships)

- **CSP Approval:** The construction contract can be awarded once the approved CSP has been received.
- **TCR:** DIA will issue the TCR which will outline the TEMPEST construction requirements for the build.
- **Pre-Con Approval:** SCIF construction can begin once the Pre-Con FFC approval has been received.

Step 8: The SSO or SSM will document the construction of the SCIF with photos, floor plans, diagrams, CSP, etc. During this time SSO Navy representatives may conduct a site visit if requested.

Step 9: Once construction has·been completed submit the final accreditation package (the updated CSP, FFC, and TEMPEST form B) to the RCSA for review. Once complete, the RCSA will forward the SCIF accreditation package to DIA via SSO Navy HQ for final accreditation.

Step 10: A Pre-Accreditation Inspection may be conducted by an SSO Navy representative.

Step 11: The final Physical and TEMPEST accreditation messages will be issued by DIA.

NAVFAC Naval Facilities Engineering Systems Command

Concept Approval Request (CAR)

The concept approval is the **first critical element** in the establishment of a SCIF/SAPF. Concept approvals certifies that a clear operational requirement exists for the SCIF and there is no existing SCIF/SAPF to support the requirement.

The Concept Approval Request (CAR) must be completed on supported command letterhead and contain the following information:

a. Address, floor and room numbers of the proposed SCIF/SAPF (if known).
b. A building description (12 story facility, located in a business park, etc.).
c. Identify the five (5) geographically closest SCIF's/SAPF's in the area *(Not required for ships).
d. Written justification from the command senior intelligence officer (SIO) on why each of these facilities are not suitable for co-utilization by organization. *(Not required for ships).
e. An official command mission brief clearly demonstrating the operational need for SCI access and SCI impact on the mission.
f. Identify organization SSO by appointment letter or status of funding and hiring of SSO position.
g. Clearly identify funding for the construction of the proposed facility and long term sustainment *(Not required for ships).
h. Documentation/memo signed by organizations comptroller showing the above funding requirements will be met *(Not required for ships).
i. DD-254 Contract number for project *(not required for government sites.)*
j. Attach the signed NISPD 001-23 RF shielding acknowledgement memo to the package.

* **Note: Be sure to review NAVADMIN 169/23, U.S. Navy Special Security Officer SCIF Operations**
* **Note: Be sure to review NISPD 009-22: SCIF concept approval process**
* **Note: Be sure to review DON SAPCO Instruction 5530 SAPF concept approval process**
* **Note: Contents may become classified, consult the appropriate classification guide for assistance.**

NAVFAC Naval Facilities Engineering Systems Command

SCIF Requirement – Concept Approval

- 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 Cognizant Security Authority (CSA), their designees, or DoD Component Senior Intelligence Official (SIO) are required to grant Concept Approval to establish a SCIF.
    - For the Navy and Marine Corps, the service CSA is SSO Navy

NAVFAC Naval Facilities Engineering Systems Command

SCIF Requirement – Concept Approval

- SSO Navy issues the Concept Approval via message. The message states:
  - **The Command must designate a Site Security Manager (SSM) to oversee the security of the project and complete all required administrative actions required for accreditation.**
  - The SSM will ensure that a Fixed Facility Checklist (FFC), Construction Security Plan (CSP), Pre-Construction Checklist, Tempest Checklist, Line Drawings along with this concept approval are submitted to SS0 Navy prior to commencing the any work related to the project.
- **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.**

NAVFAC Naval Facilities Engineering Systems Command

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 **(not NAVFAC or the construction contractor)** 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

NAVFAC Naval Facilities Engineering Systems Command

Construction Security Plan (CSP)

- Each project with SCIF/SAPF requires a CSP. The CSP:
  - Developed by the SSM and approved by the AO/SAO.
  - Addresses the application of security to planning, design, and construction.
  - Format and content is based on extent of construction and security concerns.
  - **Living document during design.**
  - Any modification of the CSP after construction contract award must be sent to the AO/SAO for approval prior to change implementation.

- DNI and DONSAPCO Policy states the CSP must be approved prior to construction. **THIS IS TOO LATE!**
  - MILCON budgets are locked 3 years prior to construction start.
    - An **initial-preliminary** CSP must be developed during the planning phase (**prior to submission of Program Final DD 1391)** to capture the scope and cost associated with security surveillance
  - CSPs must be finalized and approved by the AO during design phase.
- **CONSTRUCTION CONTRACTS CANNOT BE AWARDED WITHOUT AN APPROVED FINAL CSP.**

NAVFAC Naval Facilities Engineering Systems Command

Fixed Facility Checklist (FFC)

- The FFC is a standardized document developed by the requesting command to support the accreditation process.
  - Primary document utilized by the CSA in the decision making process for granting accreditation
  - The FFC documents physical, technical, and procedural security information for accreditation.
  - Preconstruction FFC must include all information available but inclusion of information regarding intrusion detection system, access control system and phone system are essential to ensuring approved components are installed.
- 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.

NAVFAC Naval Facilities Engineering Systems Command

Fixed Facility Checklist V1.5:

(Pre / Final) Fixed Facility Checklist

- Section A: General Information
- Section B: Security-in-Depth
- Section C: SCIF Security
- Section D: Doors
- Section E: Intrusion Detection Systems (IDS)
- Section F: Telecommunication Systems and Equipment Baseline
- Section G: Acoustical Protection
- Section H: Classified Destruction Methods
- Section I: Information Systems/TEMPEST/Technical Security

- **This checklist may contain classified information**
  - To be completed by SSM
  - NAVFAC can support

Classify Completed FFCs CONFIDENTIAL

NAVFAC Naval Facilities Engineering Systems Command

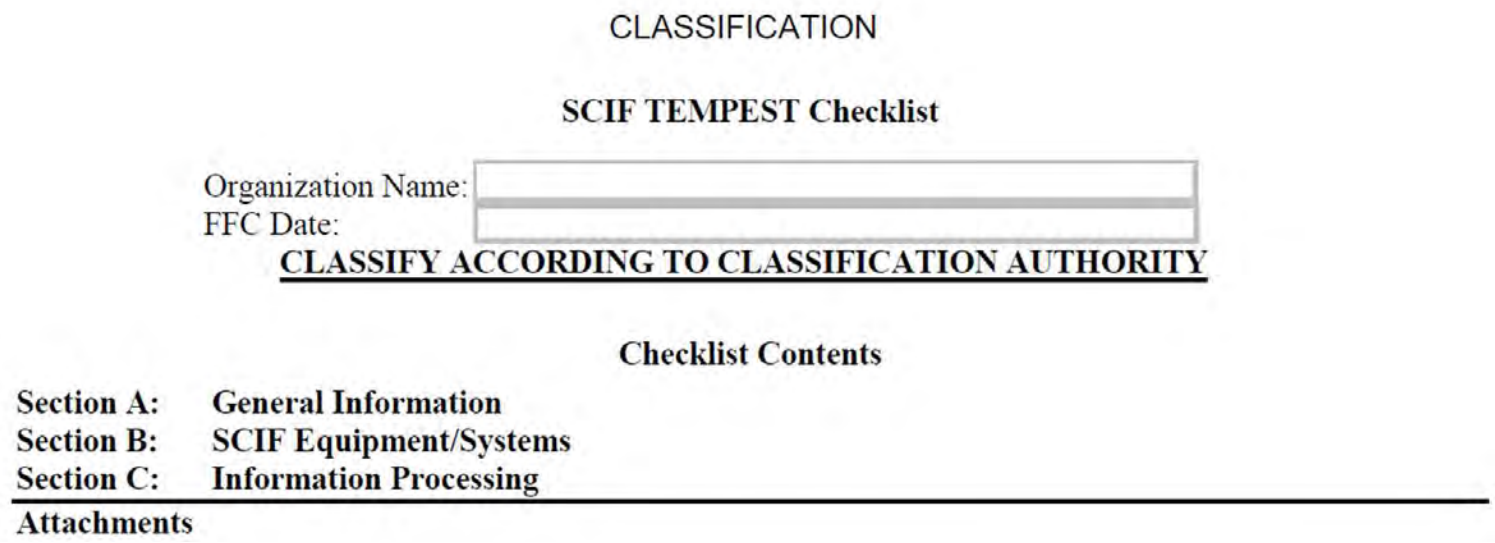
Pre-Construction Checklist

- This checklist is intended to provide the CSA/AO with the information required to determine the minimum security requirements for final SCIF accreditation and to assist the project personnel with planning and designing the SCIF appropriately and cost efficiently.
- When completing this checklist, provide as much detail as possible based upon what is known at the time it is being filled out.
    - If any information is not known, mark the question/section as unknown and provide a description in section 5 or on additional pages that are attached to the checklist when it is sent to the AO.
- This checklist is not intended to contain any classified information. Completing the checklist should not make it classified, however, consult with your AO or security office before sending a completed checklist across unclassified lines of communication.

NAVFAC Naval Facilities Engineering Systems Command

SCIF FORMS: SCIF TEMPEST Checklist :

Pre-TEMPEST Checklist



CLASSIFICATION

SCIF TEMPEST Checklist

Organization Name:
FFC Date:

CLASSIFY ACCORDING TO CLASSIFICATION AUTHORITY

Checklist Contents

Section A: General Information
Section B: SCIF Equipment/Systems
Section C: Information Processing

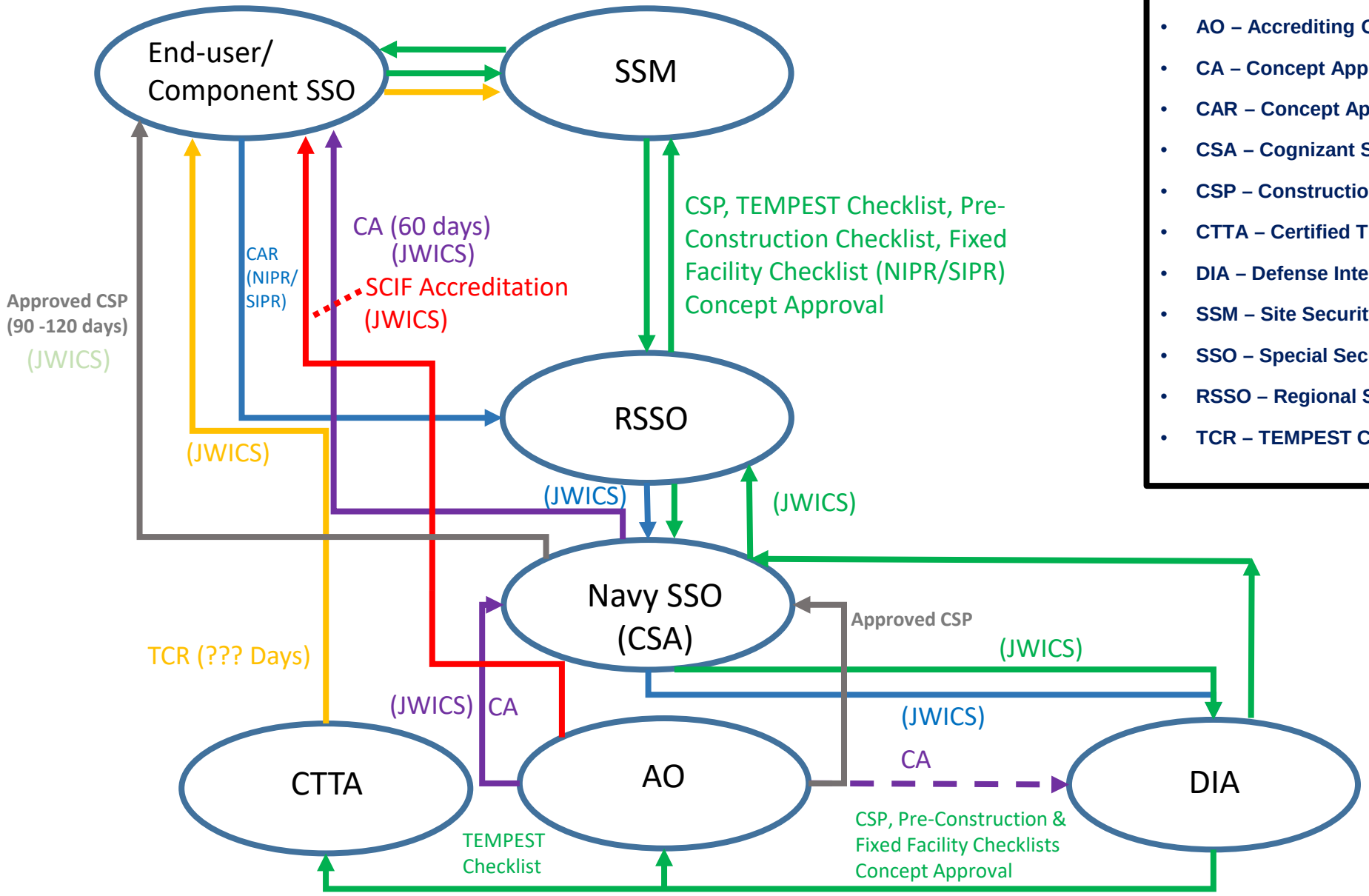
Attachments

- **The SCIF TEMPEST List will contain classified information (confidential)**
  - To be completed by SSM / submitted by SSO Navy via RCSA to AO (DIA) to CTTA for review
  - DIA CTTA sends a Tempest Countermeasure Review (TCR), which provides guidance for Tempest Accreditation; may include a list required Countermeasures
  - NAVFAC can support
  - May have impacts to Cost, Scope or Schedule

TEMPEST Countermeasure Review (TCR)
(TEMPEST Addendum/TEMPEST Checklist)

- Each facility that processes 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) with the FFC.
  - **Checklist when compiled is classified minimum of CONFIDENTIAL**
- Per DoDM 5105.21-Vol 2 (SCIF), The addendum will be submitted during the planning phase of the design. 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.**
- The CTTA will provide the TCR based on the TEMPEST addendum and recommend countermeasures to the AO as part of the accreditation process.

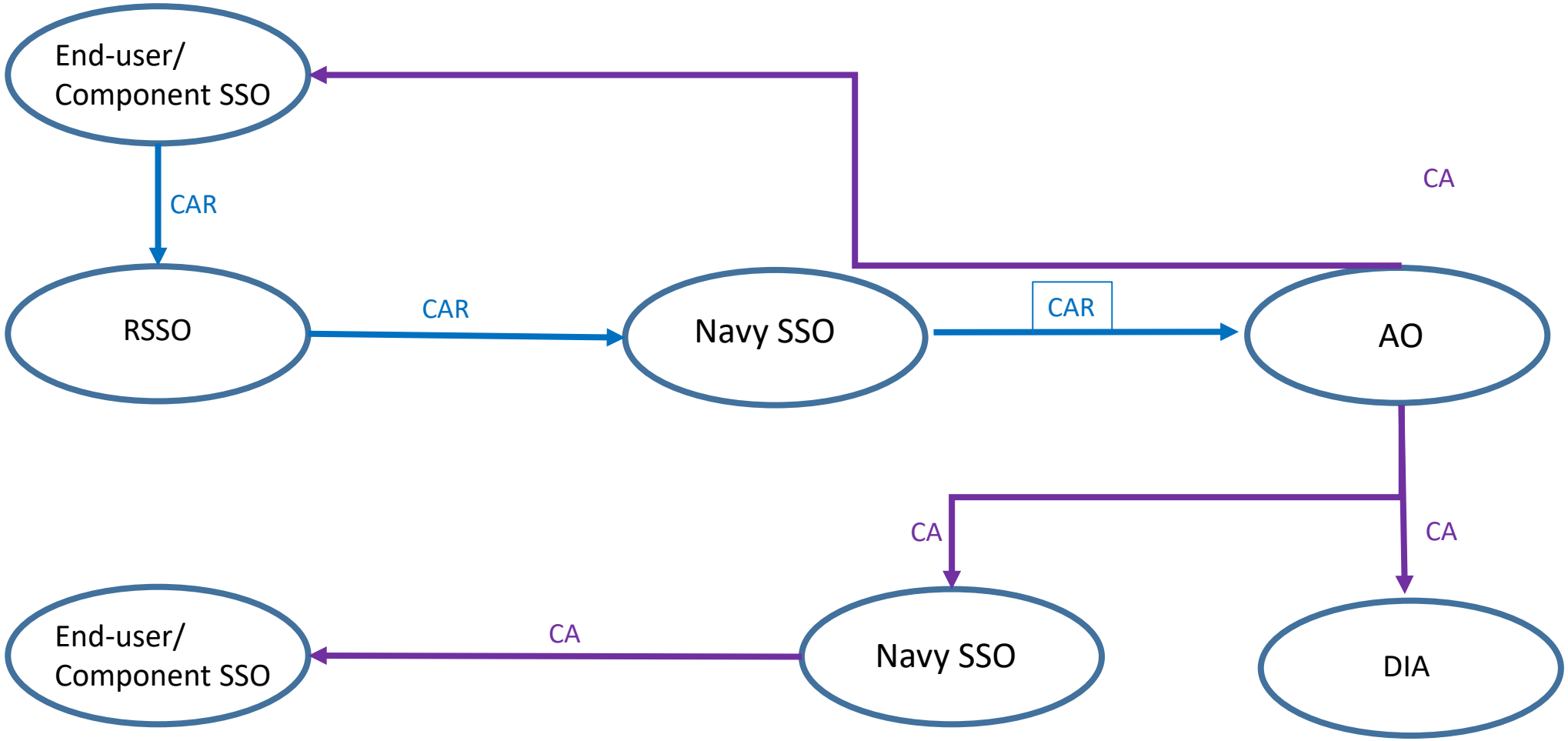
SCIF Concept Approval Process



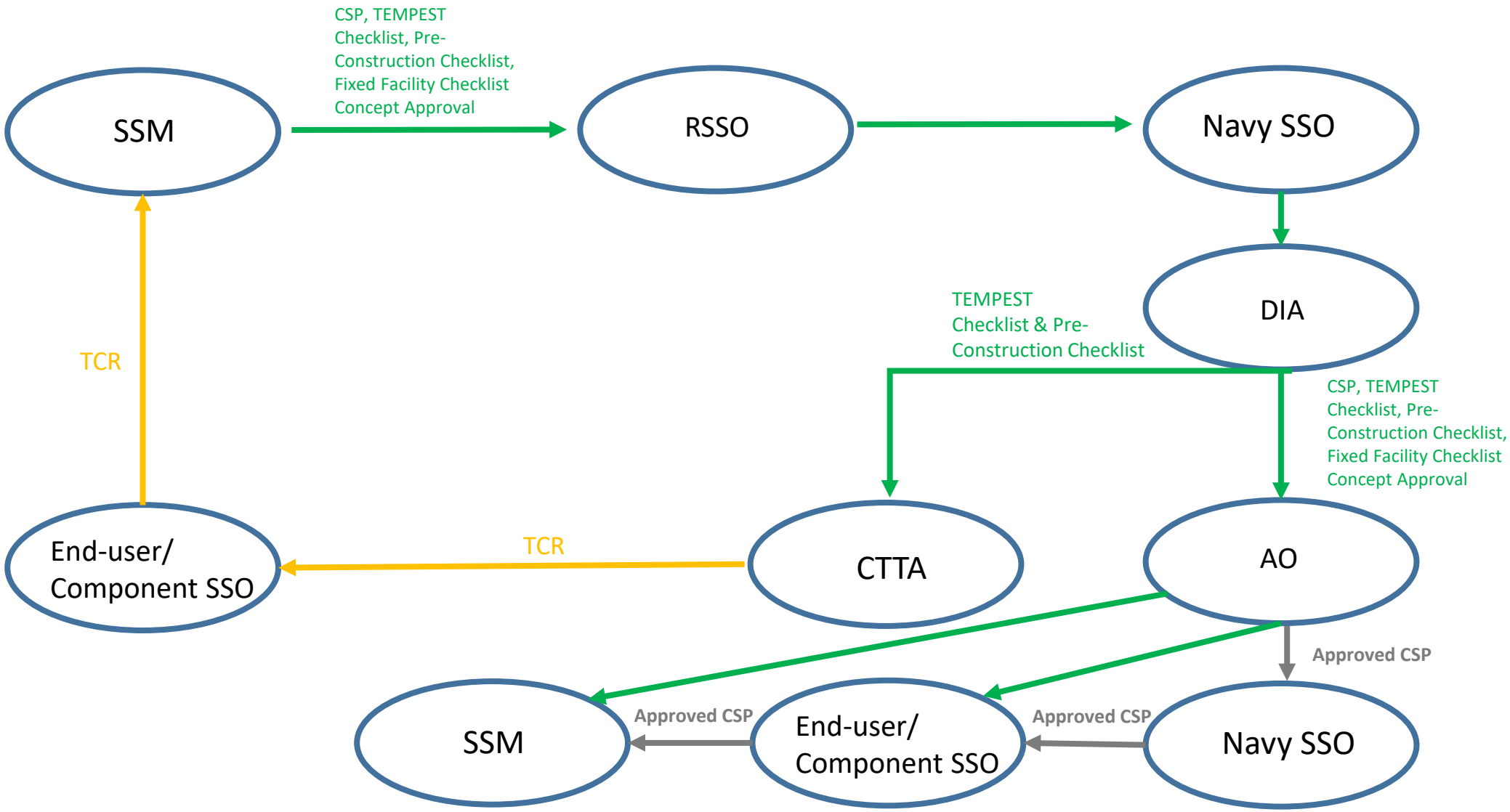
Legend

- AO – Accrediting Official (DIA)
- CA – Concept Approval
- CAR – Concept Approval Request
- CSA – Cognizant Security Authority
- CSP – Construction Security Plan
- CTTA – Certified TEMPEST Technical Authority
- DIA – Defense Intelligence Agency
- SSM – Site Security Manager
- SSO – Special Security Officer (Navy) (CSA)
- RSSO – Regional SSO (Regional CSA – RCSA)
- TCR – TEMPEST Countermeasure Review

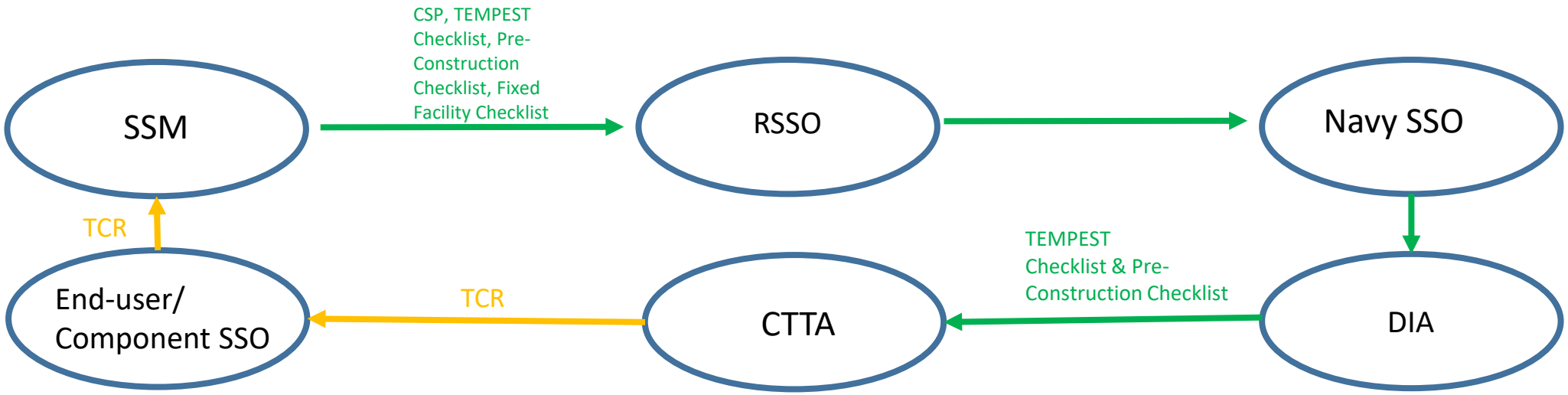
SCIF Approval Process – Concept Approval



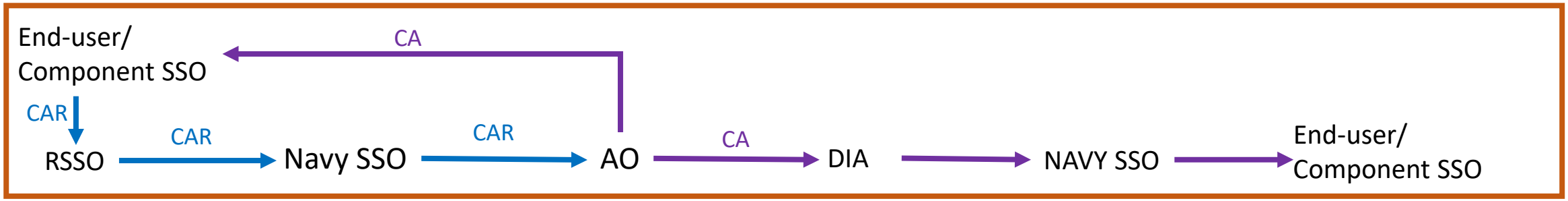
SCIF Approval Process – CSP, TEMPEST/Pre-Construction/Fixed Facility Checklists

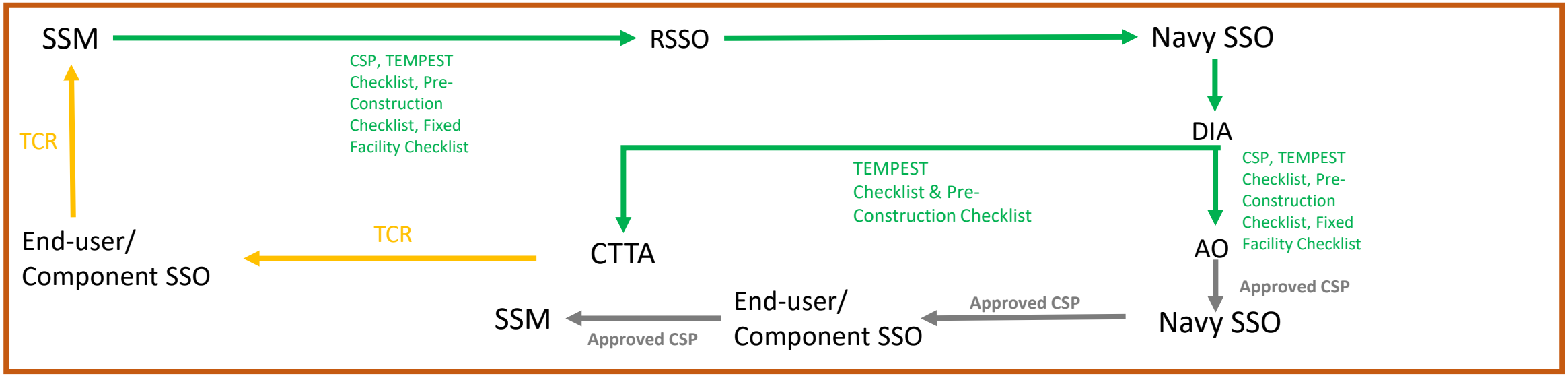


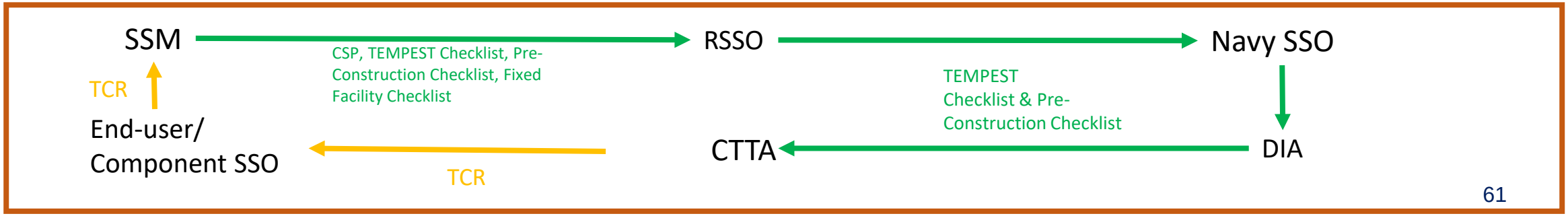
SCIF Approval Process – TCR



SCIF Approval Process







SAPF Requirement – Concept Approval

- **Per DON SAPCO Instruction 5530**
  - **SAPFs require Concept Approval**
  - **The following steps shall be taken once a new requirement for additional SAPF space is identified:**
    - **The organization with the requirement for the SAPF will submit a concept approval request (CAR) endorsed by the leadership of the requesting organization (Supported Command) via the Program Security Officer (PSO) and the Government Program Manager (GPM) and Contractor Program Manager (CPM).**
      - The CAR will include a concise statement of the mission or requirement that necessitates the establishment of a new SAPF. Include missions/functions to be supported, and work that will be performed within the SAP F. Include any co-utilization requirements (SCI, other SAP programs, etc.) Include proposed classification of the new SAPF, identify why existing SAPFs do not meet the need.
      - Identify a Site Security Manager (SSM)
    - CAR approved by DON SAPCO
      - DON SAPCO Director of Security (DoS) will send approval to PSO and GPM
      - PSO/GPM will notify SAO and CTTA

NAVFAC Naval Facilities Engineering Systems Command

SAPF ACCREDITATION

- DONSAPCO Physical Security Instruction
- Requires all grandfathered SAPFs to update to ICD705 standards within 5 years
  - 750+ SAPFs
  - Includes Fleet, Government, and Industry facilities of all sizes and purposes
- Each SAPF is required to develop a POA&M to get to compliance
- DONSAPCO has own team for TEMPEST – CTTAs that are triaging each facility and assessing risk posture
  - TEMPEST countermeasures directed by DONSAPCO
- DONSAPCO efforts are independent of SSO Navy direction (although they try to work together)
- Instruction also sets standards for new SAPFs
  - As an example, RF Foil is now mandatory on all new construction

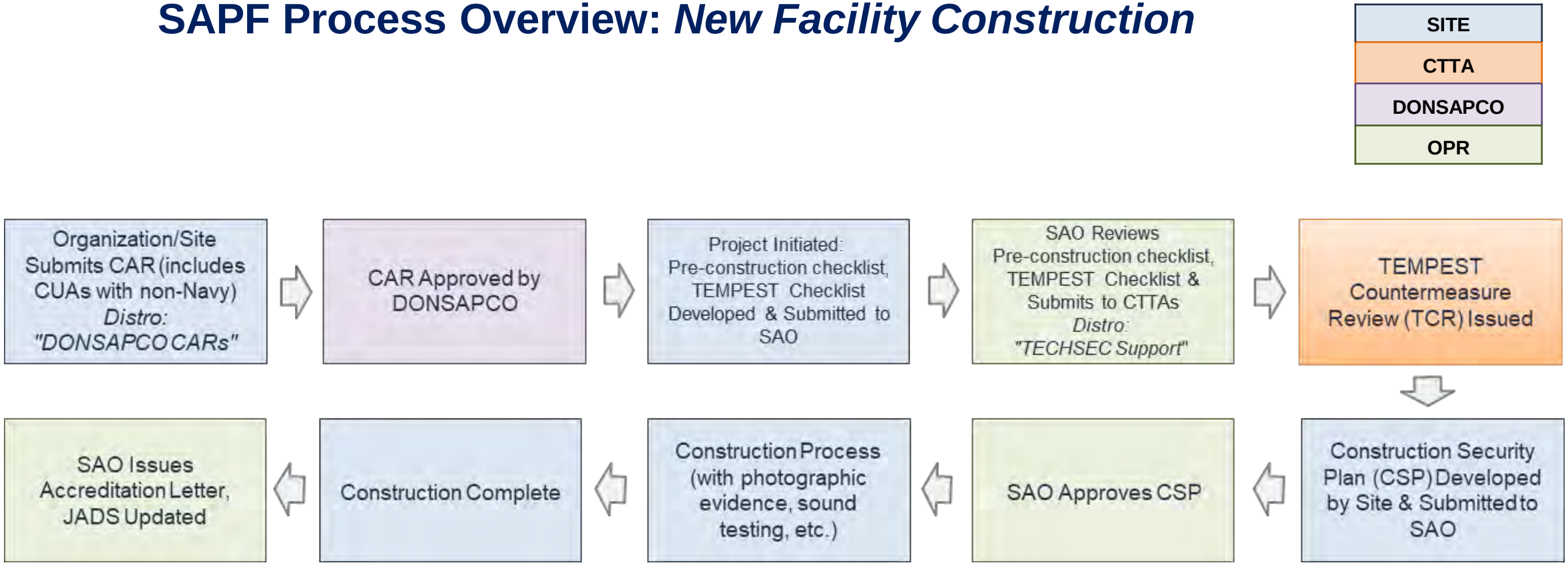
NAVFAC Naval Facilities Engineering Systems Command

SAPF ACCREDITATION

- Read the ICD 705 Technical Specifications
- Communicate **EARLY** and **OFTEN** with security teams
- Ensure that you are on the same security page before any contracts are released for solicitation
- Include the Resource Sponsor (whoever is paying the bill) **AND** the end user are involved in discussions
- The costs associated in the DD1391 should include requirements from the Concept Approval Request (if any), the Construction Security Plan (CSP), and TEMPEST Countermeasure Review (TCR)
- Make sure both SCI and SAP communities are involved if building a dual SCIF and SAPF
- Ensure that project deadlines allow SAO adequate time to review the documentation submitted – in SAP world, they have day jobs as PSOs

NAVFAC Naval Facilities Engineering Systems Command

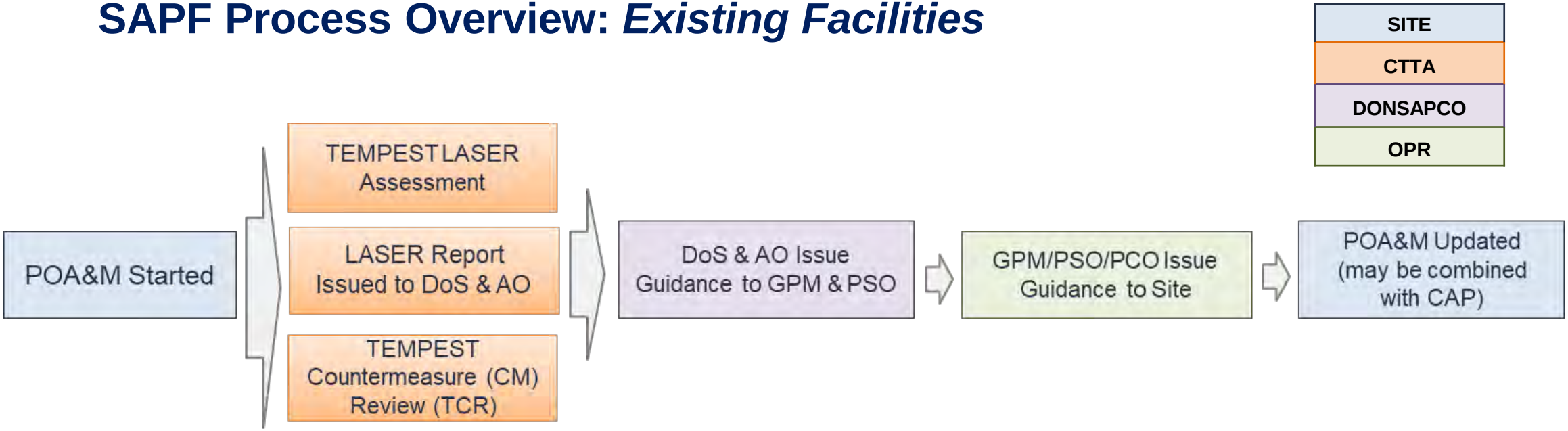
SAPF Process Overview: *New Facility Construction*



***At any point, this process can stop if requirements are not met.**

NAVFAC Naval Facilities Engineering Systems Command

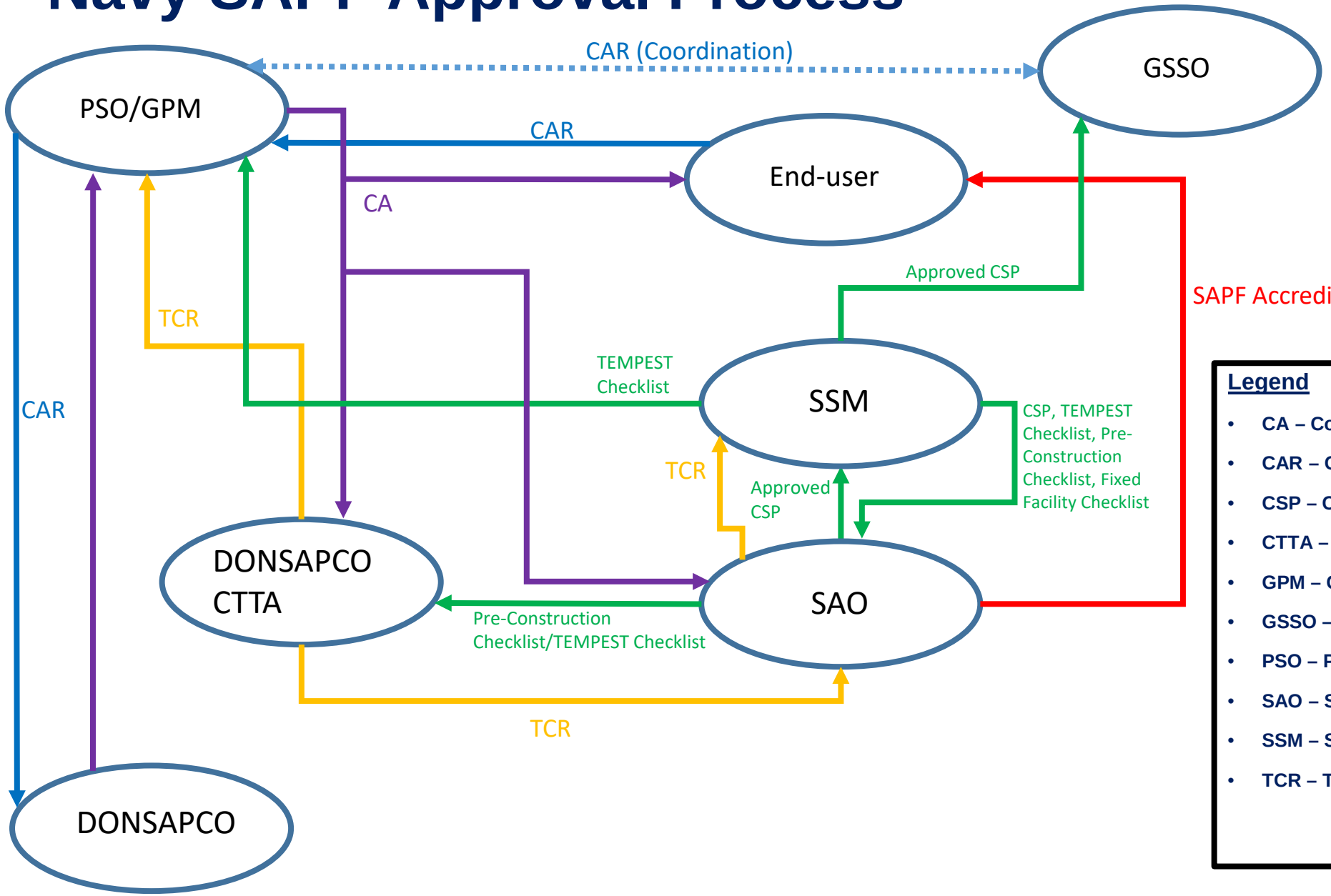
SAPF Process Overview: *Existing Facilities*



- TEMPEST Report Types:
  - TCR: defines inspectable space, sets TEMPEST CM requirements
  - LASER and/or REACT: identify and document vulnerabilities (snapshot in time)
- Facilities need to complete a thorough self-assessment of their non-ICD705 areas, and document a POA&M that identifies the issues
- Prioritized plans developed – Installation/Campus, Industry Partners, Program Offices/Commands
- Have 5 years to upgrade to ICD 705 standards - NO facility is exempt from upgrade
- POA&M can go beyond the 5 years if approved by DONSAPCO

NAVFAC Naval Facilities Engineering Systems Command

Navy SAPF Approval Process



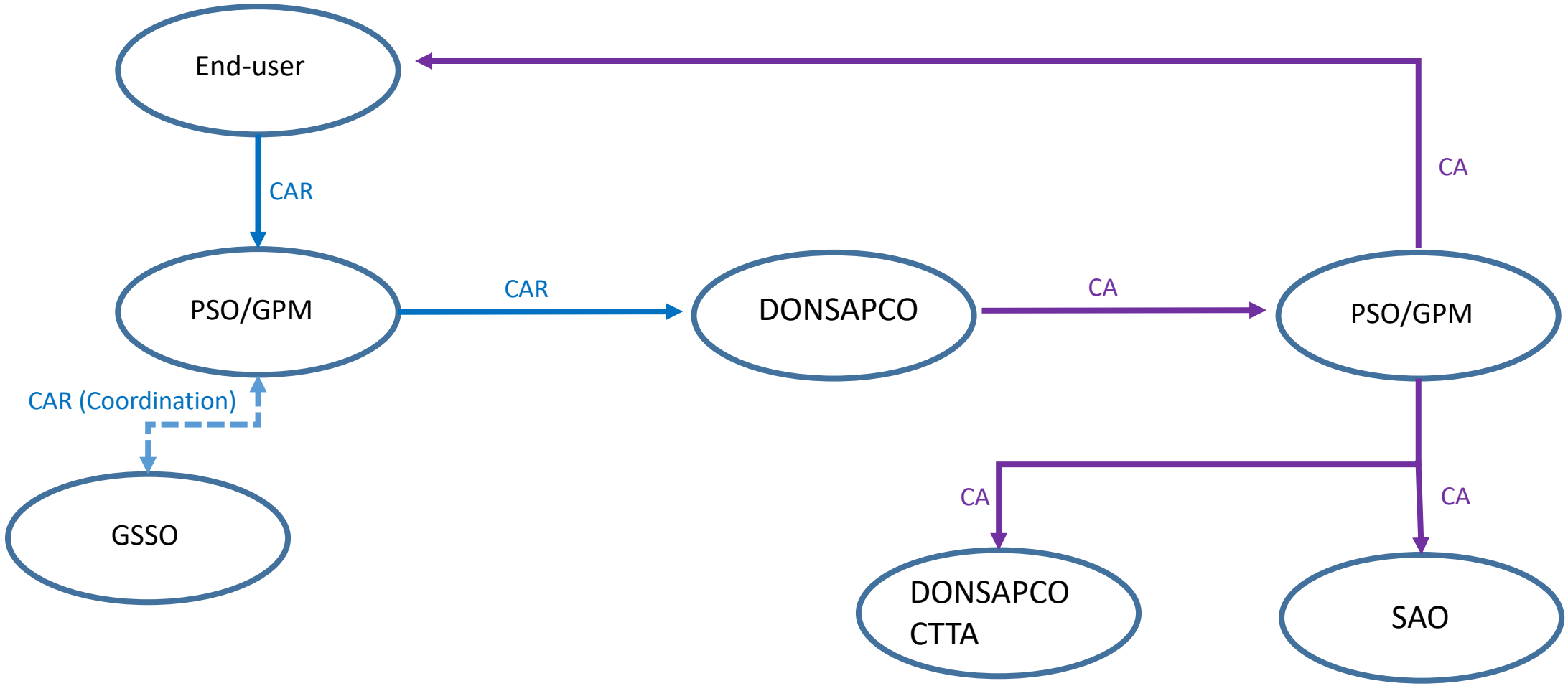
CA Issued by DONSAPCO

Legend

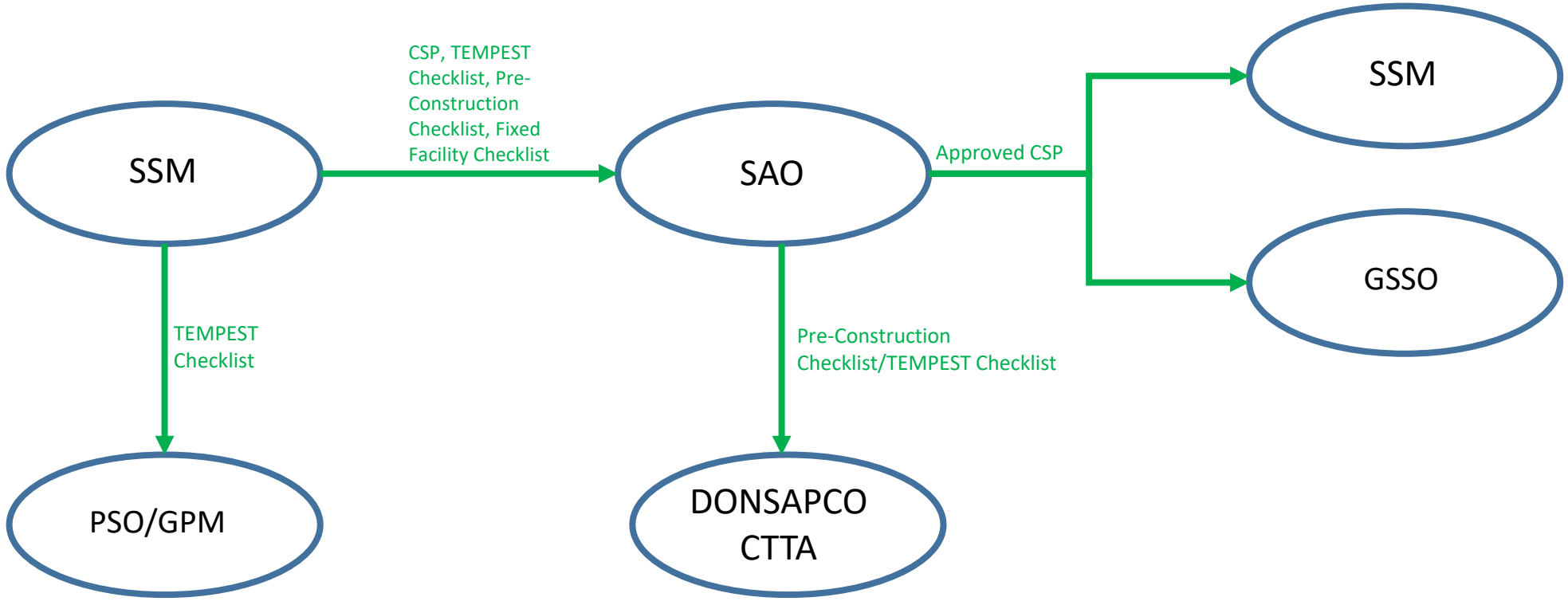
- **CA – Concept Approval**
- **CAR – Concept Approval Request**
- **CSP – Construction Security Plan**
- **CTTA – Certified TEMPEST Technical Authority**
- **GPM – Government Program Manager**
- **GSSO – Government SAP Security Officer**
- **PSO – Program Security Officer**
- **SAO – SAP Accrediting Official**
- **SSM – Site Security Manager**
- **TCR – TEMPEST Countermeasure Review**

NAVFAC Naval Facilities Engineering Systems Command

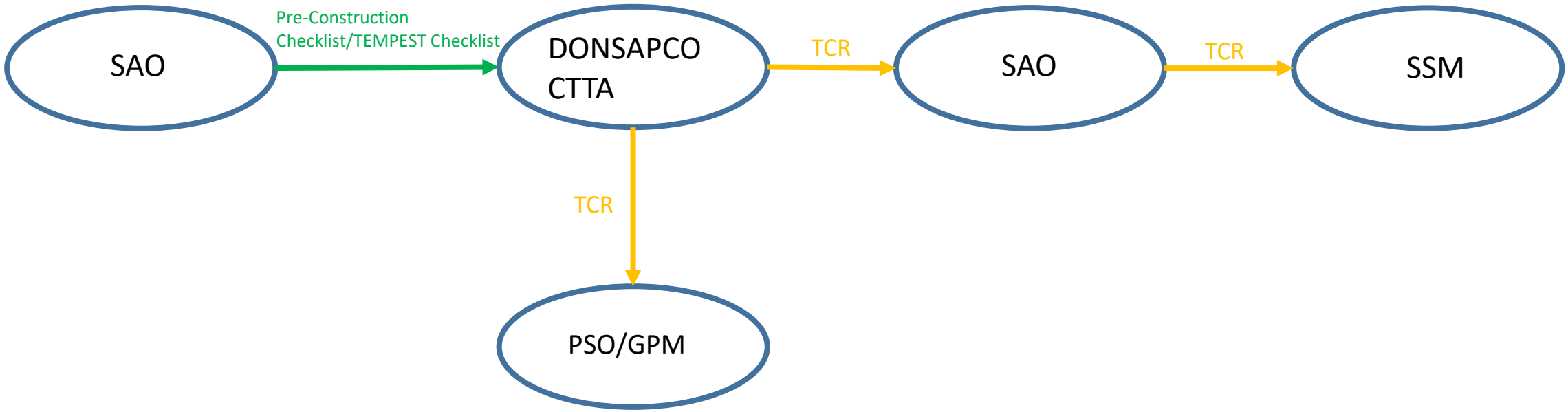
Navy SAPF Approval Process – Concept Approval



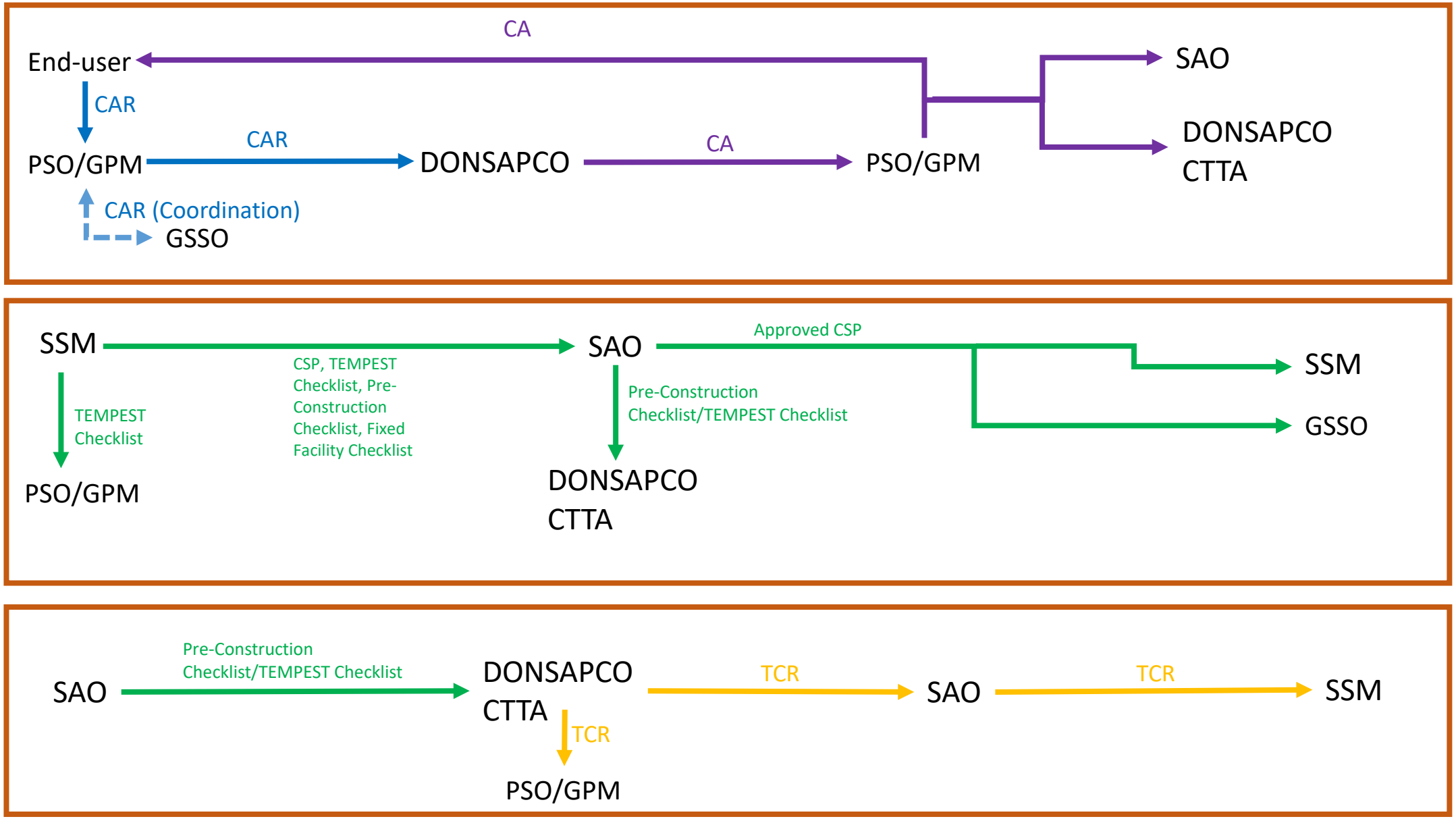
Navy SAPF Approval Process – CSP, TEMPEST/Pre-Construction/Fixed Facility Checklists



Navy SAPF Approval Process - TCR



Navy SAPF Approval Process



Design and Construction: United States

- SCIF/SAPF construction and design should 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.
- **The AO shall ensure mitigations are implemented when using non-U.S. citizens.**
- Intrusion Detection System (IDS) installation and testing shall be performed by U.S. companies using U.S. citizens with a trustworthiness determination.
- **These are documented in the CSP.**

NAVFAC Naval Facilities Engineering Systems Command

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.
  - On military facilities, the AO may authorize foreign national citizens or firms to perform general construction of SCIFs. In this situation, the SSM shall prescribe, with AO approval, mitigating strategies to counter security and counterintelligence threats.
- Applicable to the SCIF/SAPF and possibly the adjacent space.

NAVFAC Naval Facilities Engineering Systems Command

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 wall systems, trim, chair rail, molding, insulation, floor/partition/ceiling systems, painting, 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.
  - Clearance requirements based on SETL Category Level
- Applicable to finish work in the SCIF/SAPF, not other areas of the facility.

NAVFAC Naval Facilities Engineering Systems Command

Design and Construction: Outside United States

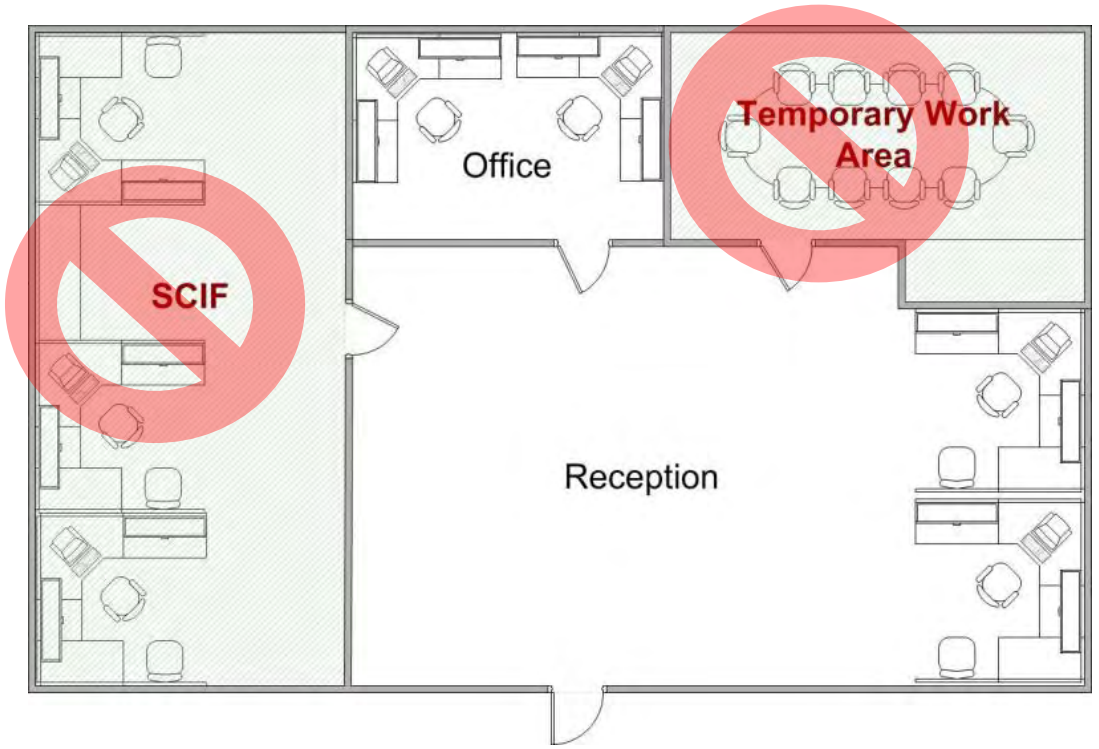
- Intrusion Detection System (IDS) installation and testing shall be performed by personnel who are U.S. TOP SECRET-cleared or U.S. SECRET-cleared and escorted by U.S. Personnel with a TS clearance.
- UFGS 01 14 00 Work Restrictions

NAVFAC Naval Facilities Engineering Systems Command

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"**



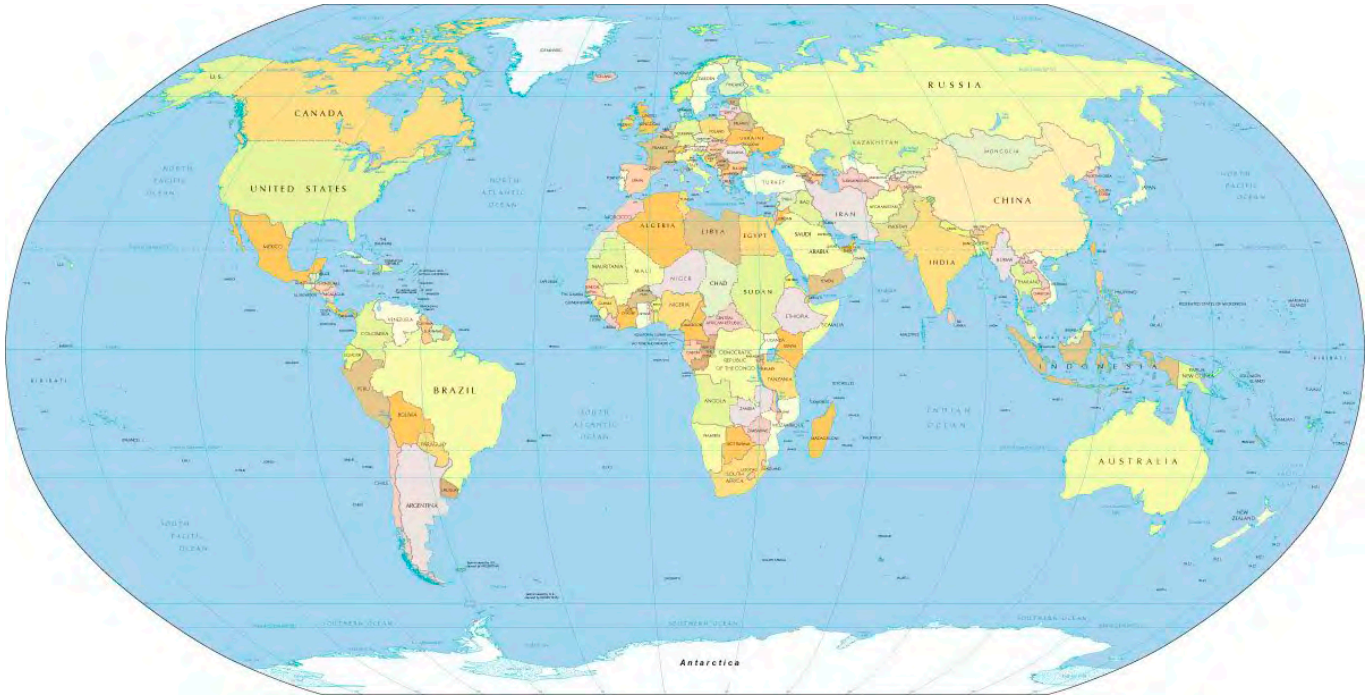
NAVFAC Naval Facilities Engineering Systems Command

Information Security

NAVFAC
Naval Facilities Engineering Systems Command

Security Requirements

- **The location (threat), its (assets/information) 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>**



NAVFAC
Naval Facilities Engineering Systems Command

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.

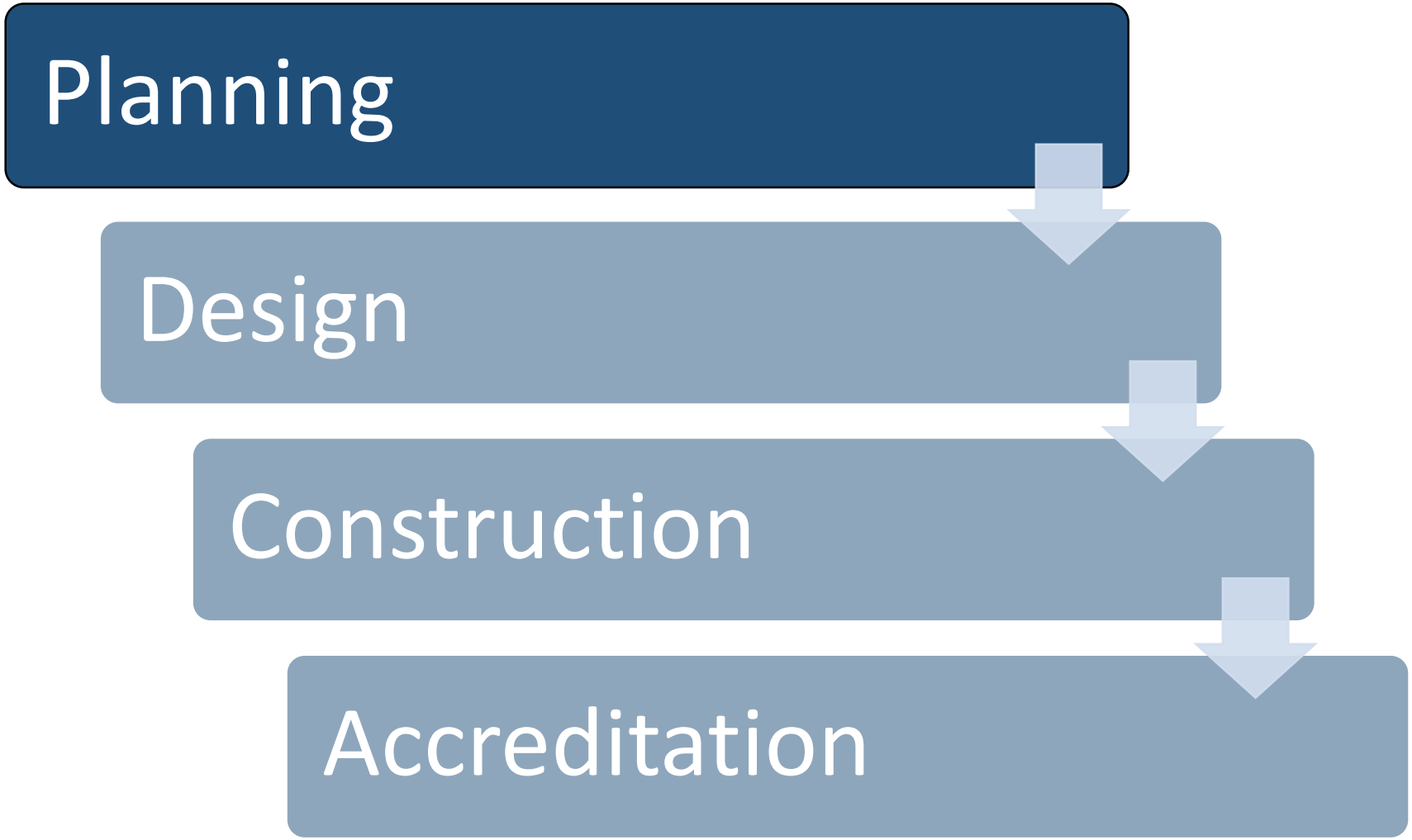
NAVFAC Naval Facilities Engineering Systems Command

Project OPSEC/SAIRC

- The OPSEC/SAIRC process provides a means of screening information prior to public release.
- Publicly released documents such as reports, studies, calculations, drawings, specifications, or Design-Build Request for Proposals (RFP) cannot reveal sensitive or critical information.
  - See NAVFACINST 3070.2, NAVFAC Operations Security (OPSEC)
  - See NAVFACINST 4200.35, Sensitive Activity and Intelligence Related Contracting Program (SAIRC) for additional guidance
- Include an OPSEC/SAIRC review per NAVFACINSTs above 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 1-300-09N 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

NAVFAC Naval Facilities Engineering Systems Command

Project Phases



NAVFAC Naval Facilities Engineering Systems Command

Planning Team

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

❖ **Some teams may require more than one SSM if the facility includes a SCIF and SAPF.**

NAVFAC Naval Facilities Engineering Systems Command

Planning Team Members

- **Supported Command**
  - Program Manager
  - Senior Intelligence Officer (SIO)
  - Program Security Officer (PSO)
  - Site Security Manager (SSM)
- **NAVFAC**
  - Facilities Planner (PL)
  - Project Manager (PM)
  - Design Manager (DM)
- **Accreditation Authority**
  - RSSO/RCSA/SSO Navy
  - Accrediting Official (AO)
  - Site Security Manager (SSM)
  - Certified TEMPEST Technical Authority (CTTA)

NAVFAC Naval Facilities Engineering Systems Command

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 **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/SAO.
    - Upon review of the preliminary CSP, the AO/SAO 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**
  - CSP is a living document and will be updated during design and finalized then approved before construction contract award

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

SCIF/SAPF Lifecycle – Planning & Design

0%

- Initial SCIF/SAPF Requirement Identified by Supported Command
- SSM Assigned
- Risk Assessment
- SSM Submits Concept Approval Request (CAR) to AO to Obtain SCIF ID
- Pre-Construction Checklist, Preliminary Construction Security Plan (CSP) & Initial TEMPEST Checklist by SSM

30%

- Funding Allocated
- Construction Security Plan (CSP) Approval by AO
- TEMPEST Countermeasure Review (TCR) by CTTA
- Design Development Submittals – Basis of Design, Plans & Outline Specs by U.S. Companies using U.S Citizens
- Design Review & OPSEC Review

60%

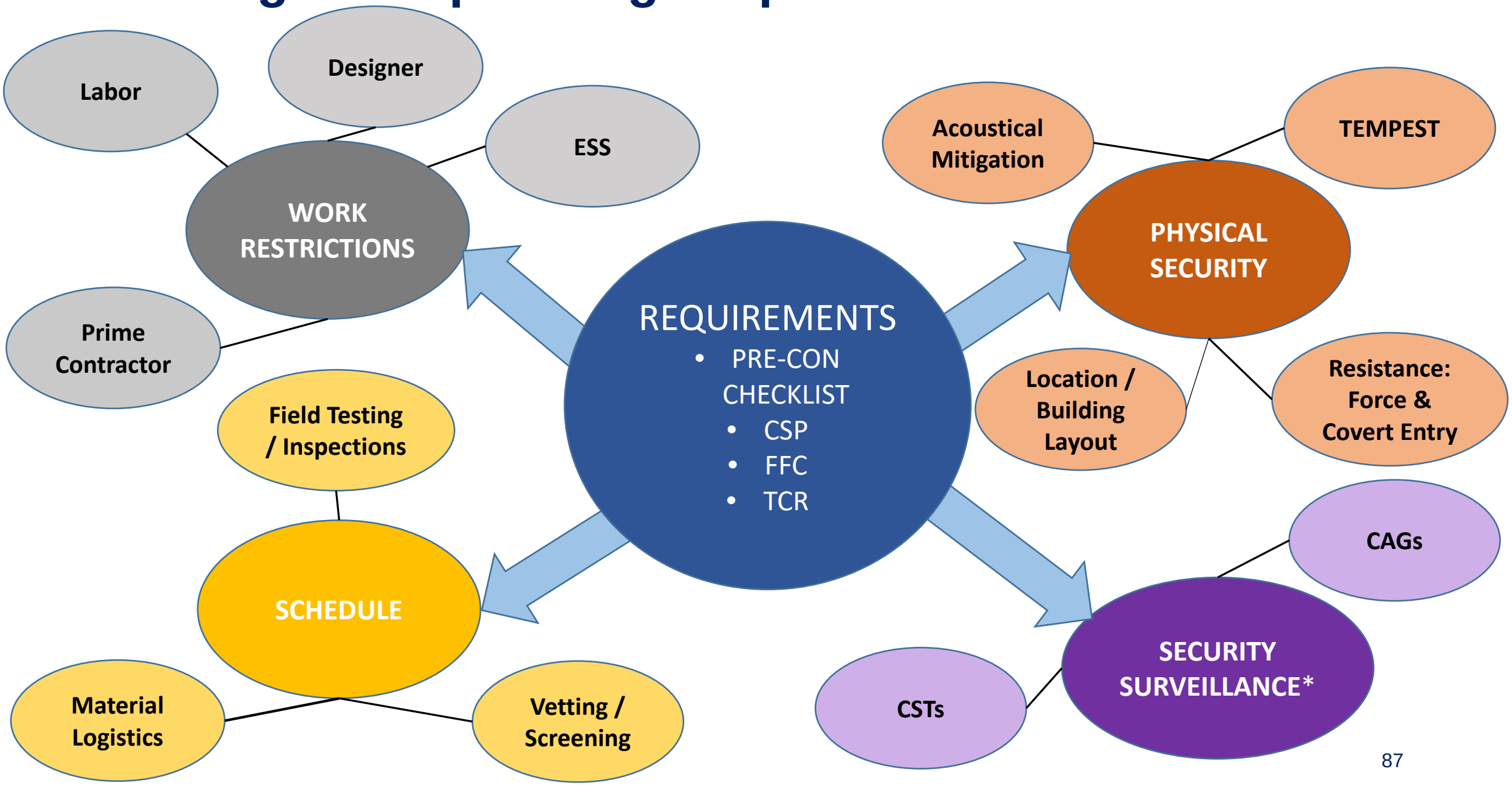
- CSP and TCR Requirements Incorporated into Design
- Prefinal Design Submittals – Basis of Design Updates, Plans, & Specifications
- Design Review & OPSEC Review
- SSM Updates CSP and Preliminary Fixed Facility Checklist (FFC) for validation by AO

100%

- Final Design Submittals Plans & Specifications
- Final Design Review & OPSEC Review
- Release to Acquisitions

NAVFAC Naval Facilities Engineering Systems Command

Planning: Incorporating Requirements in DD1391



NAVFAC INST 4700.1A - Planning

Planning, Design, and Construction Steps for DON MILCON Funded SCIF

TASK/ MILESTONE	Responsibility for Each Action L=Lead; S=Support								Notes	References
	Accrediting Official (AO)	Certified TEMPEST Technical Authority (CTTA)	Site Security Manager (SSM)	Supported Command Senior Intelligence Officer (SIO)	Facility Planner Commander, Navy Installations Command (CNIC)/U.S. Marine Corps (USMC)/ Naval Facilities Engineering Command (NAVFAC) Asset Management (AM)	Project Manager(PM) (NAVFAC/Design Agent)	Construction Manager (CM) (NAVFAC/Construction Agent)	NAVFAC Echelon 2 Headquarters Design and Construction (DC) Military Construction (MILCON)		
To be completed prior to Installation/Public Works Department (PWD) Final DD Form 1391:										
INTEL tenant defines need for Sensitive Compartmented Information Facility (SCIF) space as a part of facility requirement				L					Determined by the Supported Command coordinated with INTEL authority.	
Identify AO				L					Determined by the Supported Command SIO. Typically AO is Defense Intelligence Agency for Department of Defense (DoD) projects, National Security Agency or Special Security Office Navy for Navy Projects in U.S.	DoDM 5101.21 Vol 2, IC Tech Spec ICD/ICS 705, UFC 4-010-05

NAVFAC INST 4700.1A - Planning

Development of iNFADS Planning Action				S	L				Installation planner works with SIO to develop space requirement (Basic Facility Requirement). Facility Planning Document and planning action that acts as the scope for the eventual DD Form 1391 development.	NAVFAC SFPS Guidebook Project Readiness Index (PRI) 1 and 2 (MTP3 Process) Business Management System (BMS) (AM and DC) B-25.6.2.2, B-11.3.2 and B-25.6.1 (NOTE: Not all projects are MILCON)
Preliminary Site Planning				S	L				Installation planner assesses viable sites on installation; Installation Commander approves site selection.	NAVFAC 11010.45A BMS B-25.3.5
Request for Concept Approval Submitted				L					Completed by the supported command's SIO and sent to AO. Contents may be Classified	DoDM 5101.21 Vol 2
Concept Approval	L			S					AO issues Concept Approval message. Message is For Official Use Only	DoDM 5101.21 Vol 2
Appoint SSM				L					Typically designated by SIO, may be identified by Intelligence community or Region.	DoDM 5101.21 Vol 2
Begin Risk Management process for security requirements determination			L	S					SSM coordinates security requirements for the project.	DoDM 5101.21 Vol 2, IC Tech Spec ICD/ICS 705, UFC 4-010-05
DD Form 1391 having status level of "INSTL/ PWD FINAL" created in Electronic Project Generator (EPG) and linked to Integrated Priority List Module.			S	S	L				Typically created by the Installation PWD planner in March Budget Year (BY)3 (for Fiscal Year (FY) 2023 project: March 2020).	BMS B-25.6.2.2
To be completed prior to Program Final DD Form 1391:										
Preliminary Design Authority (PDA) issued.								L	Issued by NAVFAC Echelon 2 DC MILCON. Goal is by August BY-3 (For FY2023 Project, August 2020).	PDA Guidance ECB 2007-01
Initial Construction Security Plan (CSP) completed and submitted for approval			L	S	S				Initial CSP is completed by SSM with input from Facility Planner and submitted to the AO. Facility Planner must provide scope and budget implications associated with CSP.	DoDM 5101.21 Vol 2, IC Tech Spec ICD/ICS 705, UFC 4-010-05
Initial Fixed Facility Checklist (FFC) completed and submitted for approval			L	S	S				Initial FFC is prepared by SSM with input from Facility Planner. This may be submitted with the Initial CSP or at a later date.	DoDM 5101.21 Vol 2, IC Tech Spec ICD/ICS 705, UFC 4-010-05
Initial TEMPEST Form A submitted with initial FFC			L	S	S				Initial TEMPEST Form A is completed by the SSM in coordination with supported command. This is submitted with the Initial FFC.	DoDM 5101.21 Vol 2, IC Tech Spec ICD/ICS 705, UFC 4-010-05

NAVFAC INST 4700.1A - Planning

AO reviews Initial CSP and provides approval or acknowledgment	L		S	S					Upon review, AO will provide approval or acknowledgement message. Acknowledgement message will include guidance that must be included in the final CSP.	DoDM 5101.21 Vol 2, IC Tech Spec ICD/ICS 705, UFC 4-010-05
SCIF ID issued	L		S	S					Upon approval or acknowledgment of Initial CSP, AO will assign a SCIF ID with message.	DoDM 5101.21 Vol 2
Refine DD Form 1391 scope and budget based on Initial CSP, FFC and TEMPEST Form A, and DD Form 1391 Charrette			S	S	S	L			Project Manager with the support of the Project Technical Team (PTT) has responsibility for this action, but may be delegated to their designated design agent. PM coordinates any scope changes with AM planner.	Fiscal Law, MILCON Law, NAVFAC SFPS Guidebook BMSs 25.6.2.2, B-11.3.2 and B B-25.6.1 (NOTE: Not all projects are MILCON) PRI 2 (MTP3 Process) PDA Guidance, CRB Guidelines
Develop Budget Estimate for Electronic Security System (ESS). Provide separate estimate for: - Baseline (funded via NAVFAC Antiterrorism/ Force Protection (ATFP) Ashore) - Baseline/Enhancements (funded via Supported Command/User/Client)			S	S	S	L			PM with the support of the PTT has responsibility for this action, but may be delegated to their designated design agent.	OPNAVINST 11010.20, BMS B-1.3
Notify ATFP Ashore and supported command of ESS justification, scope, and funding requirements.			S	S	S	L			PM has responsibility for this action. Important to separate ATFP Ashore baseline scope and funding requirements from Supported Command/User/Client baseline scope or enhancements and funding requirements.	BMS B-1.3
DD Form 1391 having status level of "REGN/FEC_TEAM_FINAL" created in EPG with SCIF scope and cost incorporated.			S	S	S	L			Typically led by NAVFAC Echelon 4 Facilities Engineering Command (FEC) PM. Goal is by February BY-2 (For FY2023 Project, February 2021).	Fiscal Law, MILCON Law, NAVFAC SFPS Guidebook, OPNAVINST 11010.20H, BMSs 25.6.2.2, B-11.3.2 and B B-25.6.1 (NOTE: Not all projects are MILCON) PRI 2 (MTP3 Process) PDA Guidance, CRB Guidelines
Consistency Review Board (CRB).					S	S		L	Led by Echelon 2 DC MILCON Program Manager. Goal is by March BY-2 (For FY2023 Project, March 2021).	PDA Guidance, CRB Guidelines
DD Form 1391 having status level of "PROGRAM_FINAL" created in EPG with SCIF scope and costs incorporated.			S			L		S	Typically led by NAVFAC Echelon 4 FEC PM. Goal is by March BY-2 (For FY2023 Project, March 2021).	PDA Guidance, CRB Guidelines

NAVFAC INST 4700.1B (DRAFT) - Planning

Planning, Design, and Construction Steps for DON Funded SCIF/SAPF

TASK/ MILESTONE	Responsibility for Each Action L=Lead; S=Support									Notes	References
	Accrediting Official (AO (SCIF)/SAO (SAPF))	CSA/SSO/DON SAPCO Navy	Certified TEMPEST Technical Authority (CTTA)	Site Security Manager (SSM)	Supported Command Senior Intelligence Officer (SIO)	Facility Planner Commander, Navy Installations Command (CNIC)/U.S. Marine Corps (USMC)/ Naval Facilities Engineering Systems Command (NAVFAC) Strategic Planning (PDC3)	Project Manager(PM) (NAVFAC/Design Agent)	Construction Manager (CM) (NAVFAC/Construction Agent)	NAVFAC Echelon 2 Headquarters Planning, Design and Construction (PDC) Military Construction		
To be completed prior to Installation/Public Works Department (PWD) Final DD Form 1391:											
INTEL tenant defines need for Sensitive Compartmented Information Facility (SCIF)/Special Access Program Facility (SAPF) space as a part of facility requirement					L					Determined by the Supported Command coordinated with INTEL authority.	
Identify AO (SCIF)/SAO (SAPF)					L					Determined by the Supported Command SIO. Typically, AO (SCIF)/SAO (SAPF) is Defense Intelligence Agency for Department of Defense (DoD) projects, or the National Security Agency for SCIFs and DON SAPCO for SAPFs.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05 DON SAPCO Instruction 5530

DRAFT

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1B (DRAFT) - Planning

Development of iNFADS Planning Action					S	L				Installation planner works with SIO to develop space requirement (Basic Facility Requirement), Facility Planning Document and planning action that acts as the scope for the eventual DD Form 1391 development.	NAVFAC SFPS Guidebook Project Readiness Index (PRI) 1 and 2 (MTP3 Process) Business Management System (BMS) (PDC) B-25.6.2.2, PDC-02-01.01, and PDC-04-04.01 (NOTE: Not all projects are MILCON)
Preliminary Site Planning					S	L				Installation planner assesses viable sites on installation; Installation Commander approves site selection.	NAVFAC 11010.45A PDC-03.11
Request for Concept Approval Submitted					L					Completed by the supported command's SIO and sent to CSA/SSO Navy (SCIF)/DON SAPCO (SAPF). Contents may be Classified	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3
Concept Approval		L			S					CSA issues Concept Approval message. Message is Controlled Unclassified Information (CUI).	DoDM 5101.21 Vol 2 DoDM 5205-07 Vol 3
Appoint SSM					L					Typically designated by SIO, may be identified by Intelligence community or Region.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3
Begin Risk Management process for security requirements determination		S		L	S					SSM coordinates security requirements for the project.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
DD Form 1391 having status level of "INSTL/ PWD FINAL" created in Electronic Project Generator (EPG) and linked to Integrated Priority List Module.				S	S	L				Typically created by the Installation PWD planner in March Budget Year (BY) 3 (for Fiscal Year (FY) 2025 project: March 2022).	BMS B-25.6.2.2
To be completed prior to Program Final DD Form 1391:											
Preliminary Design Authority (PDA) issued.									L	Issued by NAVFAC Echelon 2 PDC MILCON. Goal is by August BY-3 (For FY2025 Project, August 2022).	PDA Guidance NAVFACINST 7045.1
Initial Construction Security Plan (CSP) completed and submitted for approval		S		L	S	S				Initial CSP is completed by SSM with input from Facility Planner and submitted to the AO/SAO via SSO Navy/DON SAPCO. Facility Planner must provide scope and budget implications associated with CSP.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Initial Fixed Facility Checklist (FFC) completed and submitted for approval				L	S	S				Initial FFC is prepared by SSM with input from Facility Planner. This may be submitted with the Initial CSP or at a later date.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 70 UFC 4-010-05
Initial TEMPEST Form A submitted with initial FFC				L	S	S				Initial TEMPEST Form A is completed by the SSM in coordination with supported command. This is submitted with the Initial FFC.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05

DRAFT

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1B (DRAFT) - Planning

											NAVFAC ltr 11000 CHENG/056
AO (SCIF)/SAO (SAPF) reviews Initial CSP and provides approval or acknowledgment	L	S	S	S	S					Upon review, AO (SCIF)/SAO (SAPF) will provide approval or acknowledgement message. Acknowledgement message will include guidance that must be included in the final CSP.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
SCIF/SAPF ID issued	L	S		S	S					Upon approval or acknowledgment of Initial CSP, AO (SCIF)/SAO (SAPF) will assign a SCIF/SAPF ID with message.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3
Refine DD Form 1391 scope and budget based on Initial CSP, FFC and TEMPEST Form A, and DD Form 1391 Charrette				S	S	S	L			Project Manager, with the support of the Project Technical Team (PTT), has responsibility for this action, but may be delegated to their designated design agent. PM coordinates any scope changes with PDC3 planner.	Fiscal Law MILCON Law NAVFAC SFPS Guidebook BMS B-25.6.2.2, PDC-02-01.01 and PDC-04-04.01 (NOTE: Not all projects are MILCON PRI 2 (MTP3 Process) PDA Guidance CRB Guidelines
Develop Budget Estimate for Electronic Security System (ESS). Provide separate estimate for: - Baseline (funded via CNIC N6S – Public Safety Systems and NEPPO/Electronic Security Systems Branch) - Baseline/Enhancements (funded via Supported Command/User/Client)				S	S	S	L			PM with the support of the PTT has responsibility for this action, but may be delegated to their designated design agent.	OPNAVINST 11010.20 PDC-04-02.09
Notify CNIC N6S/NEPPO/ESS and supported command of ESS justification, scope, and funding requirements.				S	S	S	L			PM has responsibility for this action. Important to separate ATFP Ashore baseline scope and funding requirements from Supported Command/User/Client baseline scope or enhancements and funding requirements.	PDC-04-02.09
DD Form 1391 having status level of "REGN/FEC_TEAM_FINAL" created in EPG with SCIF scope and cost incorporated.				S	S	S	L			Typically led by NAVFAC Echelon 4 Facilities Engineering Command (FEC) PM. Goal is by February BY-2 (For FY2025 Project, February 2023).	Fiscal Law MILCON Law NAVFAC SFPS Guidebook OPNAVINST 11010.20J BMS B-25.6.2.2, PDC-02-01.01 and PDC-04-04.01 (NOTE: Not all projects are MILCON) PRI 2 (MTP3 Process)
											PDA Guidance, CRB Guidelines
Consistency Review Board (CRB).						S	S		L	Led by Echelon 2 PDC MILCON Program Manager. Goal is by March BY-2 (For FY2025 Project, March 2023).	PDA Guidance CRB Guidelines
DD Form 1391 having status level of "PROGRAM_FINAL" created in EPG with SCIF scope and costs incorporated.				S			L		S	Typically led by NAVFAC Echelon 4 FEC PM. Goal is by March BY-2 (For FY2025 Project, March 2023).	PDA Guidance CRB Guidelines

DRAFT

NAVFAC Naval Facilities Engineering Systems Command

Determining Project Requirements

- The classification, operation, security requirements, TEMPEST countermeasures, and resulting facility related requirements must be scoped, documented, and budgeted **during the planning process.**
- Concept Approval Request, Preliminary CSP, FFC and TEMPEST Addendum/Checklist are prepared by the SSM and submitted during the planning phase.
  - These documents define the baseline requirements for the project.
  - For Navy and Marine Corps projects, refer to NAVFACINST 4700.01 for additional information.

NAVFAC Naval Facilities Engineering Systems Command

Determining Project Requirements

- Planner must work closely with the supported command, RSSO/RCSA/SSO Navy and the AO's/SAO's representative (SSM) to determine the requirements.
- The SSM, RSSO/RCSA/SSO Navy, AO/SAO 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.

NAVFAC Naval Facilities Engineering Systems Command

Determining Project Requirements

- To determine project requirements the supported command, RSSO/RCSA/SSO Navy, AO/SAO/SSM/CTTA will consider factors such as:
  - Asset/Information Classification
  - Location
  - Threat
  - Vulnerabilities
  - Security in Depth
  - Type and amount of classified information being processed
  - TEMPEST Review
  - Risk
  - **Cost****

** **Design and Construction Agent needs to make sure the RSSO/RCSA/SSO Navy/AO/SAO/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/Checklist.
  - The SSM will send the preliminary versions to the AO/SAO (via SSO Navy for SCIF and DONSAPCO for SAPF) for review.
- Upon review of the preliminary CSP, the AO/SAO will issue an approval or acknowledgment message along with the SCIF/SAPF Identification Number (SCIF/SAPF ID).
  - An approval is considered the AO's/SAO'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.

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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?
    - ESS requirements are driven by policy/instructions/directives
    - **As such ESS is required for SCIF/SAPF per policy**

NAVFAC Naval Facilities Engineering Systems Command

Planning Security Requirements

(Continued)

- In addition to non-classified Internet Protocol Router Network (NIPRNet) and voice services, what networks such as Secret Internet Protocol Router Network (SIPRNet) or Joint Worldwide Intelligence Communications System (JWICS) that will be processing National Security Information (NSI) be required?
  - Multiple networks will require equipment rooms in lieu of standard telecommunication rooms.
  - Has area been allotted for multiple equipment racks with future expansion, RED/BLACK separation, and computer room air conditioning (CRAC) units within the telecommunication spaces?
    - The smallest high-powered CRACs require a minimum 10 ft. x 3 ft. (3m×1m) footprint for equipment and clearances. • Will operations require redundant utilities such as utility power or telecommunications system connectivity?
- Will operations require standby generator and UPS for continuity of operations?
- Will operations require some level of resiliency such as N+1 chillers, CRACs or standby generators?

NAVFAC Naval Facilities Engineering Systems Command

Planning Security Requirements

(Continued)

- Has the supported command provided the CTTA with a completed TEMPEST Addendum for the TCR?
  - o If so, what will be the required TEMPEST countermeasures? RED/BLACK separation, shielding, or filters? • 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 U.S. persons be required for construction?

NAVFAC Naval Facilities Engineering Systems Command

Planning Security Requirements

(Continued)

- For projects 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.**

NAVFAC Naval Facilities Engineering Systems Command

Planning Security Requirements

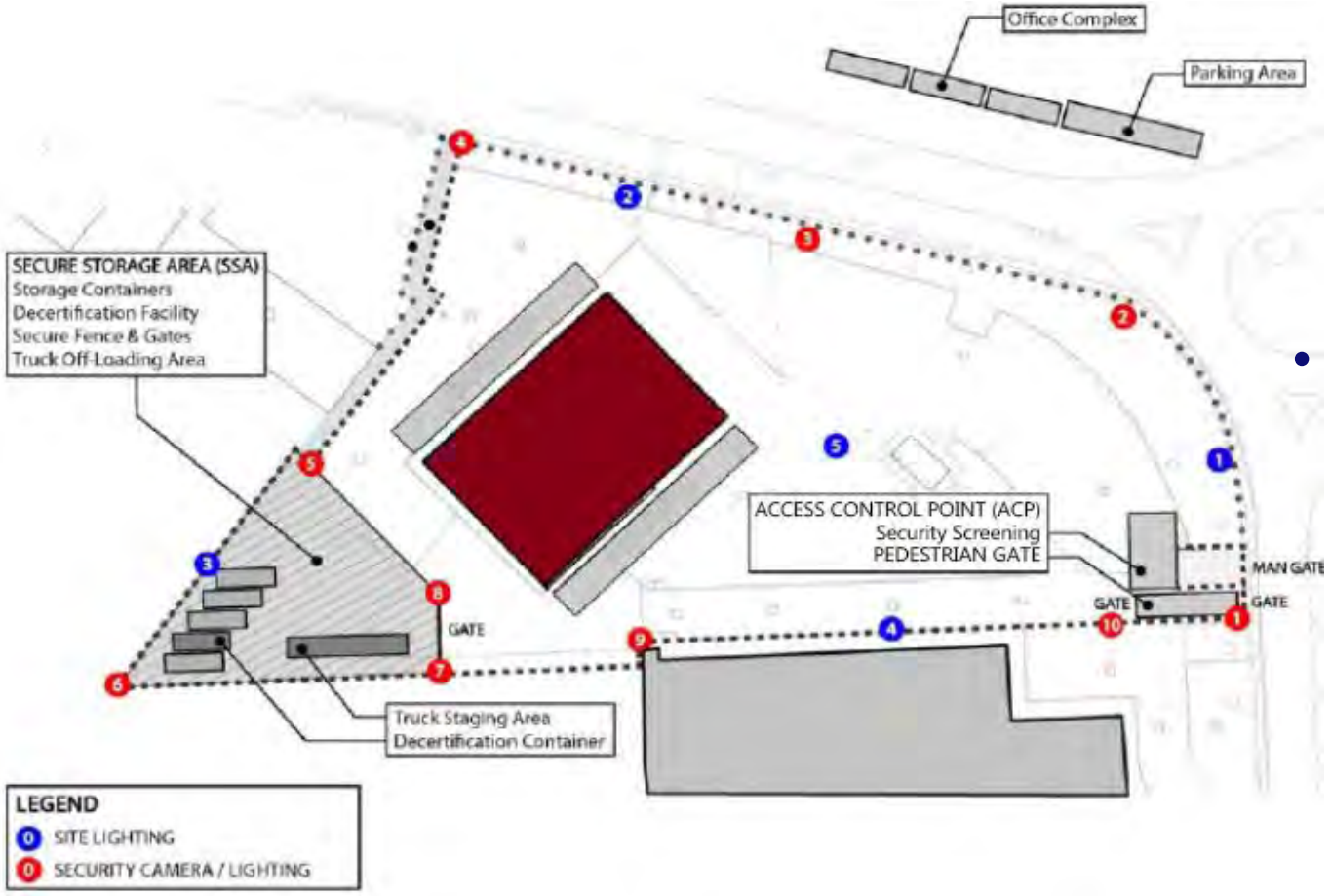
- AO/SAO will impose procedures for the procurement, shipping, and storing of construction materials at the site.
- In addition, the AO/SAO may require access control to the construction materials and the construction area, i.e. storage and inspection areas. Since these additional security measures may 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).

NAVFAC Naval Facilities Engineering Systems Command

Planning Security Requirements

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



Consider:

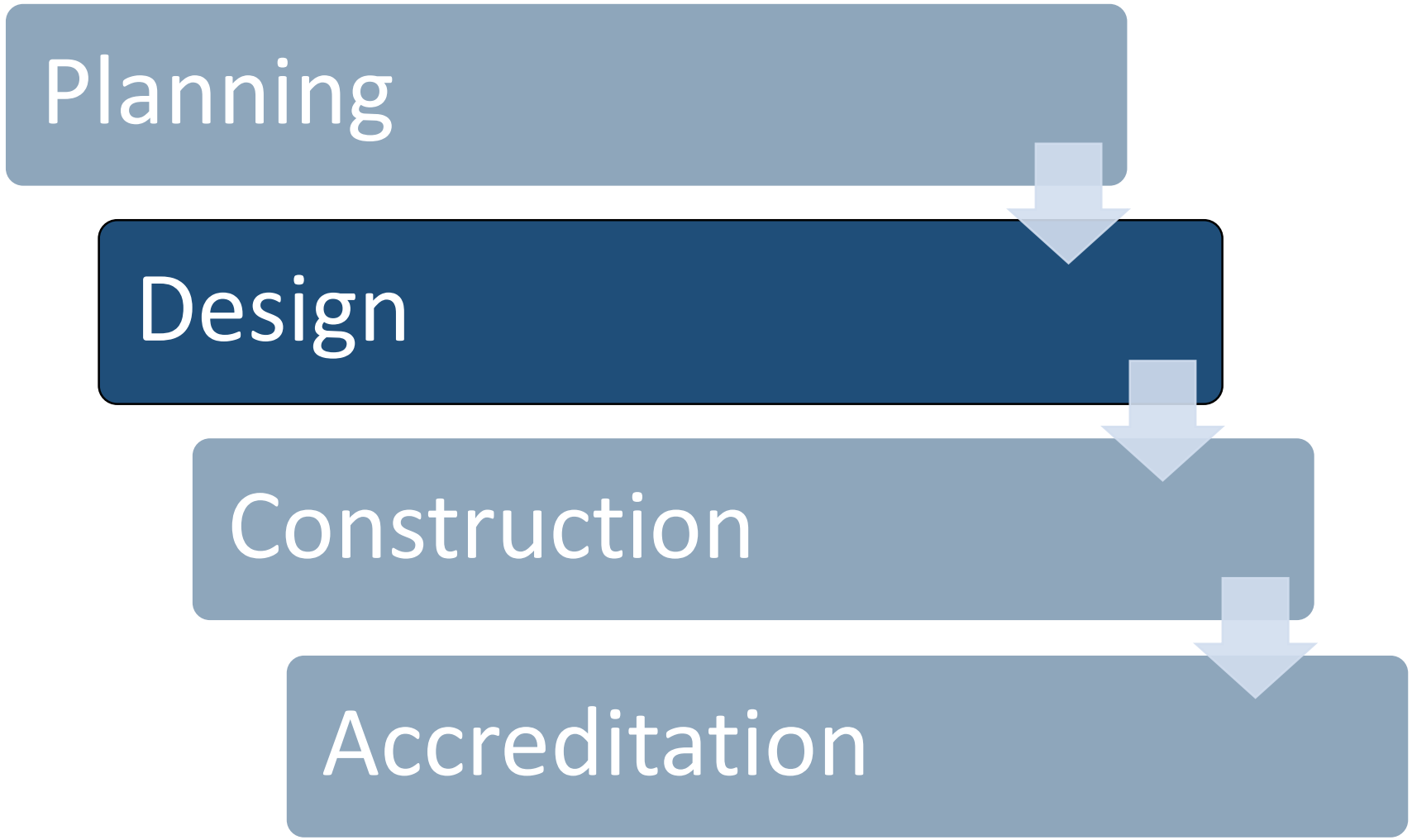
- Secure perimeter
- Access Control and Security Screening
  - Vehicle
  - Personnel
  - Material Shipment
- Material Storage
  - Size
  - Access Control

NAVFAC Naval Facilities Engineering Systems Command

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 NAVFACINSTs 4700.1, 7045.01 and CRB Guidelines.

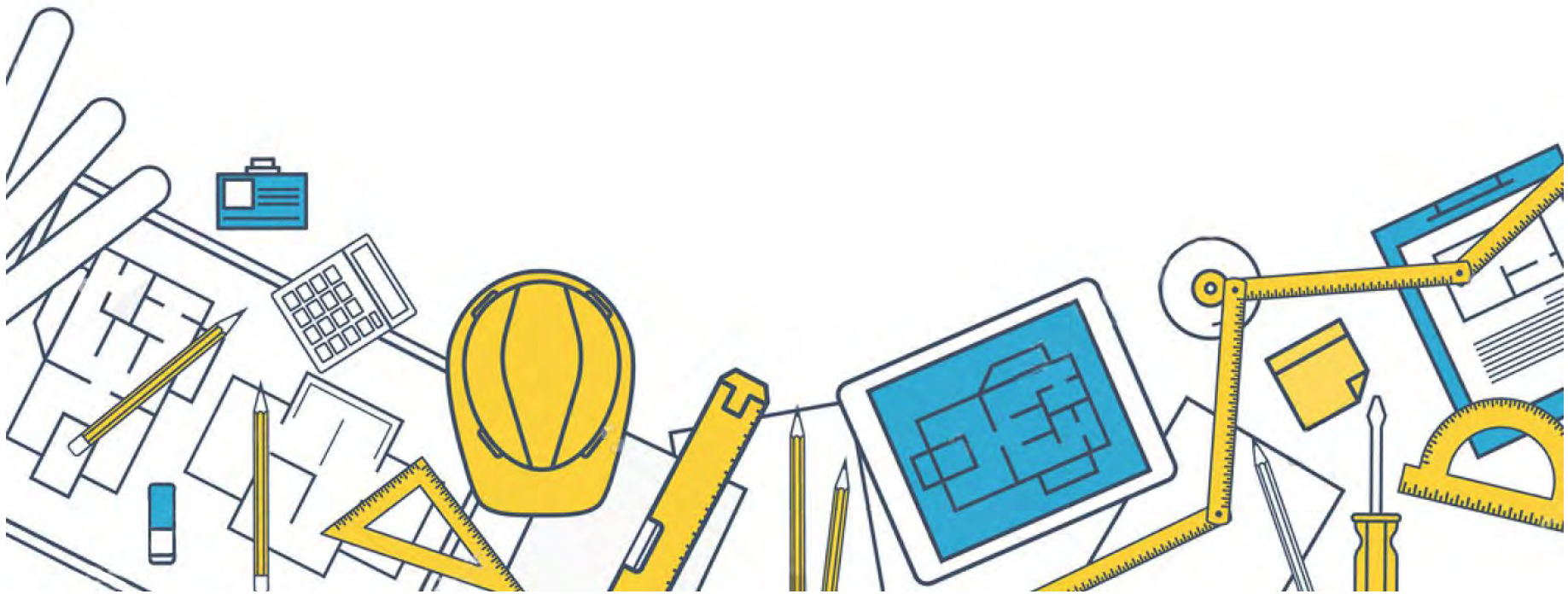
Project Phases



NAVFAC Naval Facilities Engineering Systems Command

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



NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1A - Design

To be completed prior to: Design Development (35-50%) Stage for Design Bid Build (DBB)- Request for Proposals (RFP) solicitation for Design Build (DB)										
Final Design Authority Issued								L	Issued by echelon 2 DC MILCON. Goal is by May BY-2 (For FY2023 Project, May 2021).	ECB 2007-01
Confirm SCIF ID and Initial CSP Approval/ Acknowledgment			S	S		L			PM must confirm SCIF ID has been issued and noted in CSP and that CSP has been approved or acknowledged prior to proceeding with design.	
Validate CSP requirements for Construction Personnel including General Construction, finish work, and outfitting (including Furniture, Fixtures, and Equipment (FF&E) and ESS).			S	L		S			SSM is Lead with PM/Construction Agent providing design, cost and schedule implications.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Validate CSP requirements for material purchasing, inspection, shipping, and secure storage area (SSA) including FF&E and ESS.			L			S			SSM is Lead with PM/Construction Agent providing design, cost and schedule implications.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Validate CSP requirements for site security including area/site access control for personnel, materials, and vehicles.			L			S			SSM is Lead with PM/Construction Agent providing design, cost and schedule implications.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Complete and submit updated CSP.	S		L			S			Updated by SSM and sent to AO for approval.	IC Tech Spec ICD/ICS 705, DoDM 5105.21-Vol 2
Complete and submit updated FFC	S		L			S			Updated by SSM and sent to AO for approval.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Complete and submit TEMPEST Form A	S	S	L			S			Updated by SSM and sent to AO with FFC for approval.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Review updated CSP, FFC, and TEMPEST Form A	L	S	S						AO reviews	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1A - Design

CSP, FFC, and TEMPEST Form A Approval/ Acknowledgment Message	L	S	S						AO sends an approval or acknowledgment message. Acknowledgment message will include AO recommendations for CSP approval.	DoDM 5101.21 Vol 2
TEMPEST Countermeasure Review (TCR) Message	L	S	S						AO issues TCR Message including CTTA recommendation.	DoDM 5105.21-Vol 2
Integrate updated security requirements into DB RFP or DBB design documents			S			L			PTT interprets space planning and room adjacencies with user and SSM and integrates information from the CSP, TCR, and facility requirements into the contract documents. A copy of the CSP that has been redacted to remove any classified information or contents relating to internal government processes or procedures may be included for reference.	DoDM 5105.21-Vol 2 UFC 4-010-05
DBB ONLY: Design Development (35-50%) is complete.						L			Designer of Record has developed the Basis of Design, preliminary drawings, outline specifications, and calculations. This is intended to convey the complete extent of the work in a preliminary manner.	FC 1-300-09N
To be completed prior to Pre-Final Design completion which is: - prior to Construction Contract Award for DBB - after Construction Contract Award for DB										
Confirm CSP requirements for material purchasing, inspection, shipping, and SSA requirements including FF&E.			L			S			CSP is updated by SSM	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Confirm CSP requirements for site security including area/site access control for personnel, materials, and vehicles.			L			S			CSP is updated by SSM	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
CSP is monitored and adjusted to fit design and acquisition plan			L			S			SSM updates the CSP updates coordinated with PM, Design Manager and the Designer of Record.	Fiscal Law, MILCON Law, OPNAVINST 11010.20H.IC Tech Spec ICD/ICS 705, UFC 4-010-05
Submit Final CSP	S		L			S			Final CSP is completed and submitted to the AO for approval.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705
Pre-Final Design Submittal			S			L			Designer of Record provides a complete set of design deliverables to include Basis of Design, Drawings, Specifications, Calculations and preliminary FF&E Plan.	FC 1-300-09N
To be completed prior to: - Construction Contract Award for DBB - Start of onsite construction actives for DB										
Final CSP Approval	L		S			S	S		AO issues approval message for Final CSP. This is considered the AO Final Design Approval.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 ICS 705-1, UFC 4-010-05

NAVFAC INST 4700.1B (DRAFT) - Design

To be completed prior to: Design Development (35-50%) Stage for Design Bid Build (DBB)- Request for Proposals (RFP) solicitation for Design Build (DB)											
Final Design Authority Issued									L	Issued by echelon 2 PDC MILCON. Goal is by May BY-2 (For FY2025 Project, May 2023).	NAVFACINST 7045.1
Confirm SCIF/SAPF ID and Initial CSP Approval/ Acknowledgment				S	S		L			PM must confirm SCIF/SAPF ID has been issued and noted in CSP and that CSP has been approved or acknowledged prior to proceeding with design.	
Validate CSP requirements for Construction Personnel including General Construction, finish work, and outfitting (including Furniture, Fixtures, and Equipment (FF&E) and ESS).				L			S	S		SSM is Lead with PM/Construction Agent providing design, cost and schedule implications.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
Validate CSP requirements for material purchasing, inspection, shipping, and secure storage area (SSA) including FF&E and ESS.				L			S	S		SSM is Lead with PM/Construction Agent providing design, cost and schedule implications.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
Validate CSP requirements for site security including area/site access control for personnel, materials, and vehicles.				L			S	S		SSM is Lead with PM/Construction Agent providing design, cost and schedule implications.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705

DRAFT

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1B (DRAFT) - Design

Complete and submit Final CSP.	S	S		L			S			Completed by SSM and sent to AO (SCIF)/SAO (SAPF) for approval via SSO Navy/DON SAPCO.	IC Tech Spec ICD/ICS 705 DoDM 5105.21-Vol 2 DoDM 5205.07 Vol 3
Complete and submit updated FFC	S	S		L			S			Updated by SSM and sent to AO (SCIF)/SAO (SAPF) for approval via SSO Navy/DON SAPCO.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
Complete and submit TEMPEST Form A	S	S	S	L			S			Updated by SSM and sent to AO (SCIF)/SAO (SAPF) with FFC for approval via SSO Navy/DON SAPCO	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
Review updated CSP, FFC, and TEMPEST Form A	L	S	S	S						AO (SCIF)/SAO (SAPF) reviews	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
CSP, FFC, and TEMPEST Form A Approval/ Acknowledgment Message	L	S	S	S						AO (SCIF)/SAO (SAPF) sends an approval or acknowledgment message. Acknowledgment message will include AO recommendations for approval.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3
TEMPEST Countermeasure Review (TCR) Message	L	S	S	S						AO (SCIF)/SAO (SAPF) issues TCR Message including CTTA recommendation.	DoDM 5105.21-Vol 2 DoDM 5205.07 Vol 3
Integrate updated security requirements into DB RFP or DBB design documents				S			L			PTT interprets space planning and room adjacencies with user and SSM and integrates information from the CSP, TCR, and facility requirements into the contract documents. A copy of the CSP that has been redacted to remove any classified information or contents relating to internal government processes or procedures may be included for reference.	DoDM 5105.21-Vol 2 DoDM 5205.07 Vol 3 UFC 4-010-05
DBB ONLY: Design Development (35-50%) is complete.							L			Designer of Record has developed the Basis of Design, preliminary drawings, outline specifications, and calculations. This is intended to convey the complete extent of the work in a preliminary manner.	FC 1-300-09N

DRAFT

NAVFAC INST 4700.1B (DRAFT) - Design

To be completed prior to Pre-Final Design completion which is: - prior to Construction Contract Award for DBB - after Construction Contract Award for DB											
Confirm CSP requirements for material purchasing, inspection, shipping, and SSA requirements including FF&E.				L			S			CSP is updated by SSM	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
Confirm CSP requirements for site security including area/site access control for personnel, materials, and vehicles				L			S			CSP is updated by SSM	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
CSP is monitored and adjusted to fit design and acquisition plan				L			S			SSM updates the CSP updates coordinated with PM, Design Manager and the Designer of Record.	Fiscal Law, MILCON Law OPNAVINST 11010.20J IC Tech Spec ICD/ICS 705 UFC 4-010-05
If required, submit undated Final CSP	S	S		L			S			Final CSP is completed and submitted to the AO (SCIF)/SAO (SAPF) via SSO Navy/DON SAPCO for approval.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705
Pre-Final Design Submittal				S			L			Designer of Record provides a complete set of design deliverables to include Basis of Design, Drawings, Specifications, Calculations and preliminary FF&E Plan.	FC 1-300-09N
To be completed prior to: - Construction Contract Award for DBB - Start of onsite construction actives for DB											
Final CSP Approval	L	S		S			S	S		AO (SCIF)/SAO (SAPF) issues approval message for Final CSP.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 ICS 705-1 UFC 4-010-05

Preliminary Design Phase

- Project Manager (PM), Design Manager (DM) and Designer of Record (DOR) must work closely with the supported command and the AO's/SAO's representative (SSM) to validate the security requirements for the project.
  - The SSM must validate the initial/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/SAO's sends TEMPEST Countermeasure Review (TCR) Message.

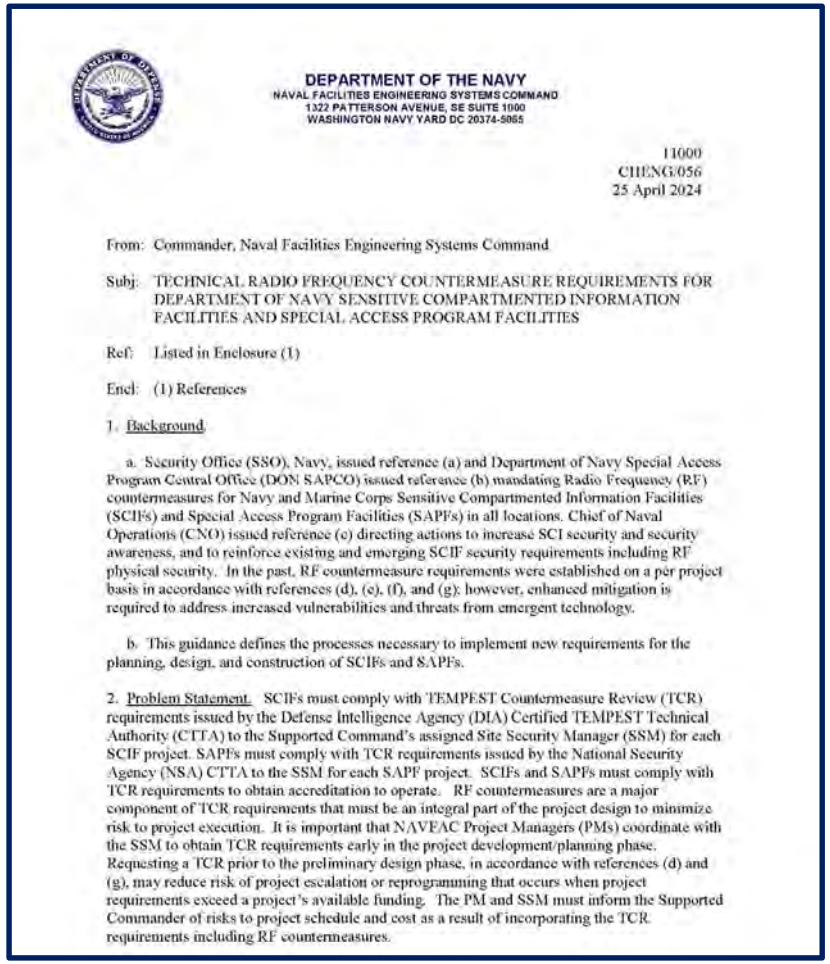
NAVFAC Naval Facilities Engineering Systems Command

TEMPEST Countermeasures

NAVFAC 11000 CHENG/056, 25 April 2024

Technical RF Countermeasure Requirements for DoN SCIFs & SAPFs

- Issued to **improve execution and budgeting** of SCIF/SAPF projects to meet mission needs of Supported Commands.
- Defines **processes** necessary to implement new requirements for the planning, design, and construction of SCIFs and SAPFs.
- Encourages NAVFAC to **coordinate with the Supported Command's SSM** to obtain TCR requirements early in the project development/planning phase.
- Requires NAVFAC to **implement TCR requirements** including RF countermeasures in construction documents for all current and future Navy and Marine Corps projects that include SCIFs/SAPFs.
- **Outlines process steps** for NAVFAC staff to coordinate with the Supported Command's SSM based on execution stage of project.



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

11000
CHENG/056
25 April 2024

From: Commander, Naval Facilities Engineering Systems Command

Subj: TECHNICAL RADIO FREQUENCY COUNTERMEASURE REQUIREMENTS FOR DEPARTMENT OF NAVY SENSITIVE COMPARTMENTED INFORMATION FACILITIES AND SPECIAL ACCESS PROGRAM FACILITIES

Ref: Listed in Enclosure (1)

Encl: (1) References

1. Background

a. Security Office (SSO), Navy, issued reference (a) and Department of Navy Special Access Program Central Office (DON SAPCO) issued reference (b) mandating Radio Frequency (RF) countermeasures for Navy and Marine Corps Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program Facilities (SAPFs) in all locations. Chief of Naval Operations (CNO) issued reference (c) directing actions to increase SCI security and security awareness, and to reinforce existing and emerging SCIF security requirements including RF physical security. In the past, RF countermeasure requirements were established on a per project basis in accordance with references (d), (e), (f), and (g); however, enhanced mitigation is required to address increased vulnerabilities and threats from emergent technology.

b. This guidance defines the processes necessary to implement new requirements for the planning, design, and construction of SCIFs and SAPFs.

2. Problem Statement. SCIFs must comply with TEMPEST Countermeasure Review (TCR) requirements issued by the Defense Intelligence Agency (DIA) Certified TEMPEST Technical Authority (CTTA) to the Supported Command's assigned Site Security Manager (SSM) for each SCIF project. SAPFs must comply with TCR requirements issued by the National Security Agency (NSA) CTTA to the SSM for each SAPF project. SCIFs and SAPFs must comply with TCR requirements to obtain accreditation to operate. RF countermeasures are a major component of TCR requirements that must be an integral part of the project design to minimize risk to project execution. It is important that NAVFAC Project Managers (PMs) coordinate with the SSM to obtain TCR requirements early in the project development/planning phase. Requesting a TCR prior to the preliminary design phase, in accordance with references (d) and (g), may reduce risk of project escalation or reprogramming that occurs when project requirements exceed a project's available funding. The PM and SSM must inform the Supported Commander of risks to project schedule and cost as a result of incorporating the TCR requirements including RF countermeasures.

TEMPEST Countermeasures

- DIA memorandum, dated 28 Nov 2022 mandated RF Countermeasures on all SCIFs starting 01 Jan 2023.
  - Memo redacted 02 Dec 2022 due to conflicting language.
  - SSO Naval Intelligence Security Policy Directives (NISPD) issued 30 Jan 2023 .
- In anticipation of receiving RF Countermeasures requirements late in design or post-award, NAVFAC updated 1391 CRB for FY25 and beyond, to require RF Countermeasures for all rooms which have classified networks.
- **SSO Navy issued a NISPD on 30 JAN 2023 and NAVADMIN 28 JUL 2023, requiring TEMPEST RF Countermeasures on new SCIFs.**
  - **SSO Navy Memo, Naval Intelligence Security Policy Directive (NISPD): 001-23 Mandatory Radio Frequency Countermeasure Requirements for all New DON SCIFS, dtd JAN 2023**
  - **NAVADMIN 169/23, U.S. NAVY SPECIAL SECURITY Officer SENSITIVE COMPARTMENTED INFORMATION (SCI) POLICY AND SCI FACILITY (SCIF) OPERATIONS, dtd JUL 2023**
  - **Both the NISPD and NAVADMIN do not address SAPFs**
- **DONSAPCO Instruction 5530, DON Special Access Program Physical Security Standards, dtd 05 Feb 2024 requires Radio Frequency Countermeasure for SAPFs.**
- All of the NAVY policies regarding RF encourage Commands to survey SCIF/SAPF Accreditation and TEMPEST Countermeasure Review (TCRs) for changes in TEMPEST countermeasures
- **All policies regarding RF provide requirements for both Navy and Marine Corps SCIF/SAPF**

NAVFAC Naval Facilities Engineering Systems Command

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.
  - Today, projects requiring TEMPEST Countermeasures such as shielding are on the increase.
- **If required TEMPEST countermeasures are omitted, the facility will not be accredited.**

NAVFAC Naval Facilities Engineering Systems Command

TEMPEST Countermeasure Review (TCR)

- 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.

NAVFAC Naval Facilities Engineering Systems Command

TEMPEST Countermeasure Review (TCR)

TEMPEST Countermeasure recommendations/considerations

- Inspectable Space/Perimeter
- SCIF/SAPF Location
- Red/Black Separation
- Wireline Shielding
- Wireline Grounding
- Red Line Identification
- Cable Distribution Systems
- Patch/Distribution Panels
- Wall Jack Separation
- COMSEC/CRYPTO Equipment
- TEMPEST Equipment
- Commercial Cable TV (CATV) and Satellite TV isolators
- Signal Line Filters/Isolators
- Red Power Line Filters/Isolators
- Non-Conductive/Dielectric Sections
- Architectural RF Shielding
- Field Testing

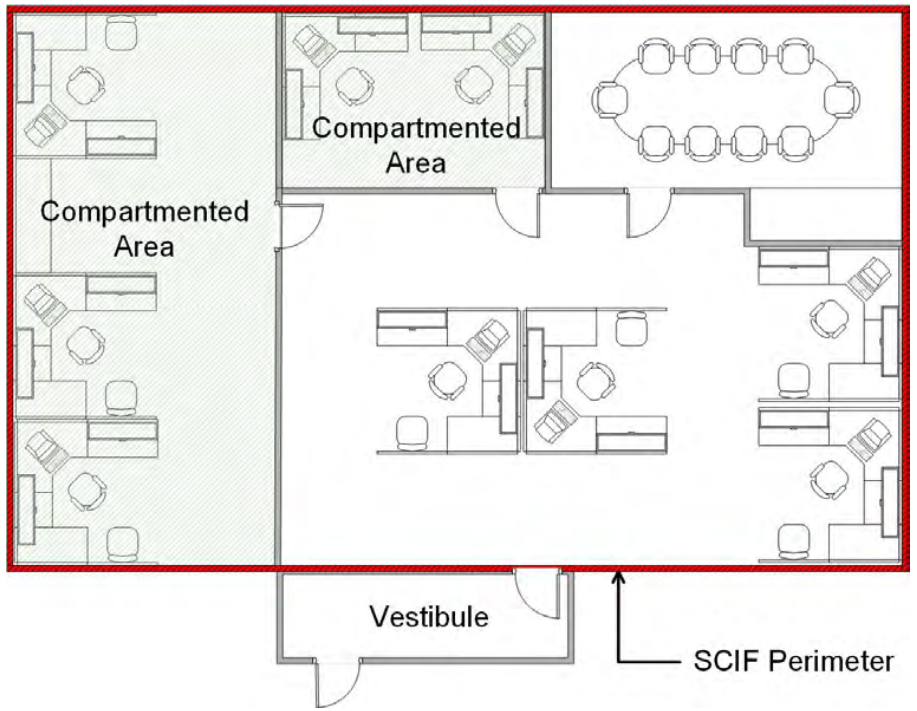
PER DoD Manual 5105.21, Volume 2:

- TEMPEST vulnerabilities and recommended countermeasures are **classified at a minimum of CONFIDENTIAL when associated with a physical location**.
- A TEMPEST vulnerability or countermeasure associated with a SCIF ID number or in a manner that cannot be connected to the physical location is UNCLASSIFIED

NAVFAC Naval Facilities Engineering Systems Command

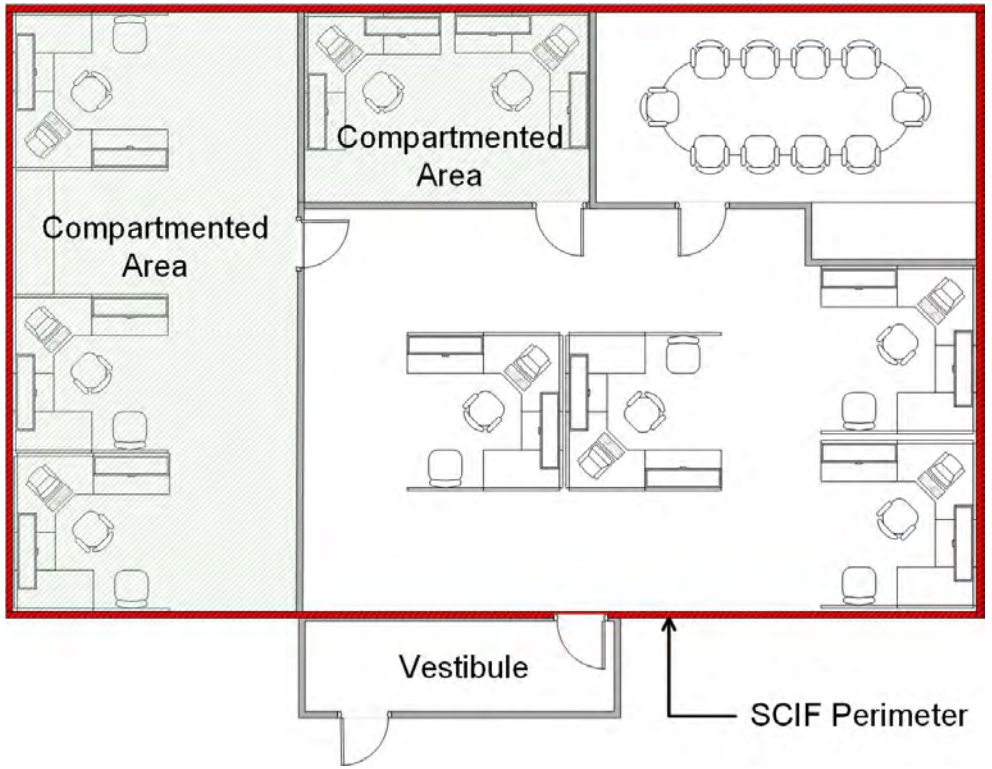
General Design Strategy: Consolidate Spaces

- 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, and sustainment.
  - Coordinate with the supported commands to ensure the configuration will meet their operational **(compartmented)** requirements.



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**
    - Type II & III have the same construction requirements



General Design Strategy: Compartmented Area (CA)

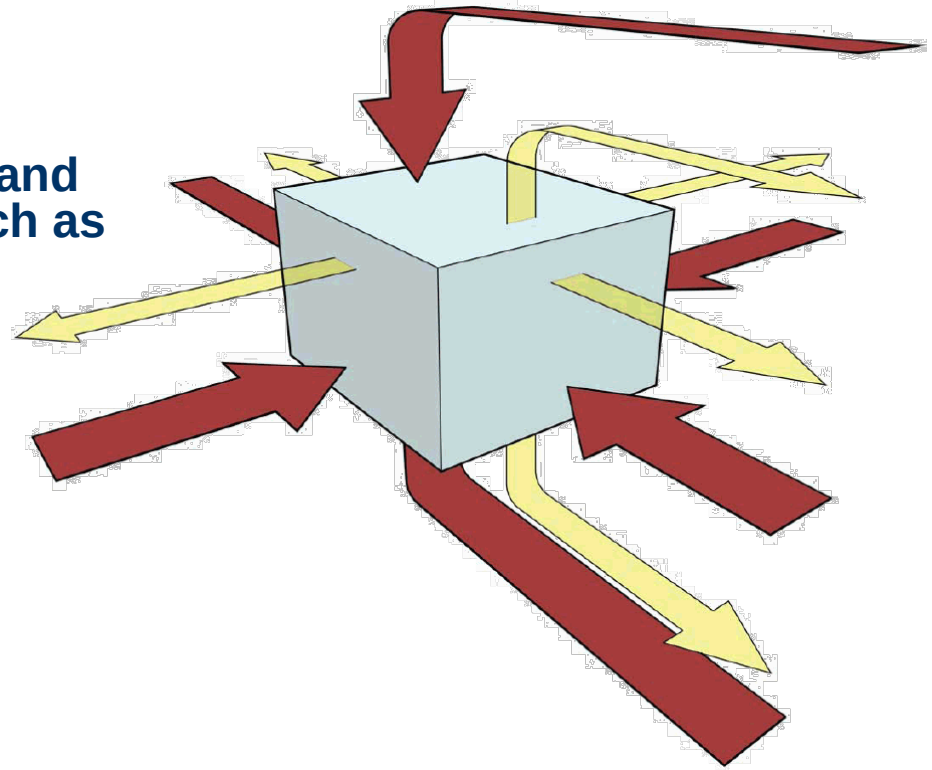
- **The design and layout of Type II &III Compartmented Areas is a critical element of the layout of the facility when acoustic protection is required for individual rooms within the space.**
- **Compartmented Areas, their type, and adjacencies must be identified early in the design process.**
  - Acoustic Z-Ducts can increase the above ceiling space requirement
  - Sound baffles can significantly affect the HVAC system design due to the increase in backpressure.

NAVFAC Naval Facilities Engineering Systems Command

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 (REQUIRED)**

NAVFAC Naval Facilities Engineering Systems Command

General Design Strategy: Building Layout

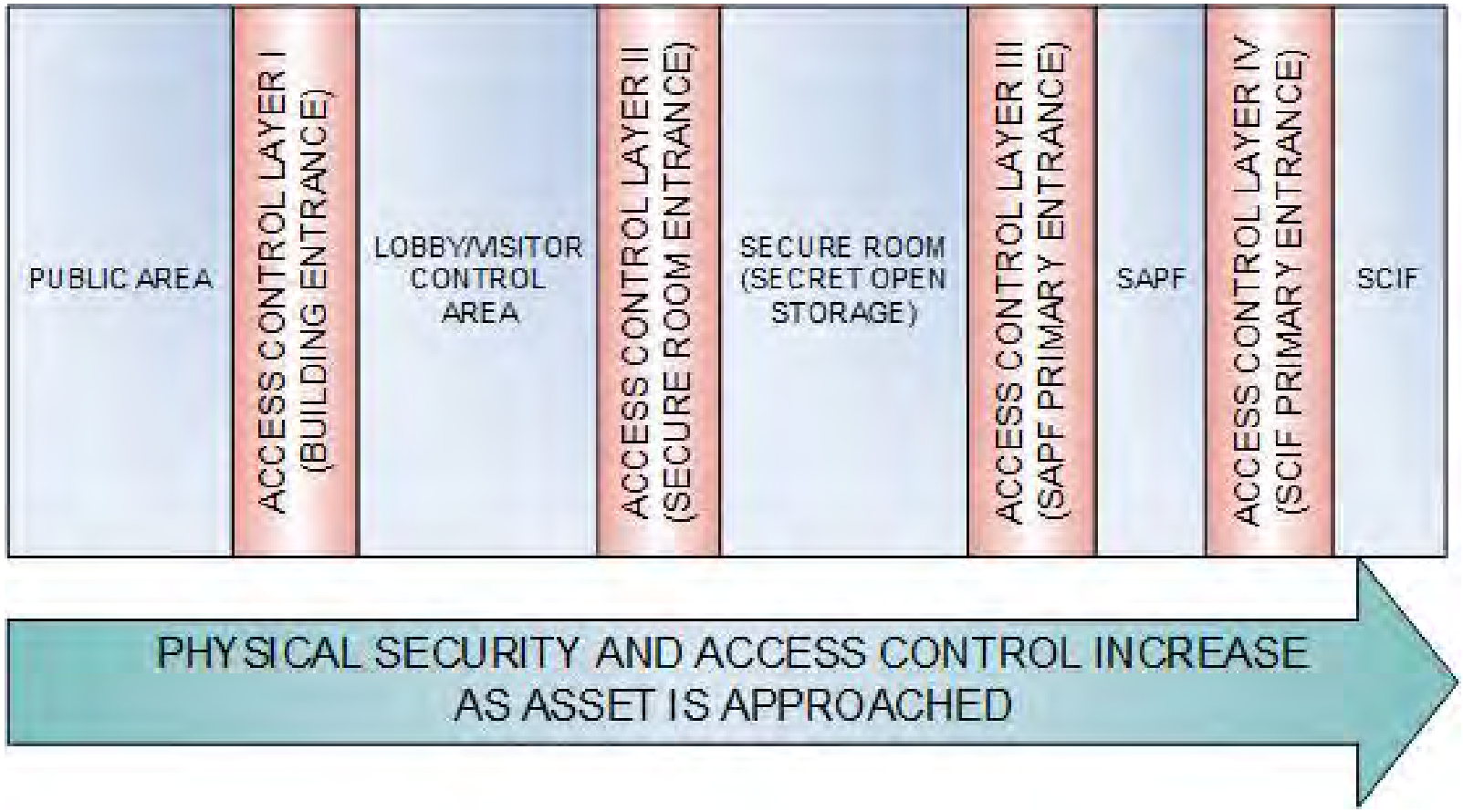
- To optimize the building layout for security and function, the designer must understand:
  - o The various secure spaces in the facility
  - o The security clearances of the occupants
  - o Visitor access and escort requirements
  - o Separations or adjacencies required
  - o Compartmented Areas
- 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.

NAVFAC Naval Facilities Engineering Systems Command

General Design Strategy: Zoning

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

ACCESS LAYERS.

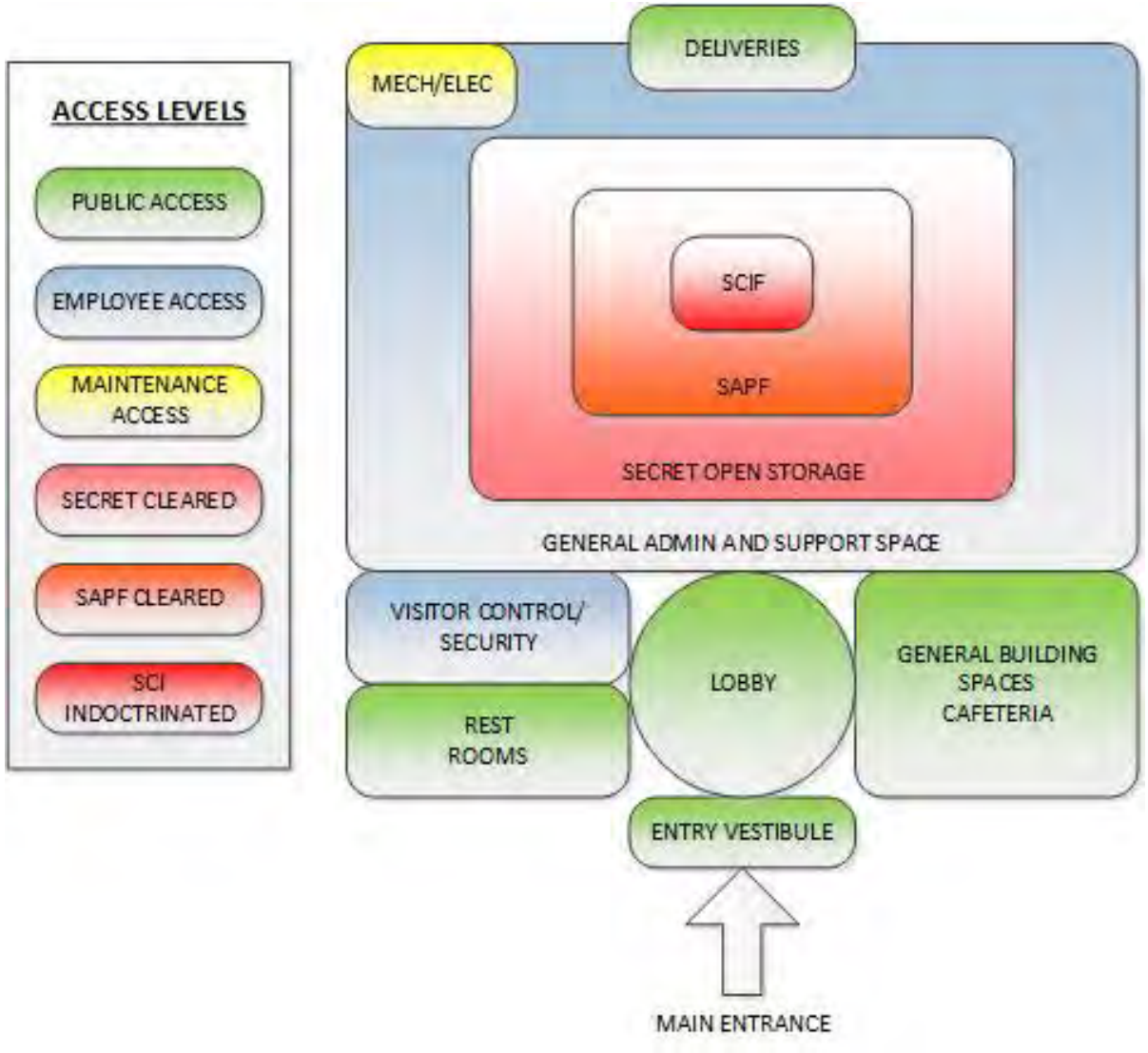


NAVFAC Naval Facilities Engineering Systems Command

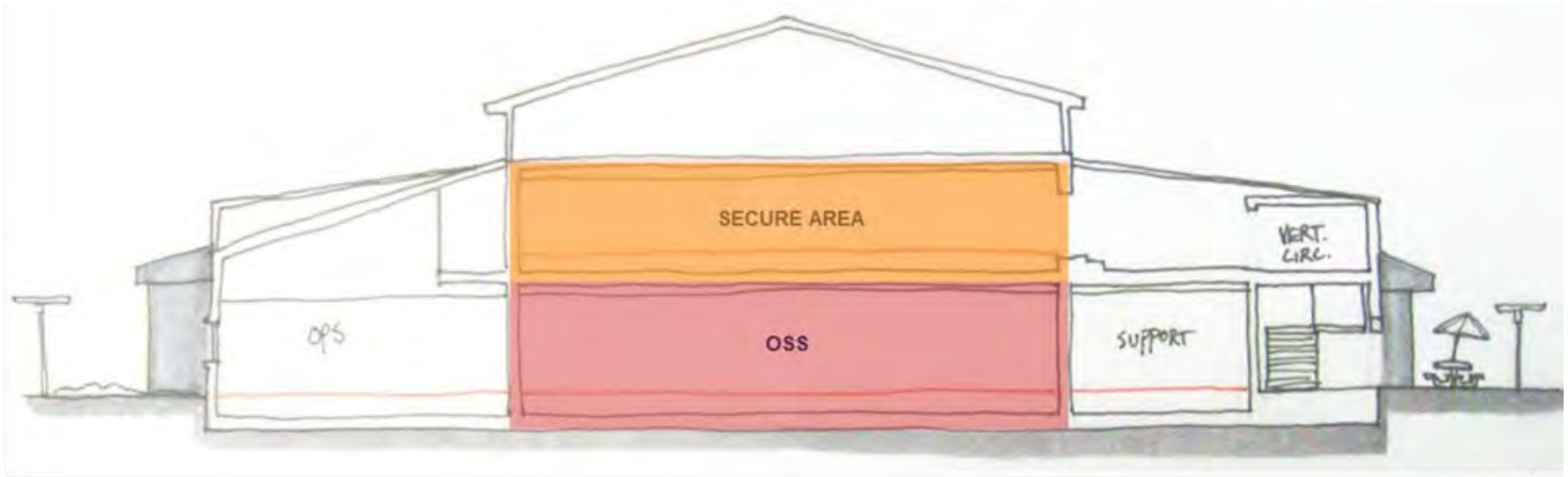
General Design Strategy: Security Zones

Zones may include

- Public Access
- Controlled Access
- Restricted Access,
- Which can be related to
  - Public/Visitor Areas,
  - Service Areas
  - Controlled Access Areas
  - Secret Open Storage
  - Top Secret Open Storage
  - SCIF or SAPF



General Design Strategy: Building Layout



BUILDING SECTION

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

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. **(See previous slide)**

NAVFAC Naval Facilities Engineering Systems Command

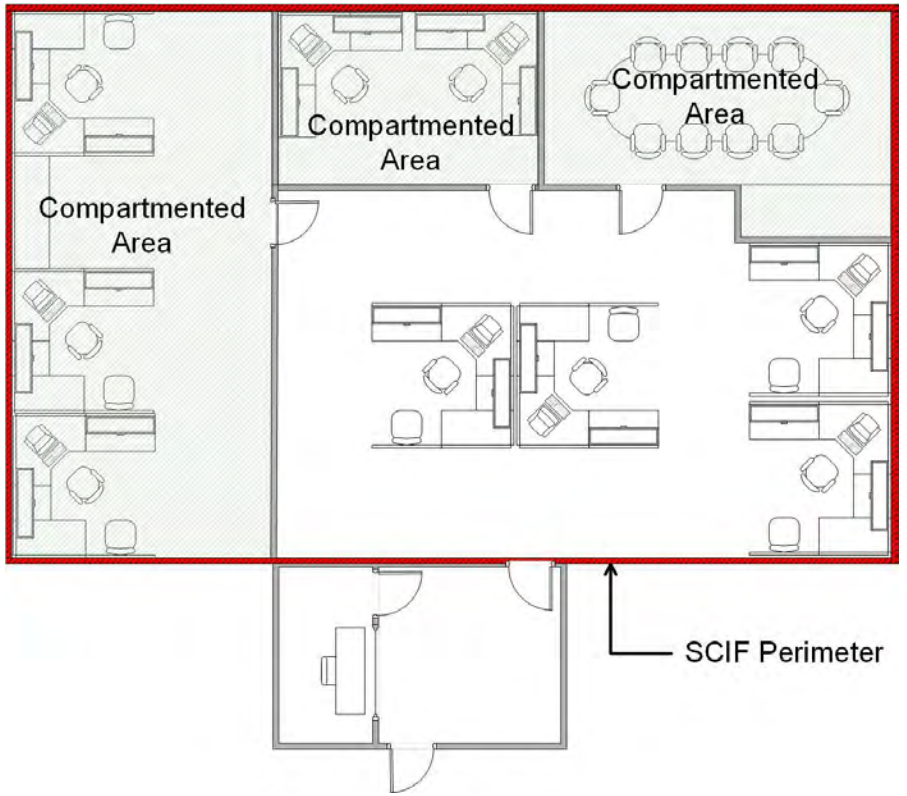
General Design Strategy: Building Layout

- 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.
  - To increase SID, locate secure space within areas that require access control.
  - 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).

NAVFAC Naval Facilities Engineering Systems Command

General Design Strategy: Layout

- PRIMARY ENTRANCE VESTIBULE: When practical, the entrance into a secure area should incorporate a vestibule to preclude visual observation and enhance acoustic protection.
  - In most applications, the interior door of the vestibule will be the secure perimeter and be sound rated.
  - Provide acoustic treatments in vestibules to help absorb and diffuse sound.
  - Vestibule may have to be sized to accommodate visitor check-in and badging.
  - 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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Acoustic Protection

- 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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Acoustic Protection

- 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.

NAVFAC Naval Facilities Engineering Systems Command

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***

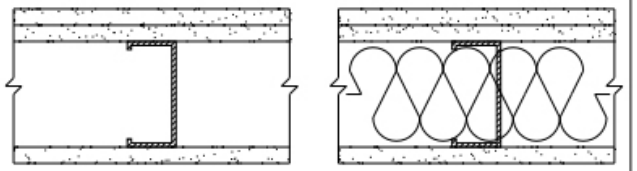
WALLS AND PARTITIONS, NONCOMBUSTIBLE

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, or column.
- 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.

NAVFAC Naval Facilities Engineering Systems Command

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.
- TCR recommended countermeasures (foil backed GWB or layer of approved Ultra Radiant Foil)
  - Foil backed GWB may be problematic
  - Installed in accordance with *Best Practices Guideline for Architectural Radio Frequency Shielding (FOUO)*.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Perimeter

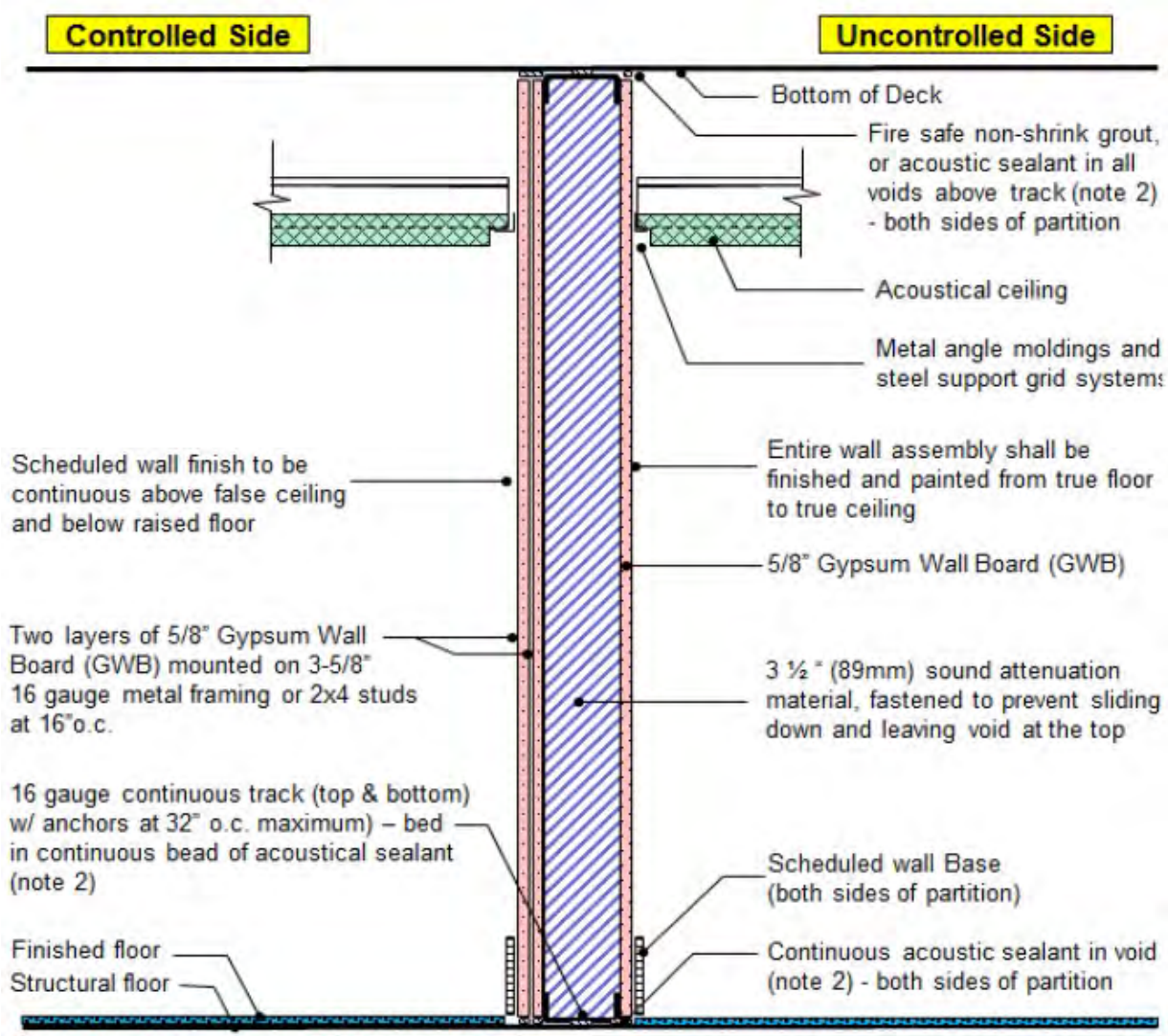
- Wall A (Standard Wall) - Sound Group 3 (STC 45 or better)
  - 3-5/8” metal or 2 x 4 wood studs.
  - Continuous runners (same gauge as studs) attached to true floor and true ceiling.
  - Three layers of 5/8 inch foiled back Type X gypsum, one layer on the outside and two on the inside of the SCIF wall. 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.

NAVFAC Naval Facilities Engineering Systems Command

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 TCR. Foil backed GWB or a layer of approved Ultra Radiant 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 a STC Rated or RF Shielded wall shall be surface mounted.



Specific Design Strategy: Perimeter

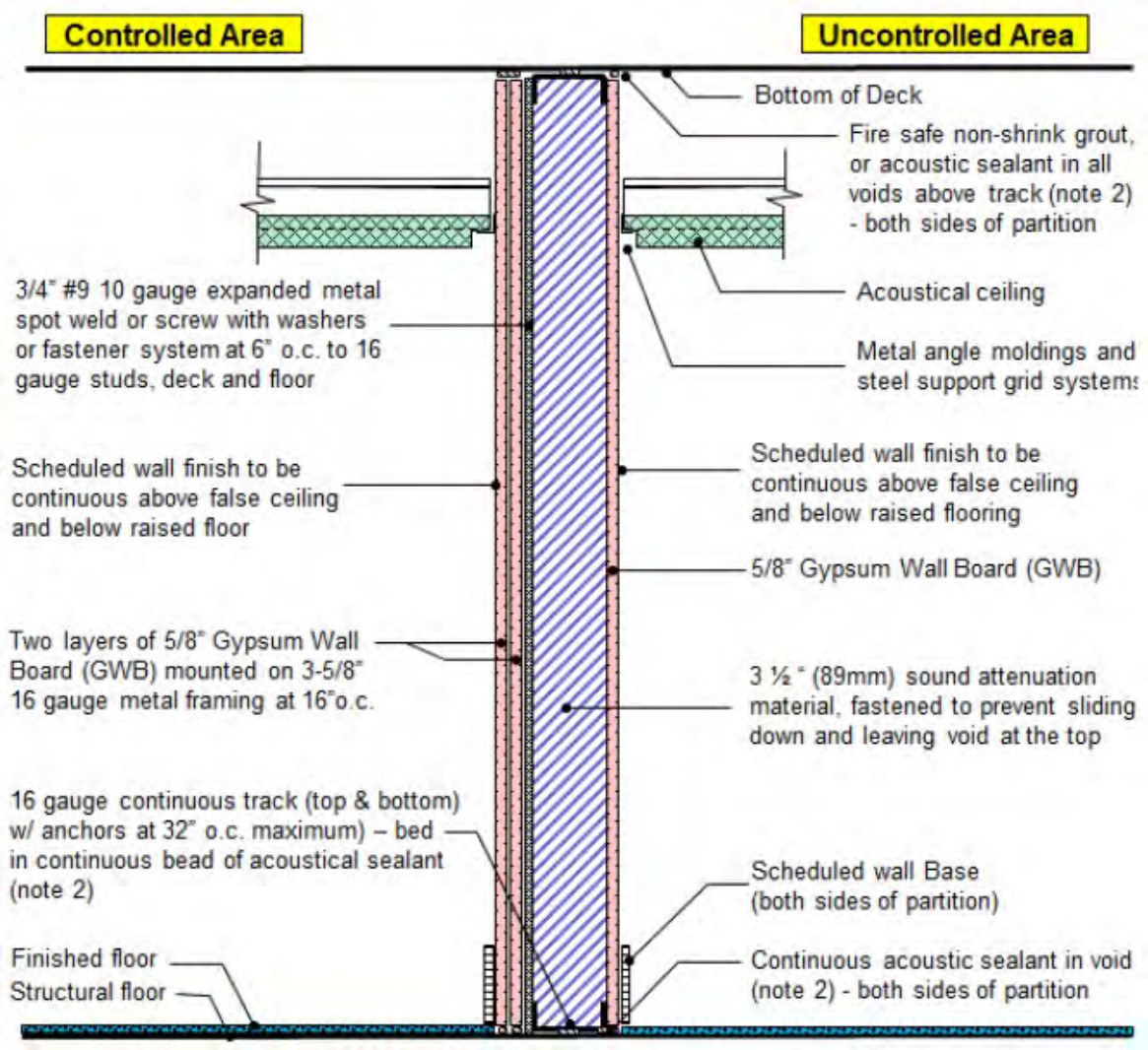
- **Wall B (Enhanced Wall) Expanded Metal Sound Group 3 (STC 45 or better):**
  - **Same as Wall A except:**
    - **Metal studs and runners shall be 16 gauge.**
    - **Wood or Metal Studs shall be 16” on center.**
    - **Provide ¾” #9 (10 gauge) case hardened expanded metal affixed to the interior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

NAVFAC Naval Facilities Engineering Systems Command

Wall B Suggested Construction for Expanded Metal

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

- TCR 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 a STC Rated or RF Shielded wall shall be surface mounted.



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.

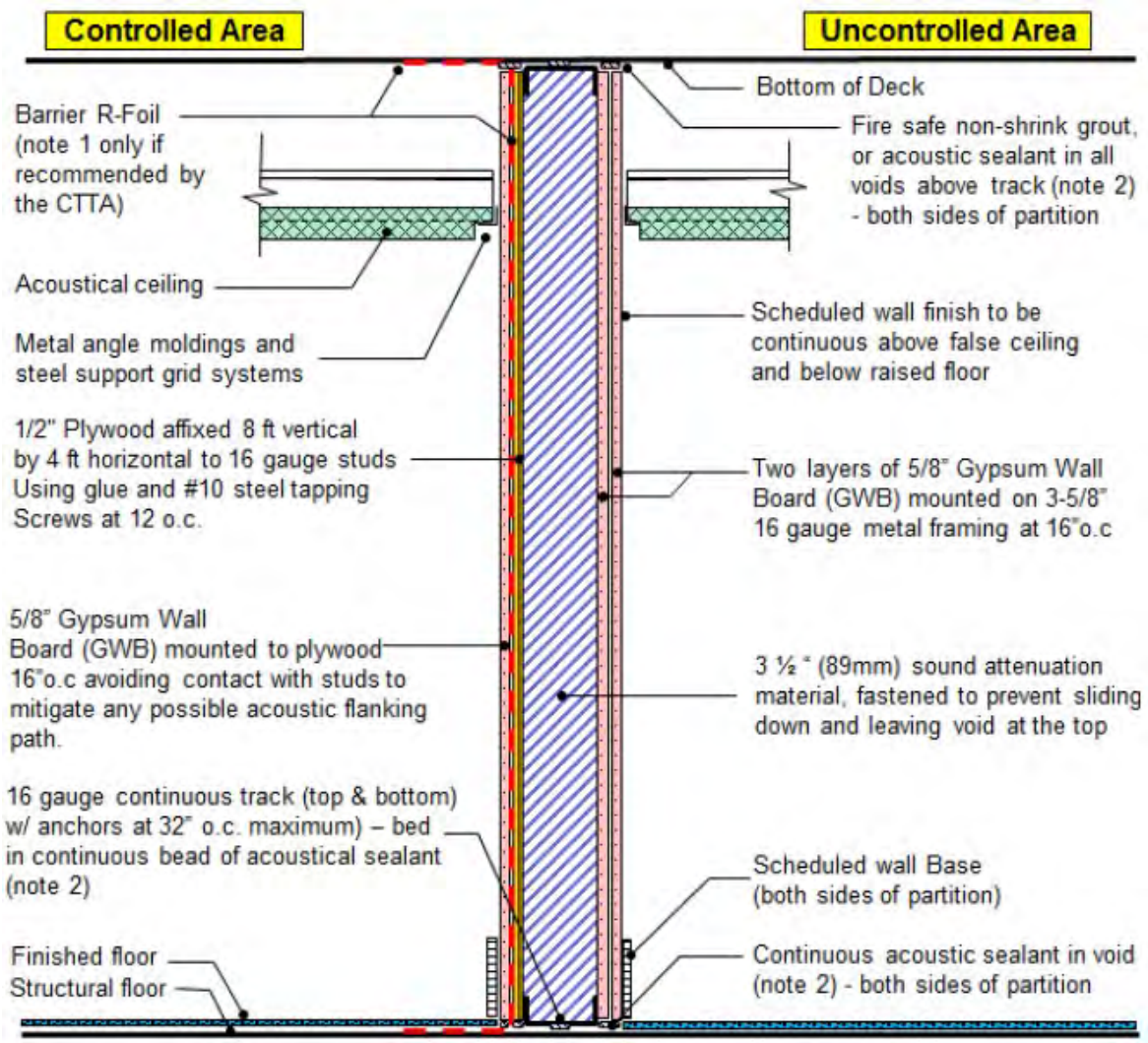
- Wall C with Fire Rated Plywood is sometimes preferred over Expanded Metal for enhanced walls to mitigate against surreptitious entry.

NAVFAC Naval Facilities Engineering Systems Command

Wall C Suggested Construction for Plywood (Fire Rated)

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

- TCR 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 a STC Rated or RF Shielded wall shall be surface mounted.



Specific Design Strategy: Perimeter

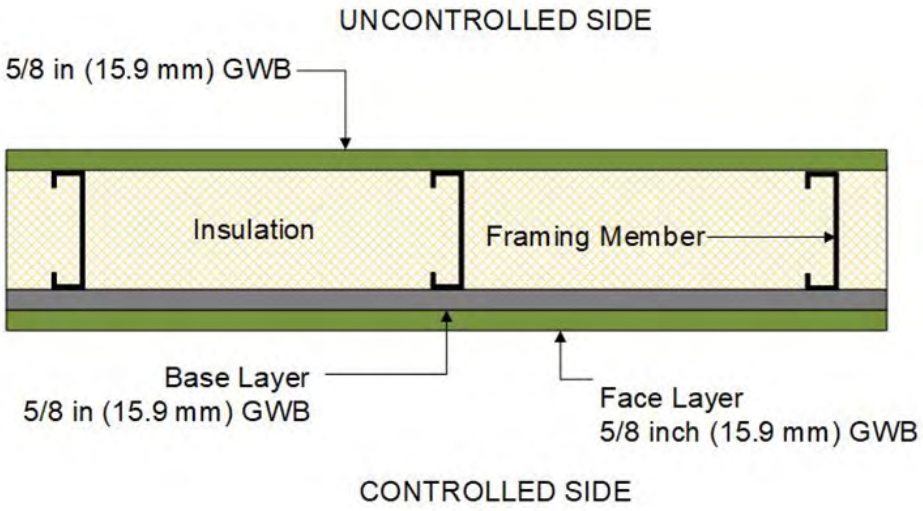
- IC Tech Spec-for ICD/ICS 705 indicates Standard STC 45 wall requires three layers of 5/8 inch (15.9 mm) gypsum wallboard (GWB). One layer on the uncontrolled side (outside) of the protected area and two layers on the controlled side (interior) of the protected area to meet STC 45, STC 50 wall requires 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.

NAVFAC Naval Facilities Engineering Systems Command

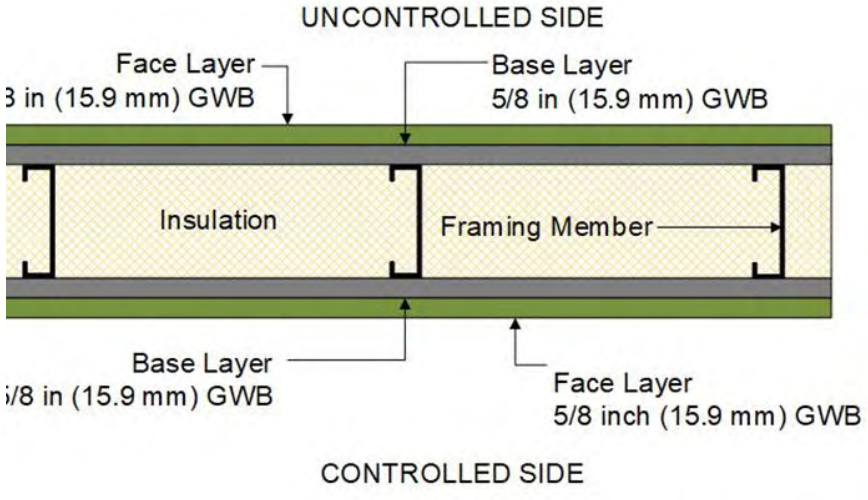
Specific Design Strategy: Perimeter

- **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

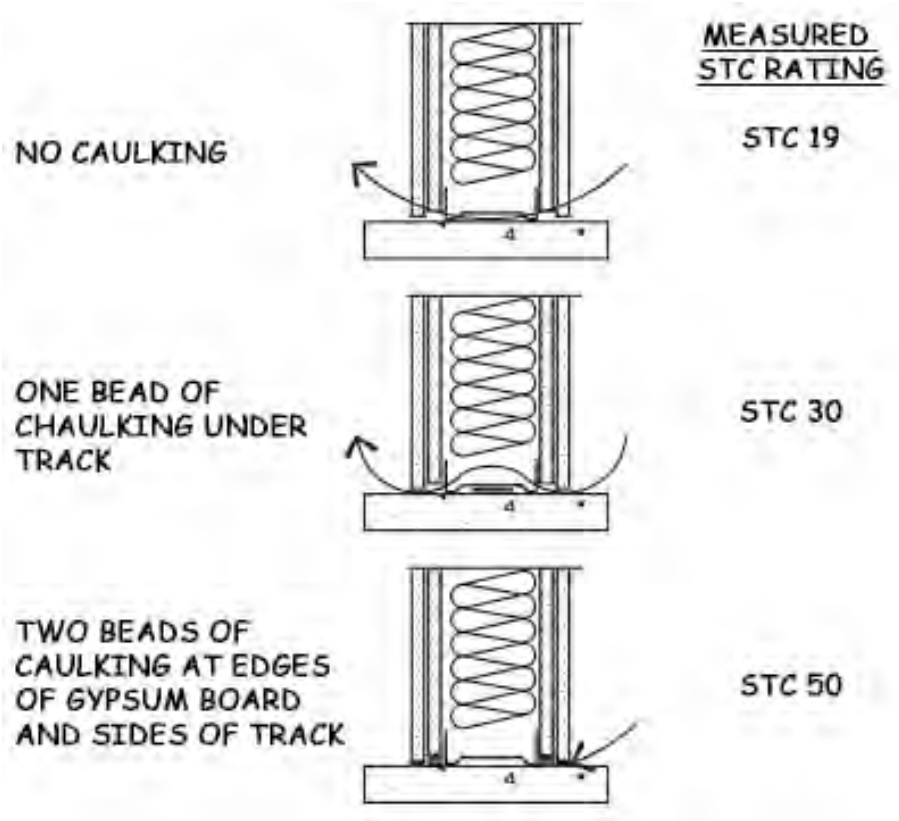


STC 50 Assembly



Specific Design Strategy: Perimeter

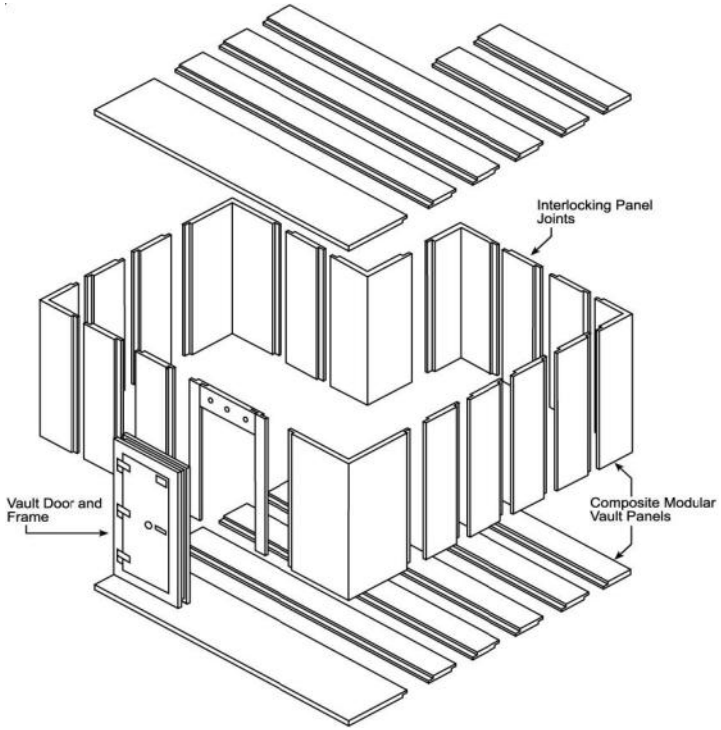
- Gypsum board panels are lifted into using a spacer under their bottom edge, so there is a small gap at the bottom.
- Sealing openings is critical to acoustical performance. Seal gaps with a non-hardening caulk so the acoustical rating of the wall is maintained
    - Minimum – Continuous sealant each 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)



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



NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Utilities

- Utilities such as power, Telecommunications, signal, or plumbing on the perimeter wall treated for acoustic or RF shielding 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.**

NAVFAC Naval Facilities Engineering Systems Command

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.

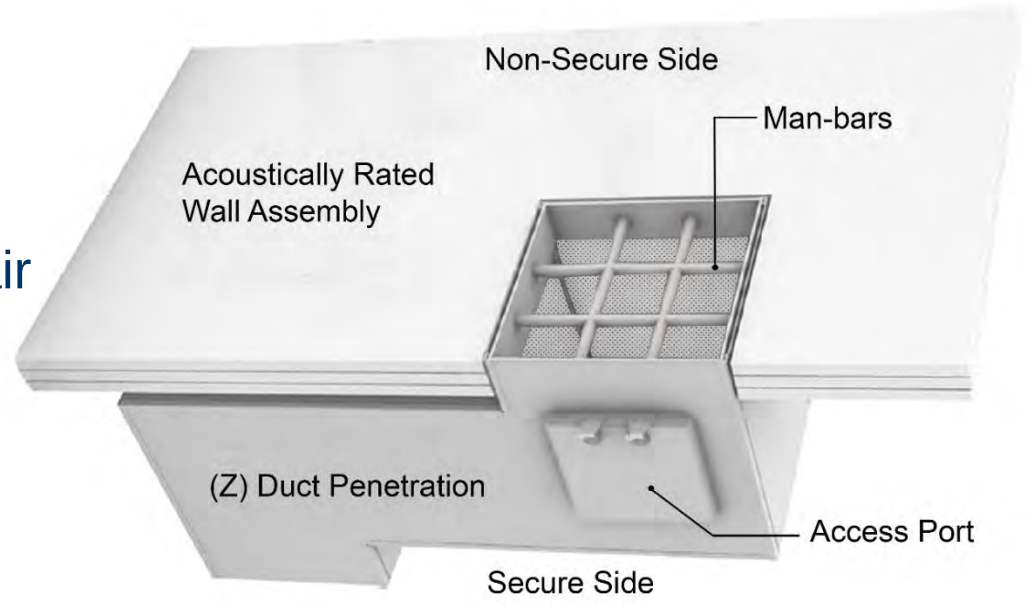
- HVAC ducts: Provide a nonconductive break (flex connection) using material appropriate for the climate, for a 2- to 6-inch section of the duct adjacent to the duct penetration through the perimeter wall (inside wall).

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Utilities

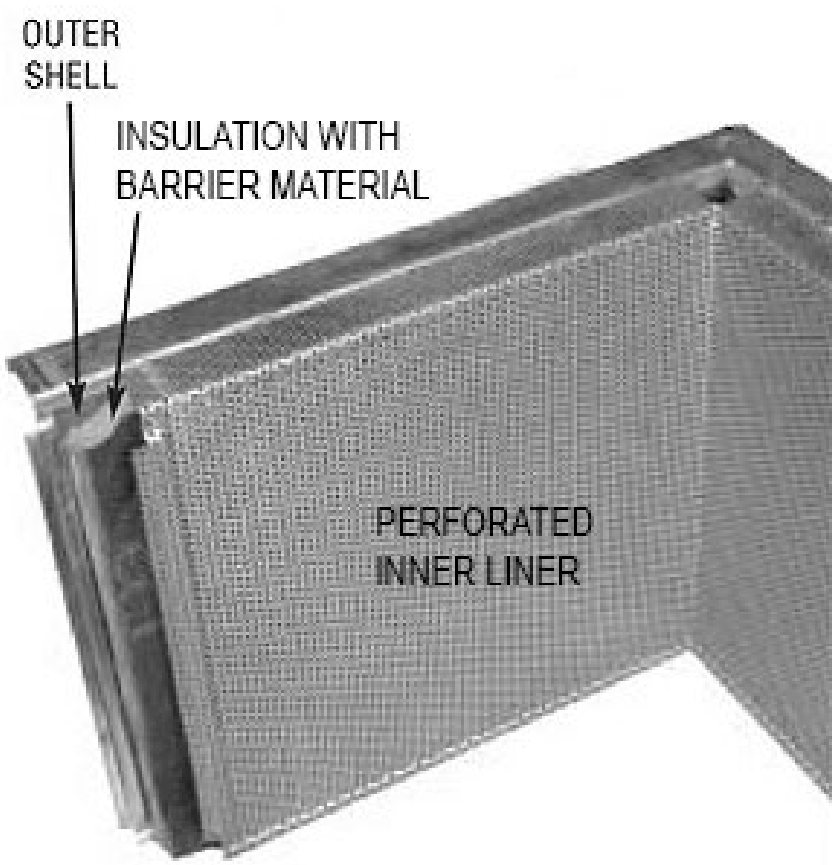
- Vents and Ducts
  - All vents and ducts must be protected to meet the acoustic requirements
  - To ensure acoustic performance of the perimeter is not compromised, provide sound baffles (duct silencers) or (Z) Duct Penetrations.
    - IC Tech Spec – for ICD/ICS 705 provides an example of a (Z) Duct 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 betweer the perforated liner and the insulation designed to prevent air quality issues caused by bacteria and other contaminates that can embed in the insulation.



NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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.

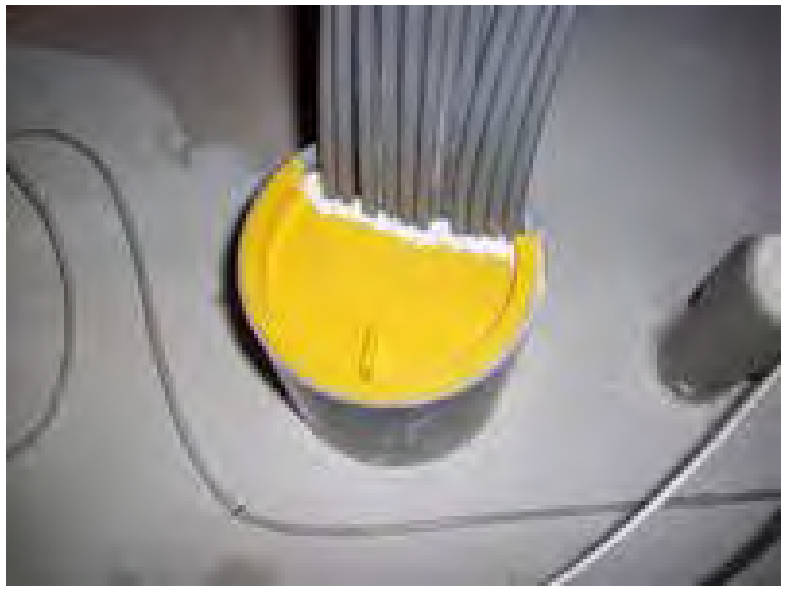
MANBARS

INSPECTION PORT

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Utilities

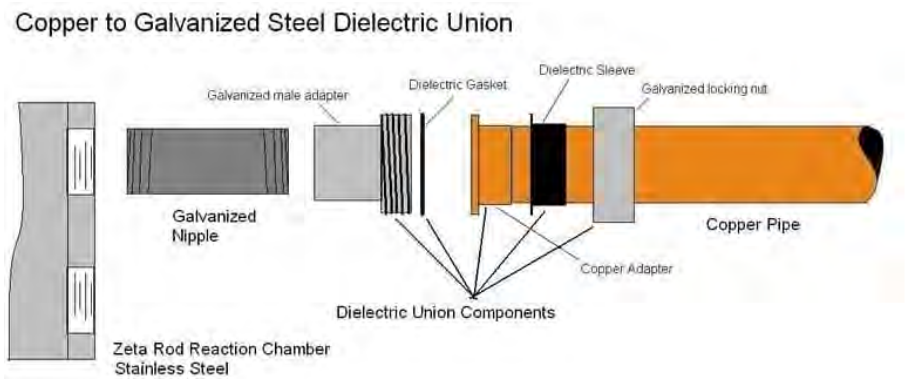
- Utilities (power & signal) should enter the perimeter at a single point.
  - All utility penetrations must be sealed to mitigate acoustic emanations and covert entry.
  - Spare conduits are allowed for future expansion provided the expansion conduit is filled with acoustic fill and capped.
- Utilities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



NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Utilities

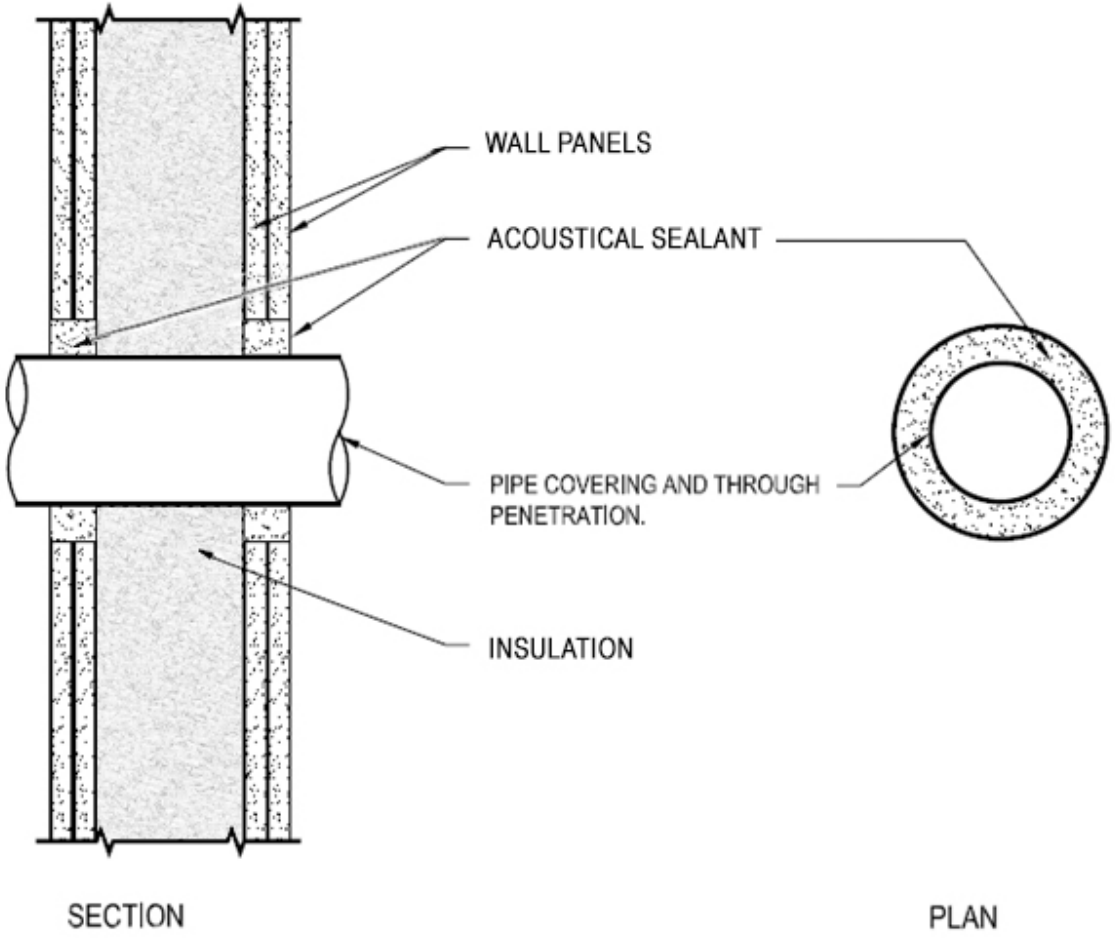
- Metallic penetrations through the perimeter may be considered carriers of compromising emanations (CE) and require TEMPEST countermeasures. Unless directed otherwise by the TCR:
  - Metallic conduit: install dielectric (non-conduction) union adjacent to the pipe penetration through the perimeter wall (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

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



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.

NAVFAC Naval Facilities Engineering Systems Command

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

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Doors

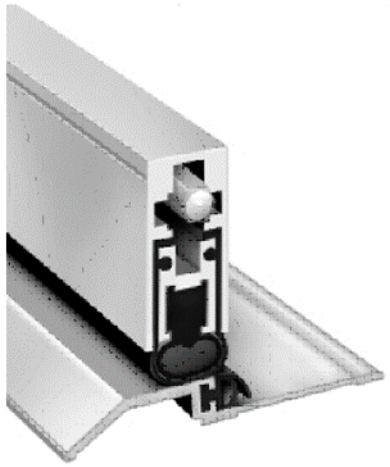
- **<u>Off the Shelf Doors – JUST DON'T DO IT!</u>**
  - **1 ¾ inch thick solid core wood or composite doors will not meet STC 45 rating.**
  - **1 ¾" Solid core door – factory sealed**
    - Best STC obtainable = 38 STC
  - **1 ¾" Solid core door – field assembly**
    - Best STC obtainable = 35 STC
  - **2" Solid core door – factory sealed**
    - Best STC obtainable = 42 STC

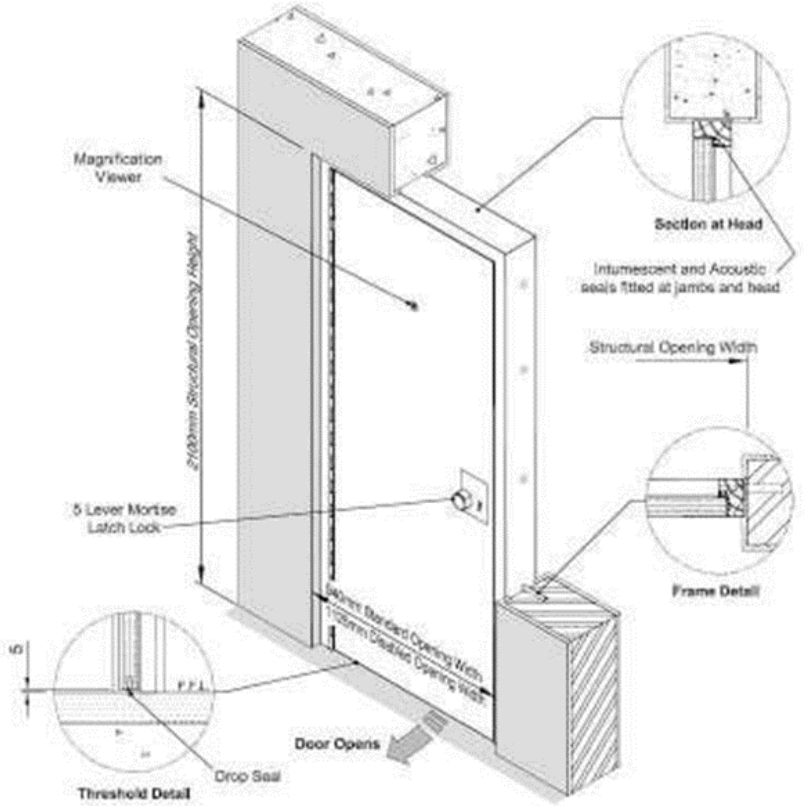
- **Unsealed gaps and clearances in door assemblies cancel the soundproofing qualities of acoustical doors.**
- **A 1% opening around a door will allow up to 50% of the sound to pass through.**

Specific Design Strategy: Doors

- In order to obtain a true STC rated door specify an acoustical doors assembly using UFGS 08 34 73 *Sound Control Door Assemblies* to include door, seals, hinges, door closer, frame 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

- 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

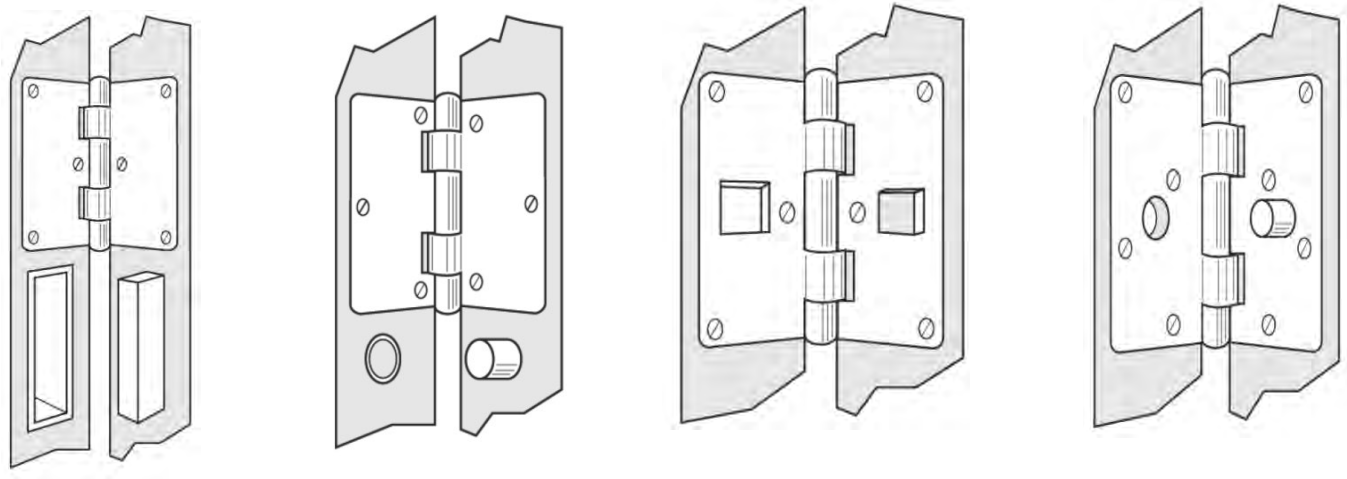
- Acoustical rated door assemblies are much heavier than typical doors and require additional structural support.
  - Coordinate design of structural support with a Structural Engineer.
  - Install in door assembly in accordance with UFGS 08 34 73 and manufacturer's instructions.

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

NAVFAC Naval Facilities Engineering Systems Command

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: 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

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

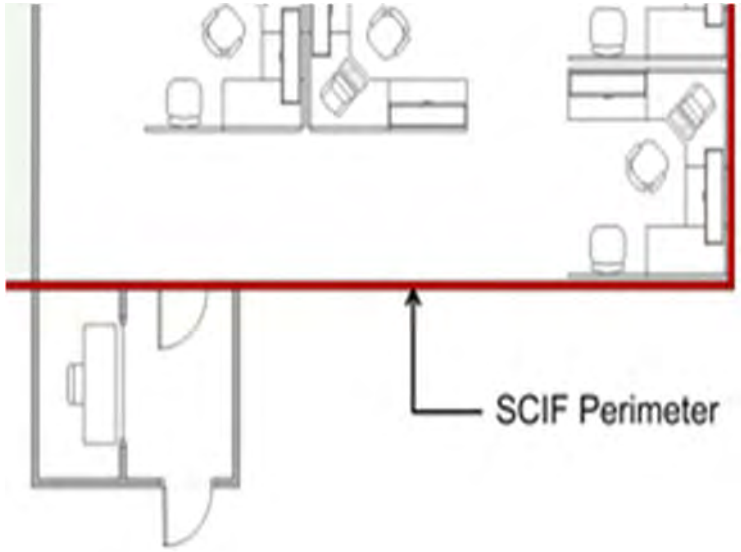
Specific Design Strategy: Doors

- 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.

NAVFAC Naval Facilities Engineering Systems Command

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.



NAVFAC Naval Facilities Engineering Systems Command

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 TCR.
- 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 monitored by Intrusion Detection System

NAVFAC Naval Facilities Engineering Systems Command

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 TCR.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Daylighting

- When provided, daylighting design must be coordinated with the SSM. Design daylighting fenestration to be non-opening, provide visual and acoustic protection and include TEMPEST countermeasures when recommended by the TCR.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Daylighting

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

NAVFAC Naval Facilities Engineering Systems Command

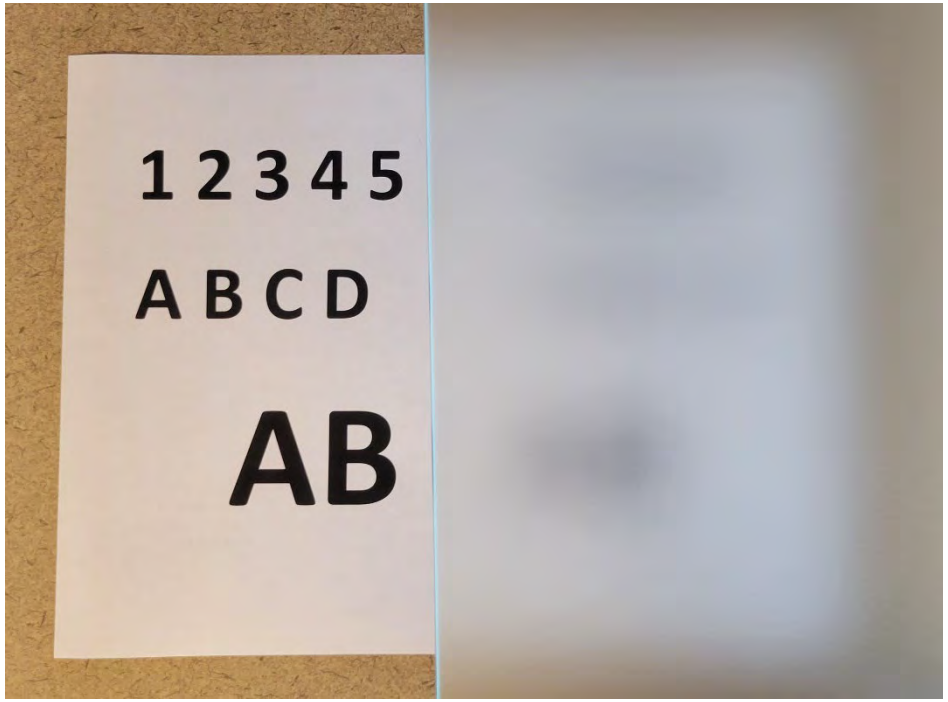
Specific Design Strategy: Daylighting

- 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
    - Be monitored by Intrusion Detection System
    - If one dimension of the penetration measures less than 6 inch (150 mm), forced entry protection and alarm is not required.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: Visual Protection

- Provide visual protection by methods such as full surface acid etching, sand blasting, or an obscure polyvinyl butyral interlayer.
- Method must obscure vision into the protected area while providing daylight penetration.
- For existing windows, blinds, drapes or other coverings may be used with SSM approval.
- Product to the right is single side acid etched :
  - 82.5 % Total Luminance Transmittance
  - 75% diffuse Transmittance
  - 90.73% Haze



NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy – Access Control

- **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. Visual notification can be handheld or installed.
    - When installed, place lights to ensure visual observation by SCIF personnel.
    - At a minimum, provide controls within the perimeter at each entrance into the space or compartmented area..

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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 TCR.
  - All incoming wiring must penetrate the 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.

NAVFAC Naval Facilities Engineering Systems Command

General Design Strategy:
Electronic Security System (ESS)

- Requirements for IDS 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.

NAVFAC Naval Facilities Engineering Systems Command

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 Standard for National Industrial Security Systems for the Protection of Classified Materials.
  - UL 2050 materials are restricted and only distributed to those demonstrating relevant national industrial security involvement.

NAVFAC Naval Facilities Engineering Systems Command

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:

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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: ESS

- Intrusion Detection System Requirements:
  - Protect all Interior areas through which reasonable access could be gained, 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 Level II High Security Switch (HSS) and a motion sensor.

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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 the IDS control panel.
    - Only SCIF/SAPF 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/SAPF, line security shall be employed.
  - Refer to UFC 4-021-02, Electronic Security Systems for more on system design including tamper protection.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: ESS

- IDS Electrical Power
  - Standby Power.
    - Provide twenty-four hours of uninterruptible standby power.
      - This may be provided by batteries, uninterruptible power supply (UPS), or engine-generators, or any combination. Standby power for IDS should not generate the requirement for a UPS or engine-generator.
      - When an engine-generator is available for standby power, provide batteries for IDS that provide a minimum of four hours of standby power to allow uninterrupted power during transitions to and from standby generator power
  - 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.

NAVFAC Naval Facilities Engineering Systems Command

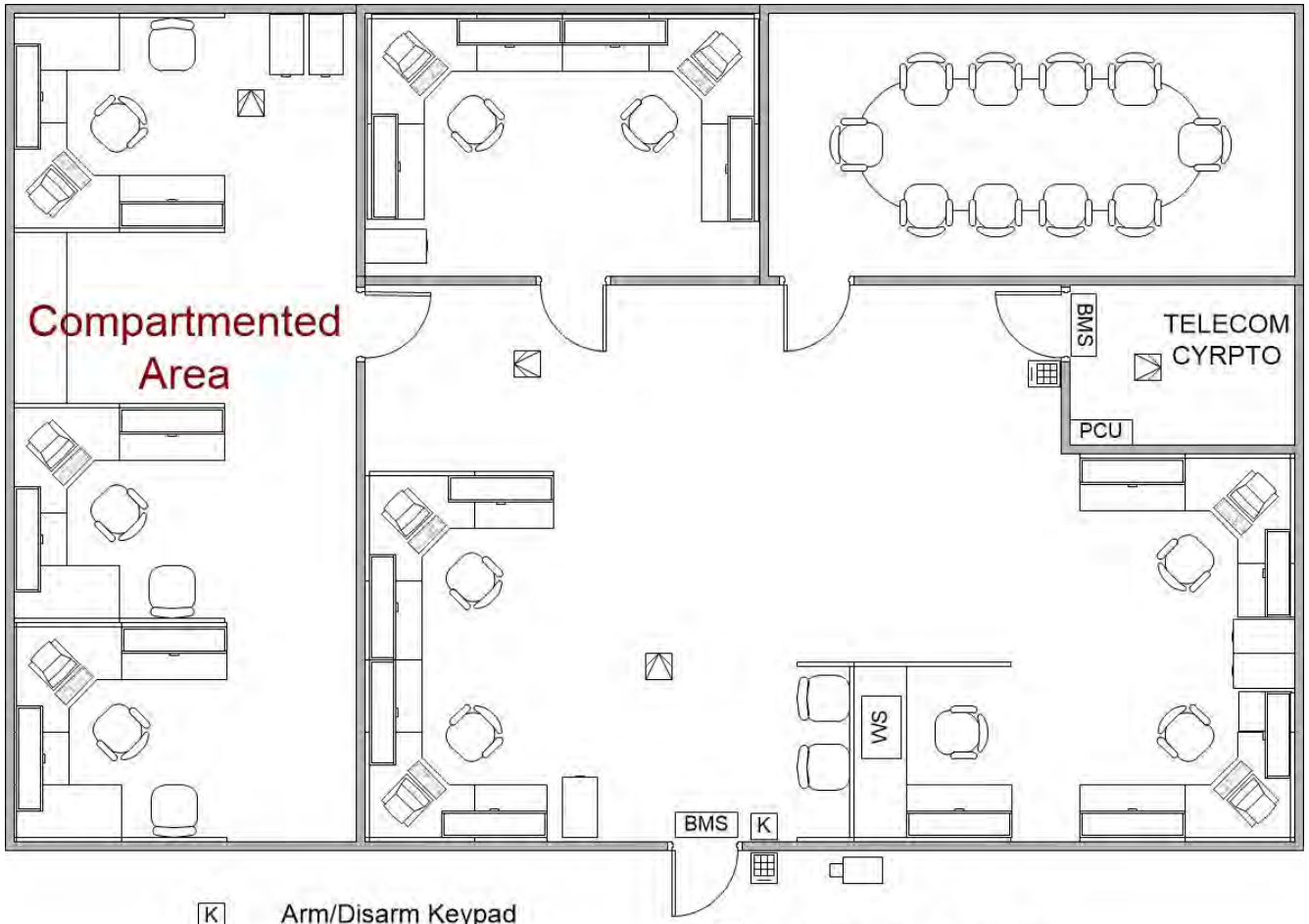
Specific Design Strategy: ESS

- 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).

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: ESS



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

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

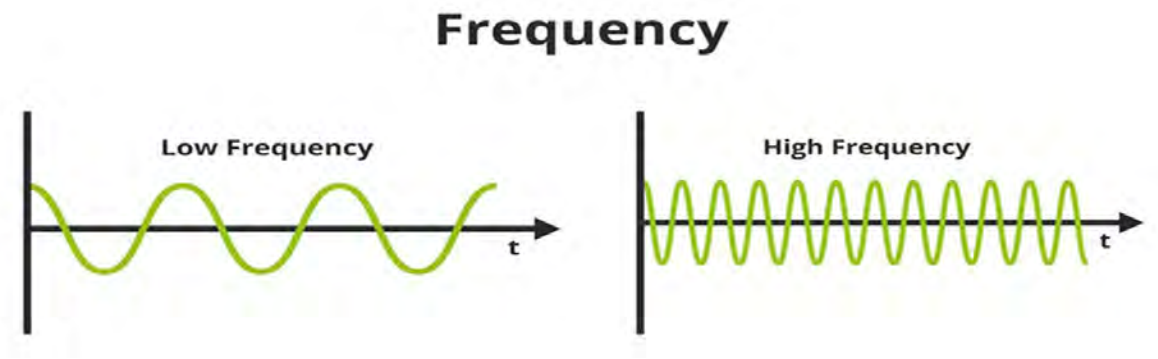
Specific Design Strategy: ESS

- **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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

- **ATTENUATION:** A general term used to denote a **decrease in magnitude of power or field strength** in transmission from one point to another caused by such factors as absorption, reflection, scattering, and dispersion. **Expressed as a power ratio or by decibels**.



Amplitude = Wave Height
Measured in Decibels

Frequency = 1 Cycle
Measured in Hertz

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

Specific Design Strategy: TEMPEST

SHIELDING EFFECTIVENESS:

- A measure of the **reduction or attenuation in the electromagnetic field strength** at a point in space caused by the insertion of a shield between the source and that point
- The difference between the free space reference level and the data measurements represents the shielding effectiveness of each tested wall type

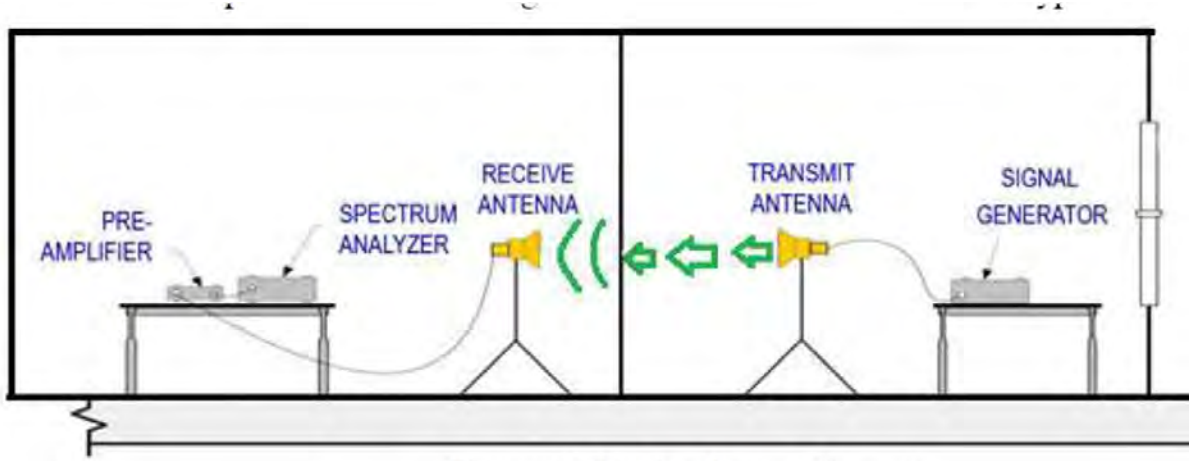


Figure 2: Testing layout diagram

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.**

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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.**

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

TEMPEST Checklist Attachments Summary:

- Floor plans showing all signal lines (phone, cable TV, PA system, alarm system, computer system, power filters, isolators or amplifiers)
- Floor plan showing ductwork routing
- Floor plan showing transmitters within 3 meters of the SCIF
- Completed information processing chart
- Drawings showing location of SCIF within base, SCIF with respect to the nearest city, SCIF within the building

Specific Design Strategy: TEMPEST

TEMPEST Checklist Attachments Summary (cont'd):

- Drawing showing distance in meters, North, South, East and West to the base boundary
- Drawing showing locations within 200 meters occupied by foreign nationals
- If multistory and not US controlled, layout of all floors identifying occupants
- Drawing of the location of any Protected Distribution System

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

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

- **For all Navy and USMC projects <u>SHIELDING IS REQUIRED</u>:**
  - **Provide foil backed GWB or Radiant Foil (R-foil) in accordance with *Best Practices Guideline for Architectural Radio Frequency Shielding*.**
  - **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.**
    - **Foil backed GWB may be problematic.**
  - **When R-foil is employed it shall be placed inside the space between the first and second layer of gypsum board.**

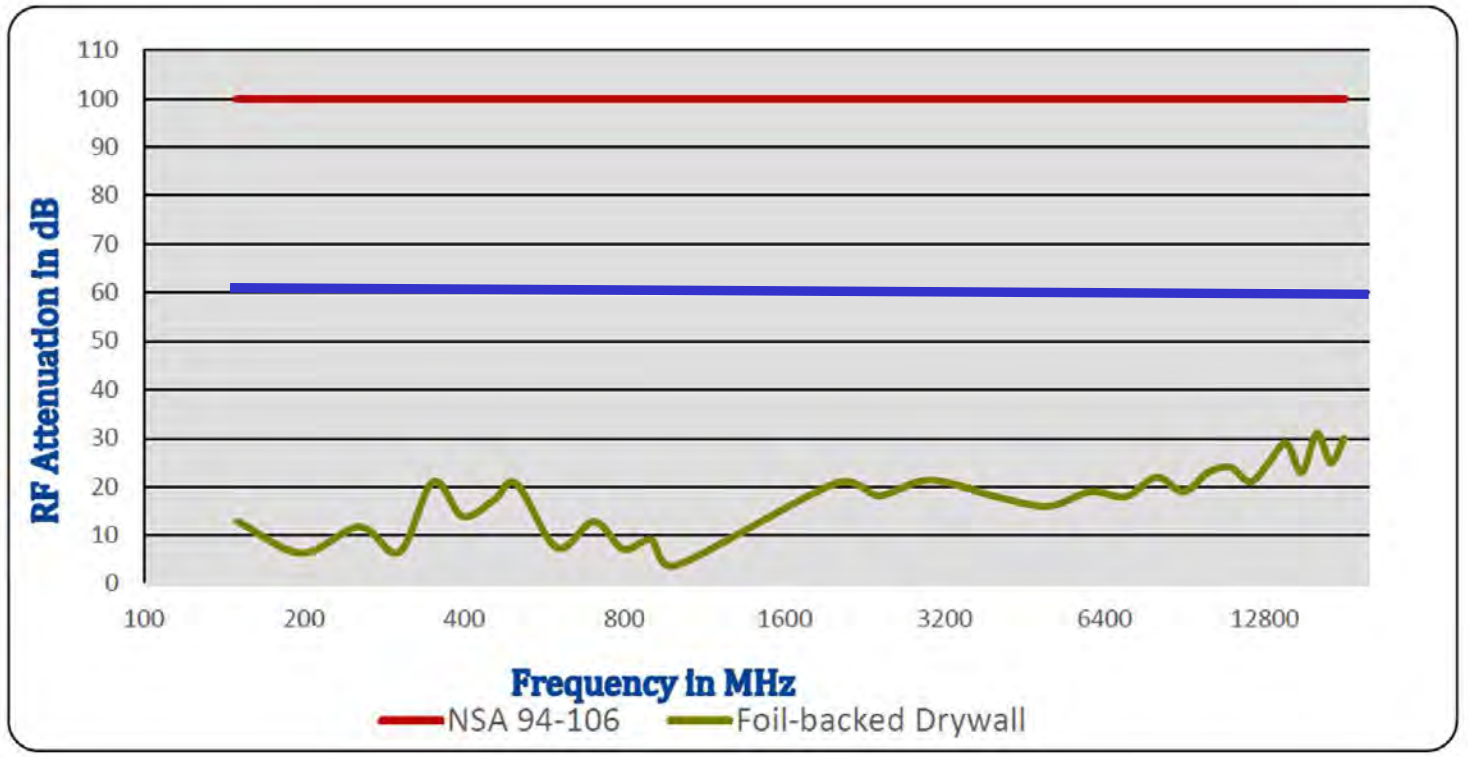
  - **Recommend furred out wall when shielding is required**
  - **Don’t forget ceiling, floor, penetrations, and connections. Remember, six-sided approach!**
  - **Completely shielded floor may not be required for slab on grade.**

NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

TEMPEST R-Foil

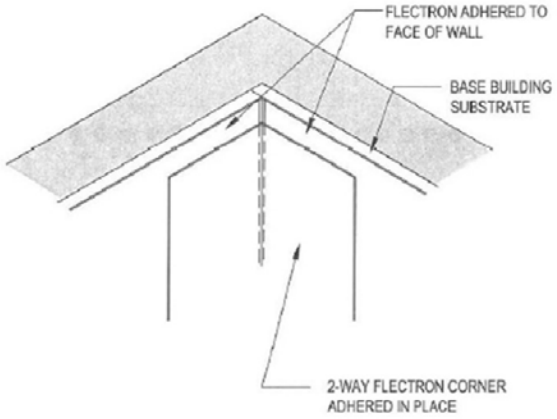
Repeated testing indicates very poor RF Shielding effectiveness with 1 Layer of foil backed gypsum wallboard

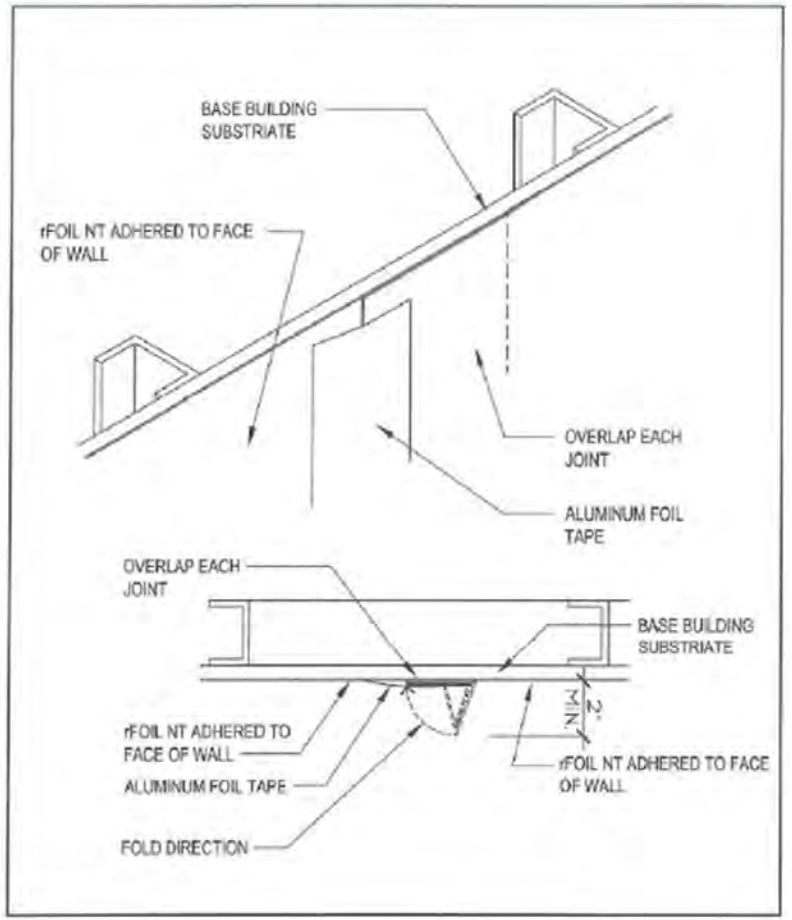


NAVFAC
Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

TEMPEST R-Foil



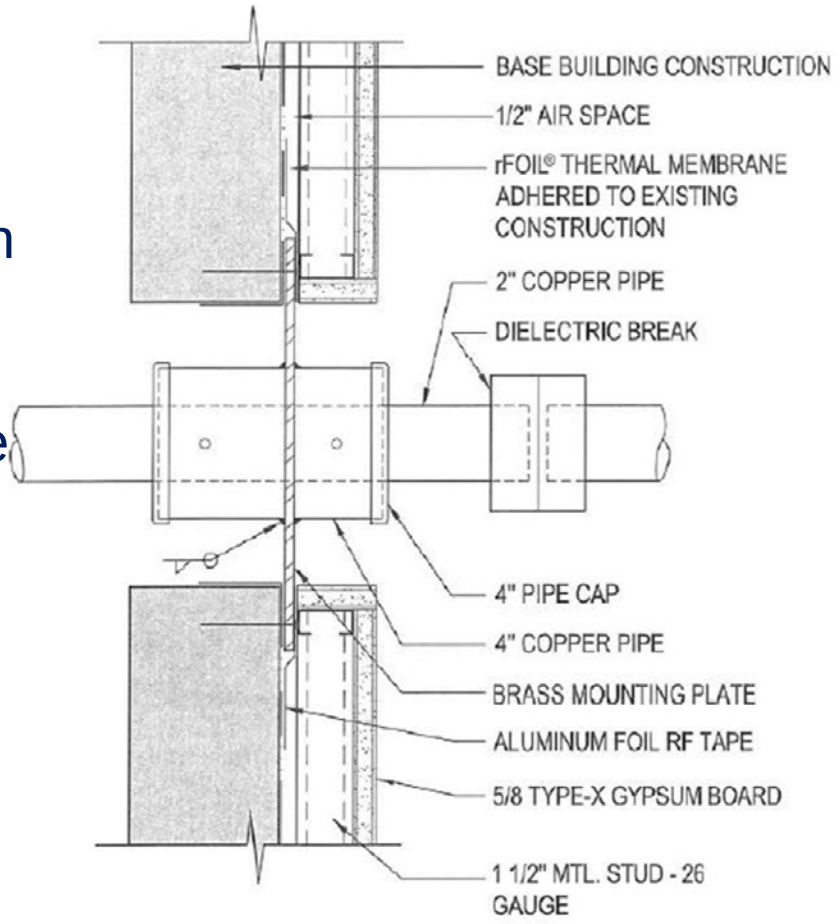


NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

TEMPEST Conductive Breaks

Piping must be RF sealed around the perimeter of the pipe where it penetrates the shielding material. To function as a waveguide, the pipe's length must be seven times its inside diameter to achieve waveguide-beyond-cutoff performance1.



NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

TEMPEST WaveGuides

WAVEGUIDES:
Any of a class of devices that confines and directs the propagation of electromagnetic waves, such as radio waves, infrared rays, and visible light.

Magnetic		*Electric*		*Planewave*		*Microwave*		
1 KHz	20 KHz	100 KHz	10 MHz	100 MHz	1 GHz	10 GHz	18GHz	40 GHz*
25 dB	120 dB	120 dB	120 dB	120 dB	120 dB	120 dB	120 dB	100 dB

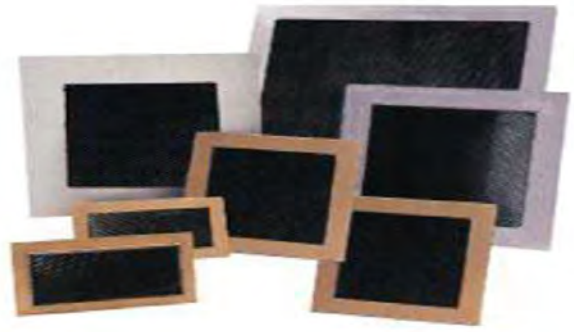
NAVFAC Naval Facilities Engineering Systems Command

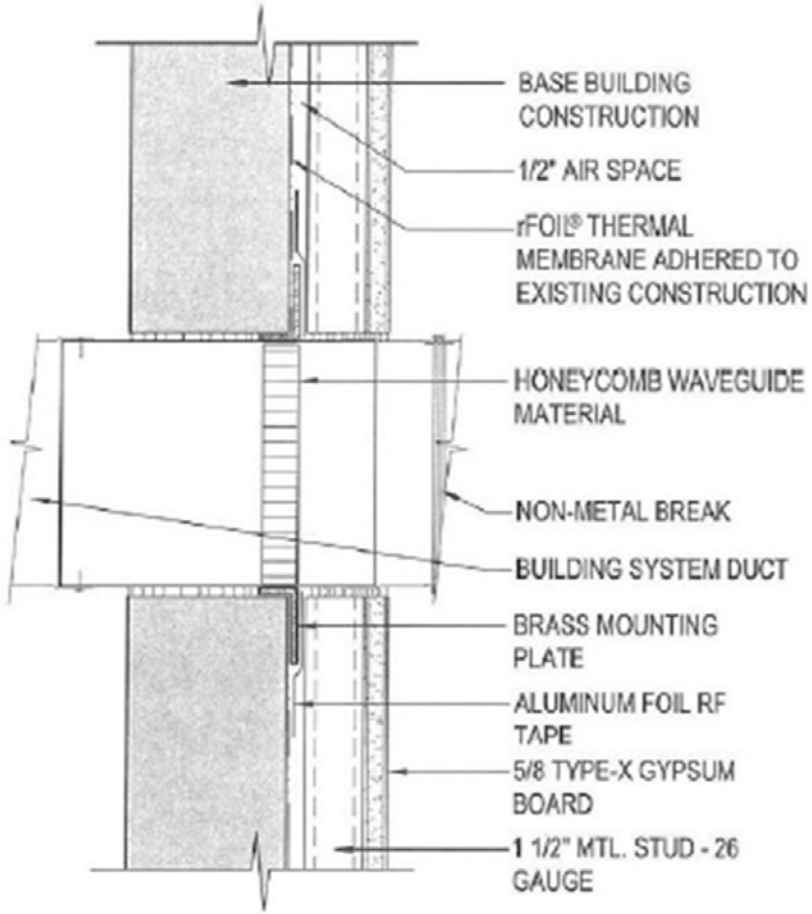
Specific Design Strategy: TEMPEST

TEMPEST WaveGuides

Honeycomb Vent:

In its most common form, it is constructed from steel or brass and hot solder plated. Sizes up to 2’ x 3’ are readily available. Provisions to attach ductwork usually takes the form of a flange located around the perimeter of the clear opening.

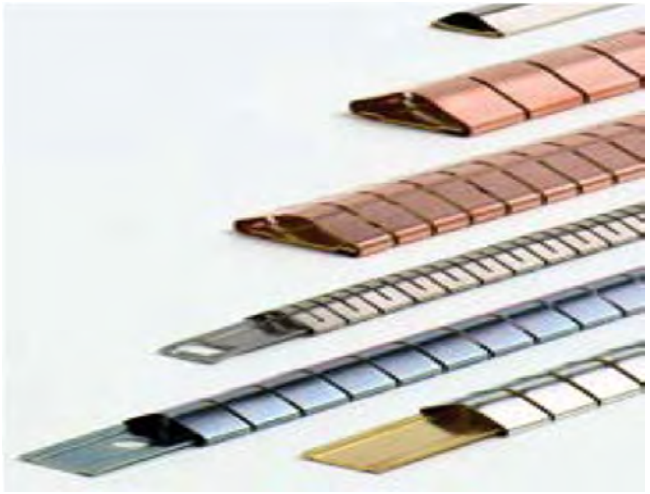




NAVFAC Naval Facilities Engineering Systems Command

Specific Design Strategy: TEMPEST

TEMPEST RF Gaskets



Maximum attenuation for all gaskets is achieved as compression force increases. The use of elastomer cores will extend the operating range. In applications where the gasket is permanently installed between two surfaces, compression set can be tolerated.

NAVFAC Naval Facilities Engineering Systems Command

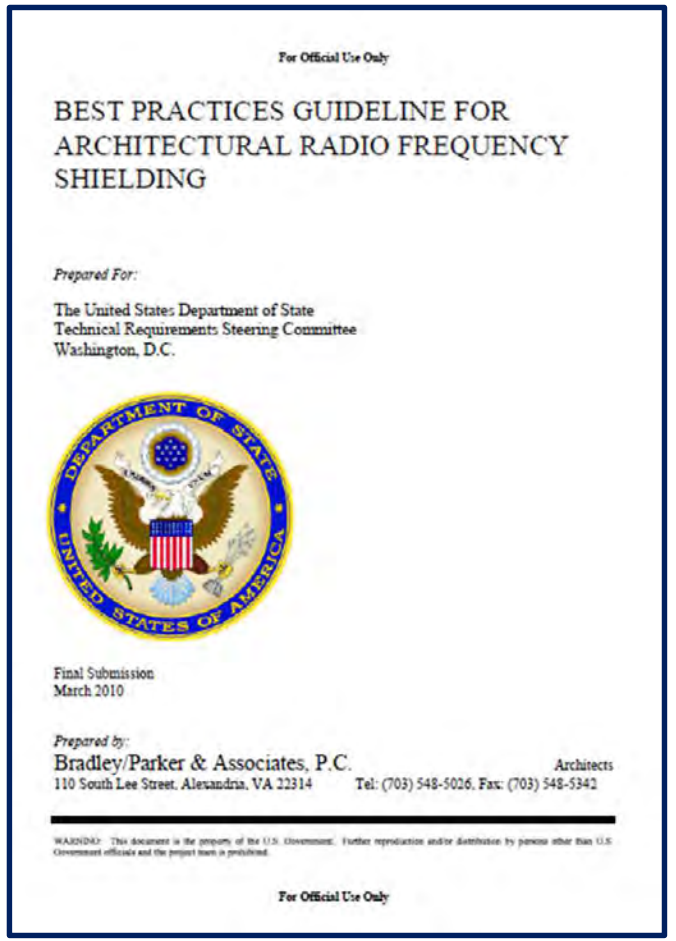
Specific Design Strategy: TEMPEST

- **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/SAPF, that means a signal distribution system containing unencrypted NSI that leaves the SCIF/SAPF.
- **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.

NAVFAC Naval Facilities Engineering Systems Command

BEST PRACTICES GUIDELINE FOR ARCHITECTURAL RADIO FREQUENCY SHIELDING FOUO

- **PURPOSE:**
  - Compendium of design standards, criteria, guidelines and supporting typical designs, design examples, generic specifications, details and product information for use as a ready reference in developing construction documents
- **PREPARING ACTIVITY:**
  - Bureau of Overseas Buildings Operations (USDOS/OBO).
  - The United States Department of State Technical Requirements Steering Committee Washington, D.C.
- **CURRENT DOCUMENT : FOUO**
  - Published March 2010



For Official Use Only

BEST PRACTICES GUIDELINE FOR ARCHITECTURAL RADIO FREQUENCY SHIELDING

Prepared For:

The United States Department of State
Technical Requirements Steering Committee
Washington, D.C.

Final Submission
March 2010

Prepared by:
Bradley/Parker & Associates, P.C. Architects
110 South Lee Street, Alexandria, VA 22314 Tel: (703) 548-5026, Fax: (703) 548-5342

WARNING: This document is the property of the U.S. Government. Further reproduction and/or distribution by persons other than U.S. Government officials and the project team is prohibited.

For Official Use Only

NAVFAC Naval Facilities Engineering Systems Command

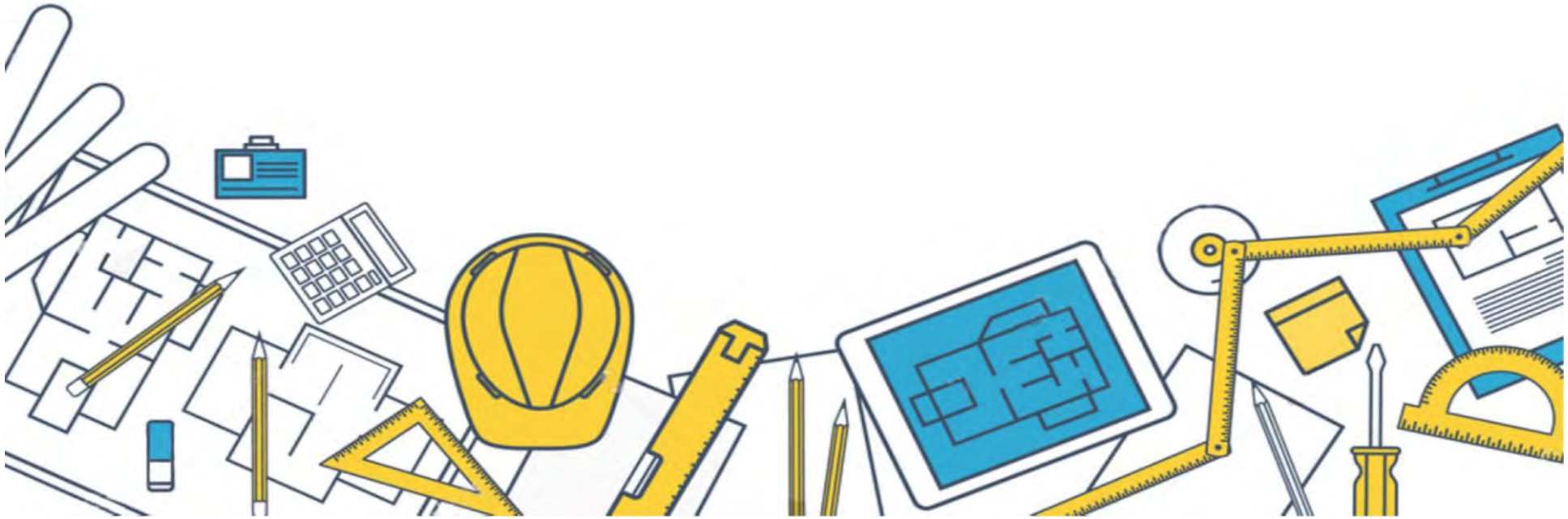
CNSSAM TEMPEST 1-13
RED / BLACK Installation Guidance

- **PURPOSE:**
  - – Provides criteria for the installation of electronic equipment, cabling, and facility support for the processing of secure information.
- **PREPARING ACTIVITY:**
  - Committee on National Security Systems Advisory Memorandum (CNSSAM) CNSS Secretariat (IE32) National Security Agency
- **CURRENT DOCUMENT : FOUO**
  - Published 17 Jan 2014

NAVFAC Naval Facilities Engineering Systems Command

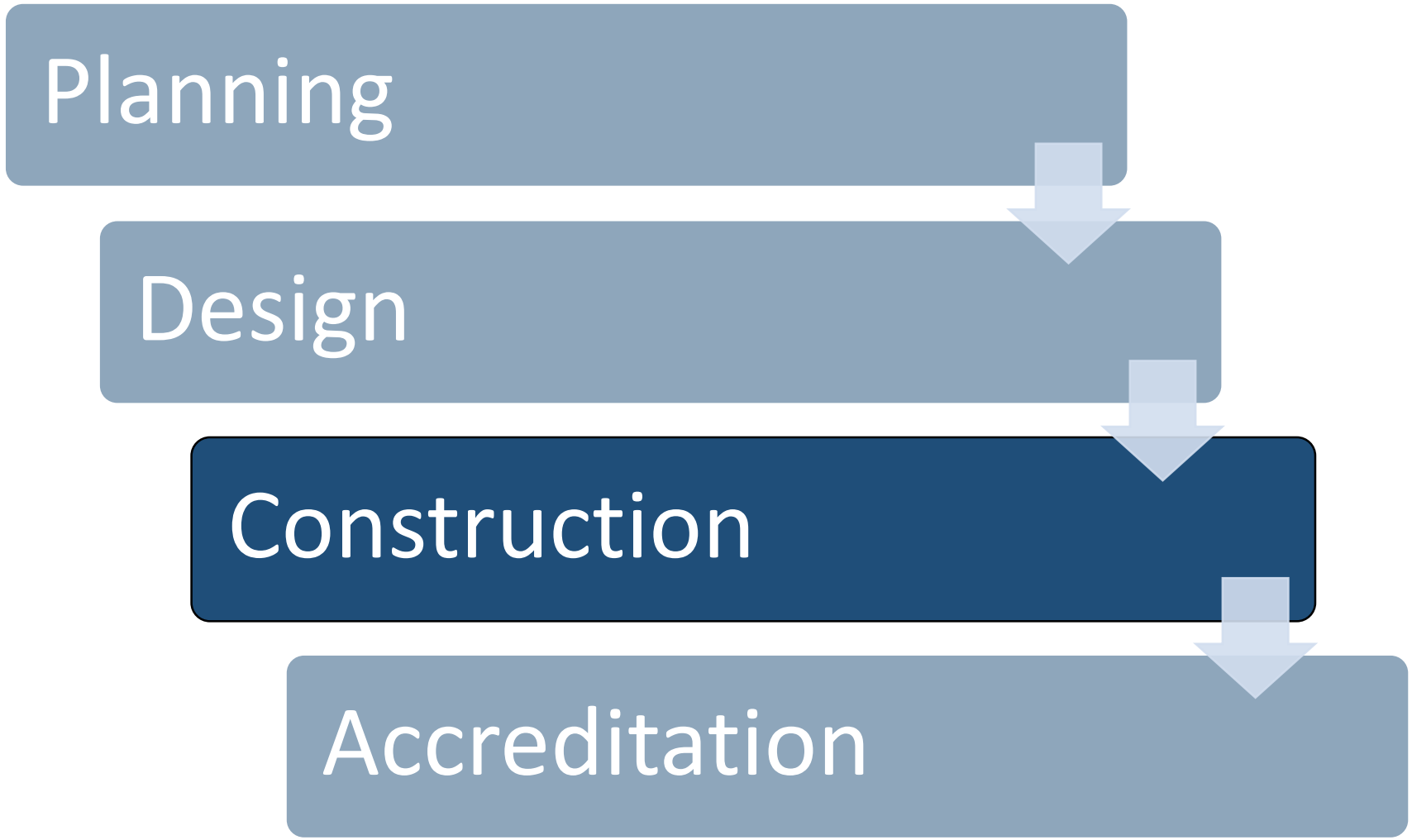
Design Approval

- **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.**



NAVFAC Naval Facilities Engineering Systems Command

Project Phases

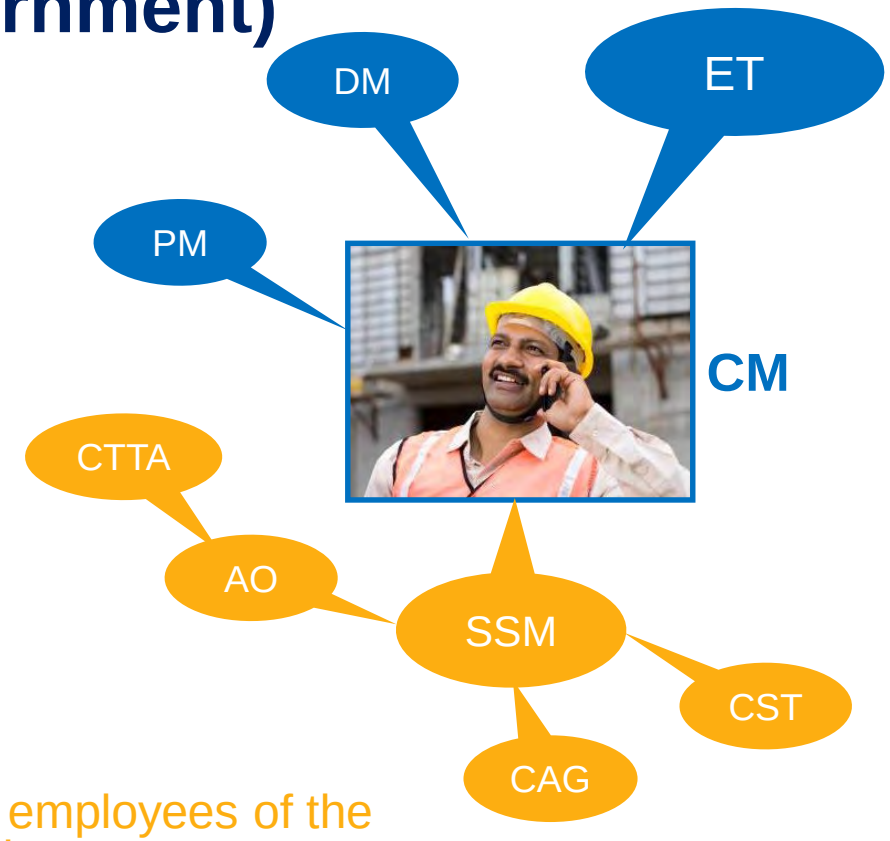


NAVFAC Naval Facilities Engineering Systems Command

SCIF and SAPF Construction

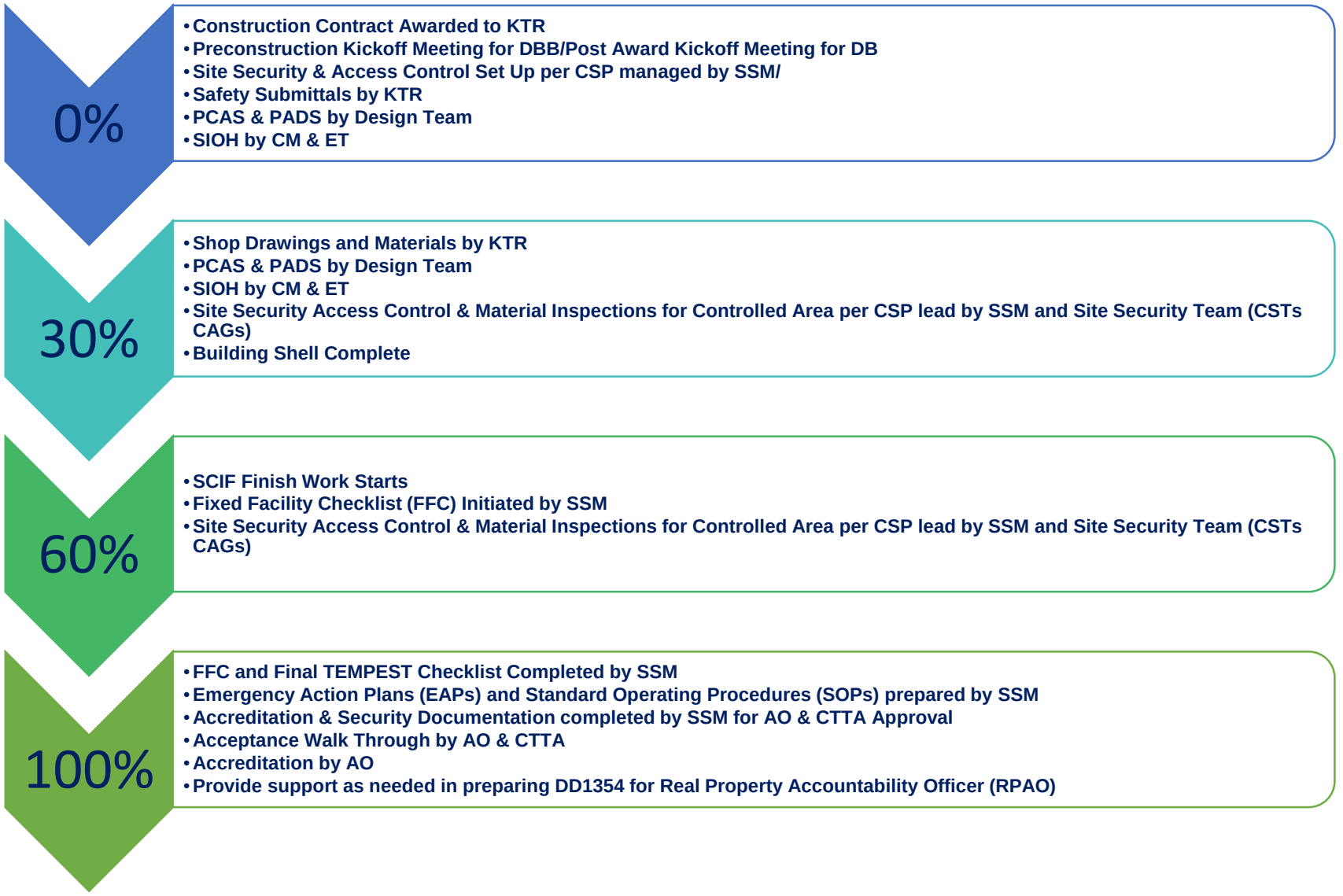
Construction Team Members (Government)

- **NAVFAC**
  - Construction Manager (CM)
  - Engineering Technician (ET)
  - Design Manager (DM)
  - Project Manger (PM)
- **Accreditation Authority**
  - Accrediting Official (AO)
  - Site Security Manager (SSM)
  - Certified TEMPEST Technical Authority (CTTA)
  - Construction Surveillance Technician (CST)
  - Cleared American Guards (CAG)
    - To avoid conflict of interest, above personnel cannot be employees of the construction contractor, employees of or contracted by the DoD construction agent



NAVFAC Naval Facilities Engineering Systems Command

SCIF/SAPF Lifecycle – Construction & Accreditation



NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1A - Construction

To be completed prior to construction start:										
Confirm Approved CSP construction personnel requirements for work including: - General Construction - Finish work - Outfitting (such as FF&E and ESS)			L				S		SSM is Lead with NAVFAC/DoD Construction Agent providing cost and schedule implications.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Confirm Approved CSP material purchasing, inspection, shipping, and SSA requirements including FF&E and ESS.			L				S		SSM is Lead with NAVFAC/DoD Construction Agent providing cost and schedule implications.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Confirm CSP requirements for site security including area/site access control for personnel, materials, and vehicles.			L				S		SSM is Lead with NAVFAC/DoD Construction Agent providing cost and schedule implications.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Conduct DB Post Award Kickoff (PAK) or DBB Pre-Construction Conference (PreCon). SSM must attend.			S	S		S	L		Discuss site security, schedule, site visits, inspections, construction personnel requirements, submittal requirements with contractor and SSM.	BMS B-1.5.5.1 BMS B-1.4.6.3 UFC 4-010-05
To be completed prior to completion of construction:										
Approved construction submittals are forwarded to SSM for inclusion in FFC.			S	S			L		CM responsible to forward approved submittals. SSM responsible for FFC	UFC 4-010-05
Construction is monitored and the CSP is adjusted as required.	S		L				S		SSM updates CSP and coordinates changes with the CM. AO must approve all changes.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 UFC 4-010-05

NAVFAC INST 4700.1A - Construction

Conduct the initial NAVFAC Red Zone (NRZ) meeting. Include inspections and acceptance testing in the critical activities			S	S			L		CM leads this effort and SSM must attend. Conducted approximately 75% prior to construction contract completion or six months prior to Beneficial Occupancy Date (BOD)	BMS B-1.6.11
Coordinate preliminary walkthrough with the SSM prior to substantial completion of space. Conduct periodic inspections of area to document and validate construction requirements			S				L		CM coordinates this effort working with the contractor and SSM	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Conduct final inspections and acceptance testing with the SSM in accordance with the NRZ critical activities.			S				L		CM coordinates this effort working with the contractor and SSM. As a subset to the final facility acceptance, the CM must coordinate with the SSM to insure the SCIF construction meets the requirements for accreditation.	DoDM 5101.21 Vol 2 IC Tech Spec ICD/ICS 705 UFC 4-010-05 BMS B-1.6.11
Document final acceptance of construction via DD-1354 Transfer and Acceptance of DoD Real Property and supporting documents.			S	S	S	S	L		A DD-1354 must be prepared and submitted by the construction agent and accepted by the Real Property Accountability Officer (RPAO) prior to acceptance and occupancy (sometimes identified as placed in service date or BOD). CM coordinates the facility acceptance with the RPAO. RPAO will complete the update to iNFADS property record card.	OPNAVINST 11010.20H, DoD FMR, UFC 1-300-08 DoDI 4165.14 and 4165.70 BMSs B-25.7.1.3 B-25.7.1.4.1 B-25.7.1.4.2 B-25.7.1.7

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1B (DRAFT) - Construction

To be completed prior to construction start:											
Confirm Approved CSP construction personnel requirements for work including: - General Construction - Finish work - Outfitting (such as FF&E and ESS)				L				S		SSM is Lead with NAVFAC/DoD Construction Agent providing cost and schedule implications.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Confirm Approved CSP material purchasing, inspection, shipping, and SSA requirements including FF&E and ESS.				L				S		SSM is Lead with NAVFAC/DoD Construction Agent providing cost and schedule implications.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Confirm CSP requirements for site security including area/site access control for personnel, materials, and vehicles.				L				S		SSM is Lead with NAVFAC/DoD Construction Agent providing cost and schedule implications.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05

DRAFT

NAVFAC Naval Facilities Engineering Systems Command

NAVFAC INST 4700.1B (DRAFT) - Construction

Conduct DB Post Award Kickoff (PAK) or DBB Pre-Construction Conference (PreCon). SSM must attend.				S	S		S	L		Discuss site security, schedule, site visits, inspections, construction personnel requirements, submittal requirements with contractor and SSM.	PDC-05.07 PDC-05.08 UFC 4-010-05
To be completed prior to completion of construction:											
Approved construction submittals are forwarded to SSM for inclusion in FFC.				S	S			L		CM responsible to forward approved submittals. SSM responsible for FFC	UFC 4-010-05
Construction is monitored and the CSP is adjusted as required.	S	S		L				S		SSM updates CSP and coordinates changes with the CM. Any changes must be incorporated into the CSP and submitted to the AO (SCIF)/SAO (SAPF), via SSO Navy/DON SAPCO, for review and approval.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Conduct the initial NAVFAC Red Zone (NRZ) meeting. Include inspections and acceptance testing in the critical activities				S	S			L		CM leads this effort and SSM must attend. Conducted approximately 75% prior to construction contract completion or six months prior to Beneficial Occupancy Date (BOD)	PDC-05.13
Coordinate preliminary walkthrough with the SSM prior to substantial completion of space. Conduct periodic inspections of area to document and validate construction requirements				S				L		CM coordinates this effort working with the contractor and SSM	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05
Conduct final inspections and acceptance testing with the SSM in accordance with the NRZ critical activities.				S				L		CM coordinates this effort working with the contractor and SSM. As a subset to the final facility acceptance, the CM must coordinate with the SSM to insure the SCIF construction meets the requirements for accreditation.	DoDM 5101.21 Vol 2 DoDM 5205.07 Vol 3 IC Tech Spec ICD/ICS 705 UFC 4-010-05 PDC-05.13
Document final acceptance of construction via DD-1354 Transfer and Acceptance of DoD Real Property and supporting documents.		S		S	S	S	S	L		A DD-1354 must be prepared and submitted by the construction agent and accepted by the Real Property Accountability Officer (RPAO) prior to acceptance and occupancy (sometimes identified as placed in service date or BOD). CM coordinates the facility acceptance with the RPAO. RPAO will complete the update to iNFADS property record card.	OPNAVINST 11010.20J DoD FMR UFC 1-300-08 DoDI 4165.14 and 4165.70 BMS (PDC) PW-04-40.02 PDC-05.15 PDC-05.23 PW-04-40.04

DRAFT

NAVFAC Naval Facilities Engineering Systems Command

Construction Security Plan (CSP)
Final

- 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 final CSP must be submitted to the AO/SAO 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 (CREQ).**

NAVFAC Naval Facilities Engineering Systems Command

Construction Security Plan (CSP)

Contract Award

- **For DBB projects:**
  - Do not award a construction contract without AO/SAO approved CSP.
- **For DB projects:**
  - An approved preliminary CSP is required for construction contract award.
  - Do not start onsite construction activities (excluding mobilization, demolition, clearing and grubbing) without AO/SAO approved final CSP.

NAVFAC Naval Facilities Engineering Systems Command

Contract Delivery Options

Design-Bid-Build (DBB)

- Must be used when entire facility is a SCIF
- Preferred delivery type and first consideration when project is located outside the U.S. or when a major portion of new facility is a SCIF
- DDB allows Construction Security Plan (CSP) requirements to be finalized and the requirements inserted into construction contract

Design-Build (DB)

- CSP requirements must be established without a final design in order to include in RFP.

NAVFAC Naval Facilities Engineering Systems Command

Site Security Manager (SSM)

DURING CONSTRUCTION:

- **Primary Point of Contact for security requirements:**
  - **Validates construction personnel requirements for work including:**
    - General secure area Construction
    - Finish work- Outfitting (such as Furniture, Fixtures and Equipment (FF&E) and Electronic Security Systems *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.

NAVFAC Naval Facilities Engineering Systems Command

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.**

NAVFAC Naval Facilities Engineering Systems Command

Construction Site 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.
  - o SSM will verify information provided on construction personnel.
  - o 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.
  - o Physical security barriers shall be erected to deny unauthorized access to the controlled areas.
  - o Cell phones may be prohibited.

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC
Naval Facilities Engineering Systems Command

Construction Security Surveillance

- **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.

NAVFAC Naval Facilities Engineering Systems Command

Construction Security Surveillance

- **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.**

NAVFAC Naval Facilities Engineering Systems Command

Construction Security 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.**
- **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.**

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

Construction: Quality Management

Required SCIF/SAPF Inspections (Per UFGS 01 45 00 – Quality Control)

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

NAVFAC Naval Facilities Engineering Systems Command

Periodic Inspections

- **What are Periodic Inspection**
  - Regular inspections performed a minimum of once every two weeksby QC Manager focusing on SCIF/SAPF perimeter construction
  - Performed jointly with QC Manager, ET, and Site Security Manager
  - Inspection frequency increases to weekly within 30 days of planned acceptance testing
  - Performed with specific emphasis on the construction of the secure area perimeter focus on sound rated assemblies, perimeter penetrations, perimeter doors, electronic security system, man-bar installation, inspection ports and TEMPEST countermeasures
  - Inspections documented in daily QC Report

NAVFAC Naval Facilities Engineering Systems Command

Periodic Inspections

- **Perimeter construction**
  - Wall goes from floor slab (true floor) to underside of floor or roof deck (true ceiling)
  - Acoustic insulation is securely fastened
  - Top and bottom of walls are sealed (both sides) with acoustical foam or sealant
  - Wall uniformly finished and painted from true floor to true ceiling

Check the metal thickness! All perimeter metal partitions must be a minimum 16 gauge (54 mil)

NAVFAC Naval Facilities Engineering Systems Command

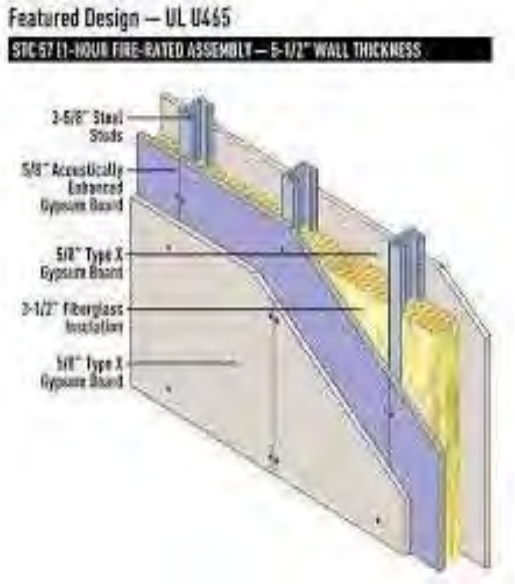
Periodic Inspections

- **Gypsum Wallboard installation**
  - Standard STC 45 wall has 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).
  - Standard STC 50 wall indicates four layers. Two layers on the uncontrolled side (outside) of the protected area and two layers on the controlled side (interior).
  - UFGS 09 29 00 GYPSUM BOARD requires submittal for sound rated assemblies that includes material and installation instructions.

NAVFAC Naval Facilities Engineering Systems Command

Periodic Inspections

- GWB Installation
  - 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



Enhanced Wall

- Three-quarter inch mesh, # 9 (10 gauge) expanded metal

Periodic Inspections

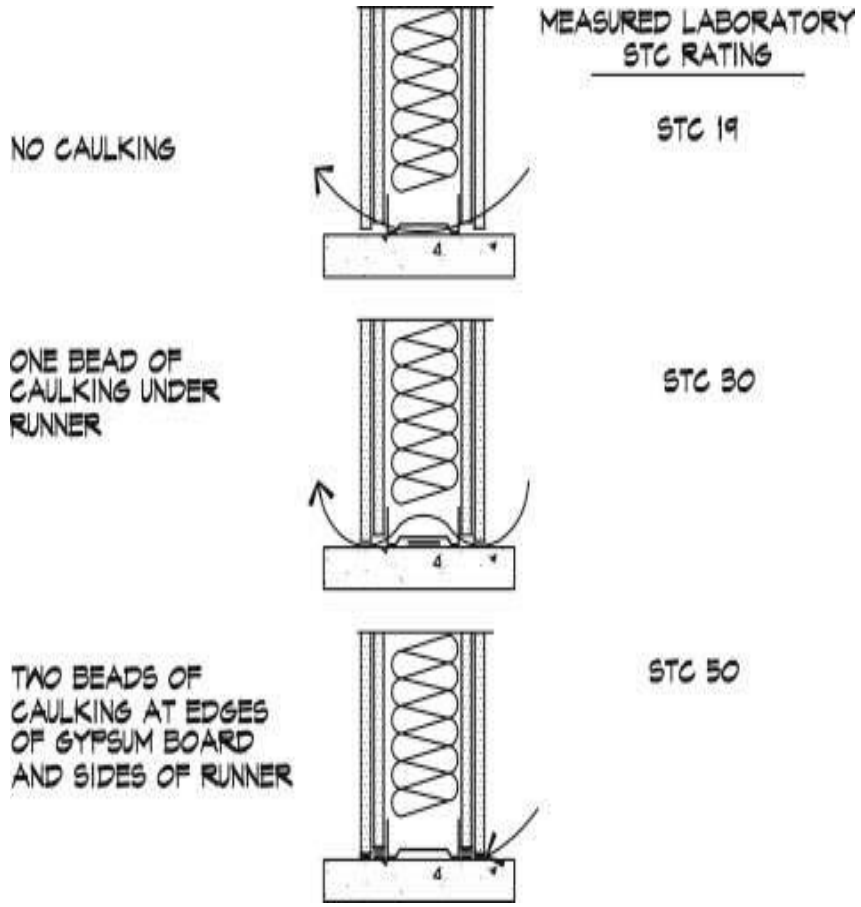
- **RF mitigation shall be provided at the direction of the CTTA when electronic processing does not provide adequate RF mitigation.**
  - **Provide foil backed GWB or R-Foil in accordance with *Best Practices Guideline for Architectural Radio Frequency Shielding*.**
    - **The use of R-foil or aluminum 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.**
    - **Stagger joints**

NAVFAC Naval Facilities Engineering Systems Command

Periodic Inspections

- Partition Sealants
  - 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)

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



Periodic Inspections

Utilities @ Perimeter

- Examples: Power, telecommunications, signal, plumbing
- Surface mounted to maintain perimeter acoustical partition rating and minimize RF shielding penetrations (where RF shielding is required)

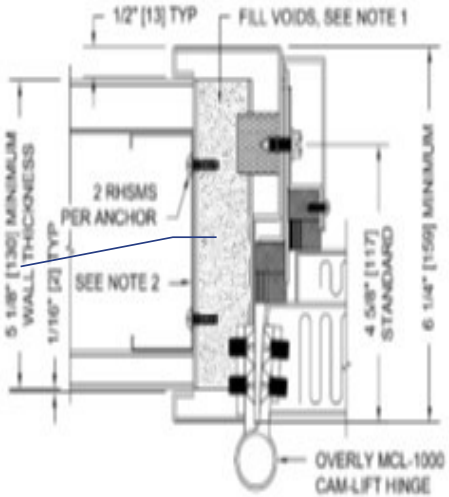
Utility can be recessed into a furred wall Furred wall terminates at false ceiling

- GWB can be 3/8” thick

Periodic Inspections

- UFGS 08 34 73 Sound Control Door Assemblies requires:
  - ASTM E 90 laboratory Test Report
  - ASTM E 336 field Test Report
- Fill jamb with acoustical insulation or sound deadening material
- Door assemblies sealed with acoustical foam or sealant (both sides) and finished to match wall
- Door hardware (locks, closers, and hinges)

Due to weight of acoustical doors – steel structure components must be used for door anchorage

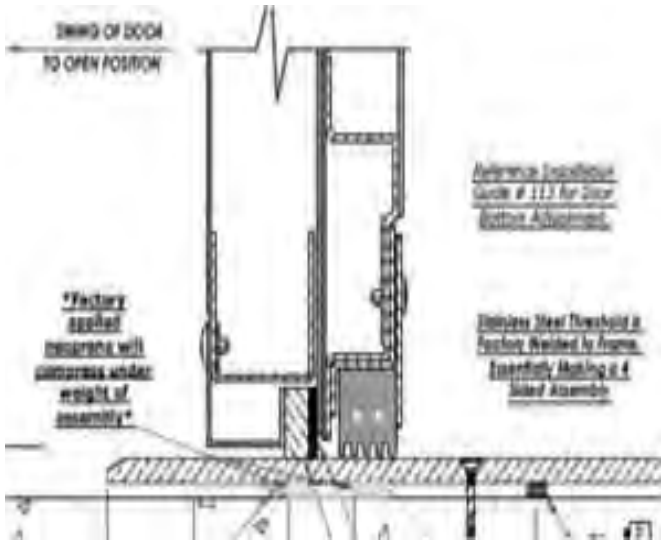


- Do not grout fill
- Fill jamb with acoustical insulation or sound deadening material

Periodic Inspections

RF Shielded Doors

- Doors come pre-assembled (Frames, door leaf(s), hardware)
- Special gasket / weatherstripping to ensure continuity of shielding when closed
- Look at door system submittal
- Knife edge difficult to meet accessibility requirements at sill
- Pneumatic types typically meet egress requirements



Knife Edge Door:
Not ABA Compliant

Periodic Inspections

Perimeter Penetrations

- Sealed (both sides) with acoustical foam or sealant
- Finished to match wall
- Metallic penetrations at perimeter (non- conductive break or grounded at the interior perimeter)
- Man-bar installation
- Inspection ports

NOTE!

- Utilities servicing areas other than the SCIF/SAPF cannot transit through the SCIF/SAPF without AO approval
- Single point entry for electrical
- Conduits for expansion can be done if filled with acoustical sealant and capped.

Periodic Inspections

- **The minimum TEMPEST Countermeasure is the 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.**
  - **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

NAVFAC Naval Facilities Engineering Systems Command

Periodic Inspections

- **Other TEMPEST Countermeasures documented in TCR.**
  - **RF Shielding**
    - » RF shielding protects the space from compromising emanations. When directed, provide RF mitigation for walls, ceilings, floors, and all penetrations including doors and windows. RF mitigation may also include waveguides, power line and telecommunication line filters.
  - **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.

NAVFAC Naval Facilities Engineering Systems Command

Required SCIF/SAPF Inspections
Preliminary Inspections

- What is Preliminary Inspection
  - Performed jointly by the QC Manager, ET, and Site Security Manager after construction is complete prior to acceptance testing
  - Requires (14) calendar day advance notification from contractor
  - Includes acceptance testing for Sound Attenuation for doors, perimeter walls (when required) and Electronic Security Systems
  - Contractor must document deficiencies and compile a Government punch list including estimated completion dates for each punch list item, and deficiencies must be corrected before scheduling a Final Acceptance Inspection

NAVFAC Naval Facilities Engineering Systems Command

Required SCIF/SAPF Inspections

➢ Acceptance Testing for Sound Attenuation

- Performed by construction contractor as part of Preliminary Testing and witnessed by Site Security Manager and Government ET or CM
- Testing performed in accordance with ASTM E336 as required by:
  - UFGS 08 34 73 SOUND CONTROL DOOR ASSEMBLIES
  - UFGS 09 29 00 GYPSUM BOARD (field testing when required)
- Deficiencies identified must be included in the Government SCIF/SAPF punch list and corrected prior to the Final Inspection
- Failure to successfully test sound attenuation will prevent accreditation and require mitigation
  - Rework
  - Last resort: customer funded sound generators

NAVFAC Naval Facilities Engineering Systems Command

Required SCIF/SAPF Inspections

➢ Acceptance Testing for Electronic Security Systems

- Performed by construction contractor as part of Preliminary Testing and witnessed by Site Security Manager and Government ET or CM
- Testing performed in accordance with:
  - UFGS 28 08 00 ELECTRONIC SECURITY SYSTEM ACCEPTANCE TESTING
  - Approved ESS Test Plan
- Deficiencies identified must be included in the Government SCIF/SAPF punch list and corrected prior to the Final Inspection
- Failure to successfully test electronic security systems will prevent accreditation and require mitigation.
  - Rework

NAVFAC Naval Facilities Engineering Systems Command

Required SCIF/SAPF Inspections

➢ Final Inspection

- Performed only after all required acceptance testing is complete and deficiencies corrected
- Requires (14) calendar day advance notification from contractor
- Final SCIF/SAPF Inspection should be performed separately from the Final inspection of the rest of the facility unless entire facility is SCIF/SAPF
- Contractor attendees include QC Manager and Superintendent
- Government attendees include ET, CM, and Site Security Manager. Other representatives may also attend.

NAVFAC Naval Facilities Engineering Systems Command

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

NAVFAC Naval Facilities Engineering Systems Command

Construction: Lessons Learned

- **Acoustic insulation is securely fastened**

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

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**

NAVFAC Naval Facilities Engineering Systems Command

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?

NAVFAC Naval Facilities Engineering Systems Command

Construction: Lessons Learned

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

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

NAVFAC Naval Facilities Engineering Systems Command

Construction: Lessons Learned

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

NAVFAC Naval Facilities Engineering Systems Command

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.

NAVFAC Naval Facilities Engineering Systems Command

Construction: Lessons Learned

- Duct openings that penetrate the SCIF/SAPF perimeter wall and exceed 96 in^2 must be protected
  - If one dimension of the penetration measures less than 6 inches, bars or grills are not required.

  - Protection could be:
    - Manbars
    - Metal Grill
    - Welded Wire Fabric
    - Metal Sound Baffle
    - Waveguide

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

NAVFAC Naval Facilities Engineering Systems Command

Construction: Lessons Learned

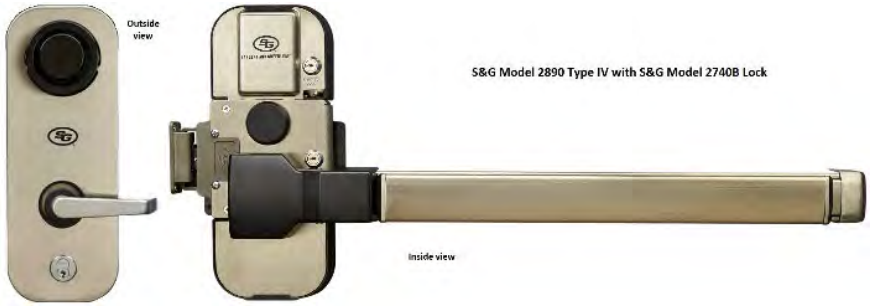
- Duct openings that penetrate the SCIF/SAPF perimeter wall and exceed 96 in^2 must be protected
  - If one dimension of the penetration measures less than 6 inches, bars or grills are not required.

  - Protection could be:
    - Manbars
    - Metal Grill
    - Welded Wire Fabric
    - Metal Sound Baffle
    - Waveguide

Construction: Lessons Learned

Primary Entry Door

- Deadlocking panic hardware (FF-L-2890)
- Combination lock meeting Federal Specification FF-L 2740A
- Equipped with a key override in the event of a malfunction or loss of power to the automated access control device.
- Recessed Personal Electronic Device (PED) cabinets are prohibited on perimeter walls.
- PED cabinets cannot be located within 10 ft. (3 m) of equipment processing unencrypted NSI.



NAVFAC Naval Facilities Engineering Systems Command

Construction: Lessons Learned

Quality Verification

- Emergency Exit Doors
  - Exterior hardware is prohibited
  - Deadlocking panic hardware
  - Alarmed 24/7 with local annunciation

NAVFAC Naval Facilities Engineering Systems Command

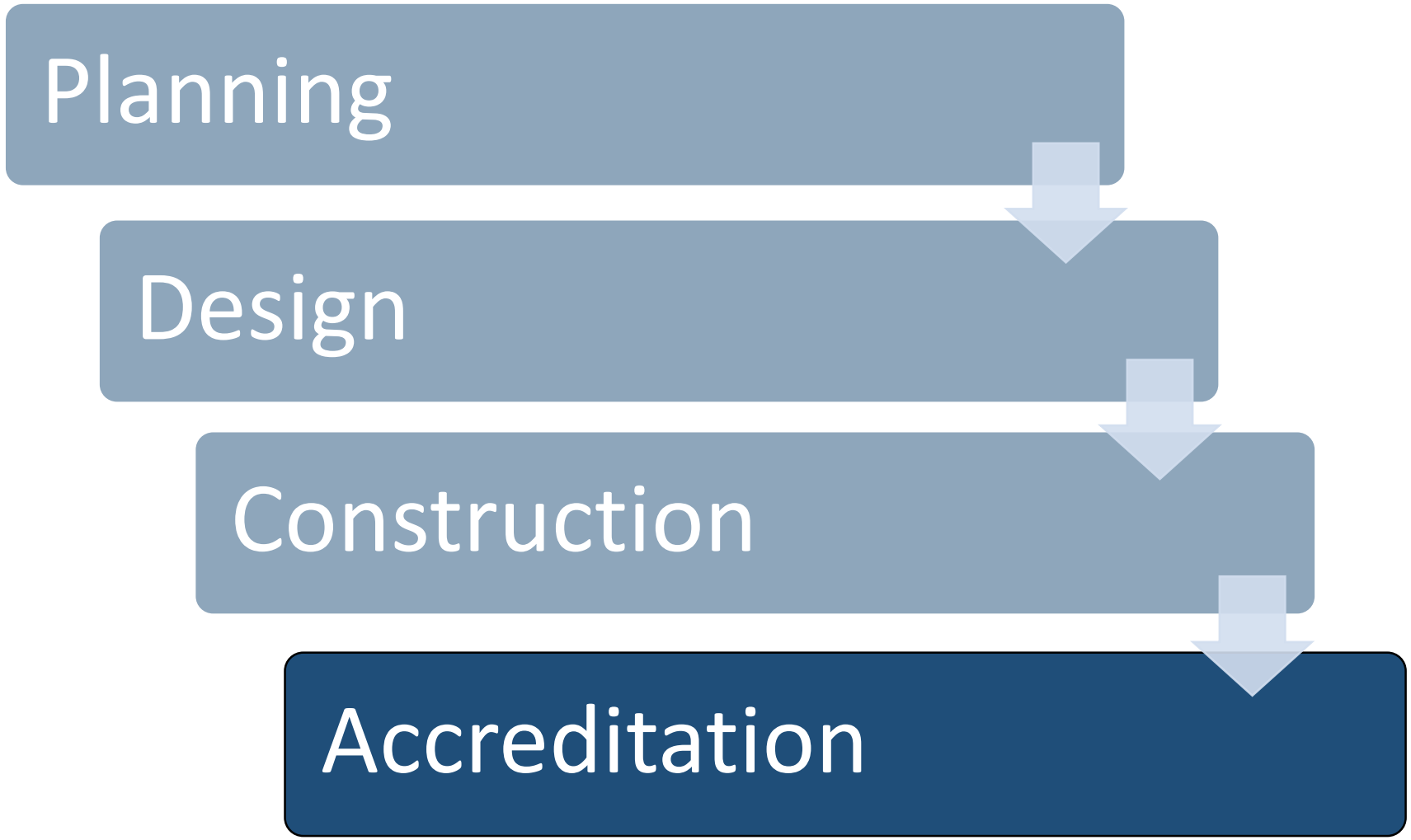
Construction: Lessons Learned

Summary

- ✓ Ensure SSM and QC perform joint Quality Control inspections
- ✓ Ensure acceptance testing is performed as required
- ✓ Wall are finished and painted and go from true floor to true ceiling.
- ✓ Gaps around penetration in perimeter walls are prohibited
- ✓ Excess penetrations in perimeter walls must be avoided
- ✓ Large ducts penetrating perimeter may require physical protection such as manbars
- ✓ Access panels that permit visual inspections of duct are required on underside of ducting
- ✓ Emergency exit doors must not have exterior hardware

NAVFAC Naval Facilities Engineering Systems Command

Project Phases



NAVFAC Naval Facilities Engineering Systems Command

Accreditation Cycle

- **ISC 705-2 provides accreditation policy requirements.**
  - **Inspections and evaluations are performed by the AO/SAO, or designee (SSM), prior to initial accreditation.**
  - **The accreditation includes a review of documents relating to design and construction and include**
    - Fixed Facility Checklist (FFC)
    - Standard Operating Procedures (SOP)
    - Emergency Action Plan (EAP)
    - CSP
    - TCR/Verification of Countermeasures by CTTA
    - Technical Surveillance Countermeasures (TSCM) review conducted by trained TSCM professionals, when deemed necessary by the AO
- **To facilitate this process, Project/Construction Managers shall provide the AO/SAO/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.**

NAVFAC Naval Facilities Engineering Systems Command

Accreditation Cycle

- **Upon construction completion a Final Fixed Facility Checklist (FFC)/drawings and TEMPEST package must be submitted to SSO Navy via the supporting RCSA.**
- **RSSO reviews submitted documentation and works with local SSO/SSR to schedule an accreditation inspection.**
- **The following 3 documents pertains to facility accreditation and system approvals must be completed prior to commencing SCIF operations.**
  - **Facility Physical Security Accreditation (DIA)**
  - **TEMPEST Accreditation (DIA Certified TEMPEST Technical Authority (CTTA))**
  - **SCI Systems Approval To Operate (ATO) (System Designated Approval Authority (DAA))**

Unclassified

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

NAVFAC Naval Facilities Engineering Systems Command

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**

NAVFAC Naval Facilities Engineering Systems Command

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

NAVFAC Naval Facilities Engineering Systems Command

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**

NAVFAC Naval Facilities Engineering Systems Command

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))**

NAVFAC Naval Facilities Engineering Systems Command

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**

NAVFAC Naval Facilities Engineering Systems Command

Accreditation Cycle

- The SSO/PSO or SSM will document the construction of the SCIF with photos, floor plans, diagrams, CSP, etc. During this time Cognizant Security Authority (CSA) representatives may conduct a site visit if requested.
- Once construction has been completed submit the final accreditation package (the updated CSP, FFC, and TEMPEST form B) to the CSA for review. Once complete, the RCSA will forward the SCIF accreditation package to AO via CSA for final accreditation.
- A Pre-Accreditation Inspection may be conducted by an CSA representative.
- The final Physical and TEMPEST accreditation messages will be issued by AO.

NAVFAC Naval Facilities Engineering Systems Command

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!”
- When a command states they require a SCIF or SAPF
  - First Question: Do you have Concept Approval?
  - Second Question: Who is your designated SSM?
  - Third question: Are they working on the CSP?
  - Fourth question: What are the TEMPEST requirements?

NAVFAC Naval Facilities Engineering Systems Command

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**

NAVFAC Naval Facilities Engineering Systems Command

Take Away

- **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.**

NAVFAC Naval Facilities Engineering Systems Command

Knowledge Check Questions

5 Questions

NAVFAC Naval Facilities Engineering Systems Command

Knowledge Check Questions

Question #1

(1) Who is responsible for preparing the Construction Security Plan (CSP)?

A. Construction Manager

B. Construction Contractor

C. Site Security Manager

D. Accrediting Official

Knowledge Check Questions

Question #2

(2) When is it acceptable for either the Construction Manager (CM) or Contractor Superintendent to also serve as the Site Security Manager (SSM)?

A. Never

B. When appointed by the Accrediting Official

C. When delegated by the Site Security Manager

D. When the project is outside the U.S.

Knowledge Check Questions

Question #3

(3) Where are the contract requirements located for SCIF/SAPF Quality Control inspections?

A. UFC 4-010-05 Sensitive Compartmented Information Facilities Planning, Design and Construction

B. ICD/IDS 705 Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities

C. B-1.4.4.3 Construction Quality Management

D. UFGS 01 45 00.00 20 and UFGS 01 45 00.05 20

NAVFAC Naval Facilities Engineering Systems Command

Knowledge Check Questions

Question #4

(4) Changes made to the Construction Security Plan (CSP) after award could potentially lead to a contract modification resulting is additional time and money.

A. True

B. False

Knowledge Check Questions

Question #5

(5) When required, who is responsible for the Construction Surveillance Technicians?

A. Construction Contractor

B. Site Security Manager

C. NAVFAC

D. Installation Commander

QUESTIONS?

Thanks!

NAVFAC PDCC:

John Lynch, PE
john.j.lynch8.civ@us.navy.mil
(757) 322-4207

Julie Heup, PE
julie.m.heup.civ@us.navy.mil
(757) 322-4447

NAVFAC
Naval Facilities Engineering Systems Command