

# UNIFIED FACILITIES CRITERIA (UFC)

---

## SCIF/SAPF PLANNING, DESIGN, AND CONSTRUCTION



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

*This Page Intentionally Left Blank*

**UNIFIED FACILITIES CRITERIA (UFC)**  
**SCIF/SAPF**  
**PLANNING, DESIGN, AND CONSTRUCTION**

Any copyrighted material included in this UFC is identified at its point of use.  
Use of the copyrighted material apart from this UFC must have the permission of the  
copyright holder.

Indicate the preparing activity beside the Service responsible for preparing the document.

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

Record of Changes (changes are indicated by \1\ ... /1/)

<b>Change No.</b>	<b>Date</b>	<b>Location</b>

*This Page Intentionally Left Blank*

## FOREWORD

The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with [USD \(AT&L\) Memorandum](#) dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate. All construction outside of the United States, its territories, and possessions is also governed by Status of Forces Agreements (SOFA), Host Nation Funded Construction Agreements (HNFA), and in some instances, Bilateral Infrastructure Agreements (BIA). Therefore, the acquisition team must ensure compliance with the most stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.

UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Military Department's responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Systems Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC) are responsible for administration of the UFC system. Technical content of UFC is the responsibility of the cognizant DoD working group. Defense Agencies should contact the respective DoD Working Group for document interpretation and improvements. Recommended changes with supporting rationale may be sent to the respective DoD working group by submitting a Criteria Change Request (CCR) via the Internet site listed below.

UFC are effective upon issuance and are distributed only in electronic media from the following source:

- Whole Building Design Guide website <https://www.wbdg.org/ffc/dod>.

Refer to UFC 1-200-01, *DoD Building Code*, for implementation of new issuances on projects.

### AUTHORIZED BY:



---

PETE G. PEREZ, P.E., SES  
Chief, Engineering and Construction  
U.S. Army Corps of Engineers



---

R. DAVID CURFMAN, P.E., SES  
Chief Engineer  
Naval Facilities Engineering Systems Command



---

DAVID H. DENTINO, SES  
Deputy Director of Civil Engineers  
DCS/Logistics, Engineering &  
Force Protection (HAF/A4C)  
HQ United States Air Force



---

MICHAEL McANDREW, SES  
Deputy Assistant Secretary of Defense  
(Construction)  
Office of the Secretary of Defense

*This Page Intentionally Left Blank*

## TABLE OF CONTENTS

<b>CHAPTER 1 INTRODUCTION</b> .....	<b>1</b>
<b>1-1 PURPOSE AND SCOPE</b> .....	<b>1</b>
<b>1-2 REISSUES AND CANCELS</b> .....	<b>1</b>
<b>1-3 APPLICABILITY</b> .....	<b>1</b>
1-3.1 SCIF. ....	1
1-3.2 SAPF. ....	1
<b>1-4 GLOSSARY</b> .....	<b>1</b>
<b>1-5 REFERENCES</b> . ....	<b>1</b>
<b>1-6 POLICY</b> . ....	<b>1</b>
1-6.1 Office of the Director of National Intelligence.....	2
1-6.2 Department of Defense.....	2
<b>1-7 REGULATORY AUTHORITY</b> .....	<b>2</b>
1-7.1 DoD SCIF Authorities. ....	2
1-7.2 Non-DoD SCIF Authorities.....	2
1-7.3 DoD SAPF Authorities. ....	2
<b>1-8 IMPLEMENTATION</b> .....	<b>3</b>
1-8.1 Department of Navy.....	3
1-8.2 Department of the Army.....	3
1-8.3 Department of the Air Force.....	3
<b>1-9 GENERAL BUILDING REQUIREMENTS</b> . ....	<b>3</b>
<b>1-10 CYBERSECURITY</b> . ....	<b>3</b>
1-10.1 Mission Critical Facility-Related Control Systems.....	4
<b>1-11 FACILITY CLASSIFICATION</b> .....	<b>4</b>
1-11.1 Secure Working Area (SWA) or SAP Working Area (SAPWA).....	4
1-11.2 Temporary Secure Working Area (TSWA) or Temporary SAP Working Area (TSAPWA).....	4
1-11.3 Temporary SCIF (T-SCIF) or Temporary SAPF (T-SAPF).....	4
1-11.4 Closed Storage. ....	4
1-11.5 Open Storage. ....	4
1-11.6 Continuous Operation.....	4
<b>1-12 SECURITY IN DEPTH</b> .....	<b>4</b>
<b>1-13 SECURITY REQUIREMENTS</b> .....	<b>5</b>

<b>1-14</b>	<b>SITE SECURITY MANAGER (SSM).</b> .....	<b>5</b>
<b>1-15</b>	<b>CONSTRUCTION SECURITY PLAN (CSP).</b> .....	<b>5</b>
<b>1-16</b>	<b>INFORMATION SECURITY.</b> .....	<b>6</b>
1-16.1	SCIF Location and Identity.....	6
1-16.2	SAPF Location and Identity. ....	6
1-16.3	TEMPEST Vulnerabilities and Recommended Countermeasures. ....	6
1-16.4	Security Environment Threat List (SETL) Information.....	6
<b>1-17</b>	<b>DESIGN SECURITY.</b> .....	<b>6</b>
<b>1-18</b>	<b>CONSTRUCTION SECURITY.</b> .....	<b>6</b>
1-18.1	Within the United States. ....	7
1-18.2	Outside the United States. ....	7
<b>1-19</b>	<b>ACCREDITATION.</b> .....	<b>7</b>
1-19.1	Accreditation Process. ....	8
1-19.2	Fixed Facility Checklist (FFC). ....	8
1-19.3	TEMPEST Addendum. ....	8
1-19.4	Pre-Construction Checklist. ....	8
<b>1-20</b>	<b>HISTORIC PRESERVATION COMPLIANCE.</b> .....	<b>8</b>
1-20.1	Security and Stewardship. ....	9
1-20.2	Compliance with Laws. ....	9
1-20.3	Compliance with DoD Standards. ....	9
<b>1-21</b>	<b>SECURITY ENGINEERING UFC SERIES.</b> .....	<b>9</b>
1-21.1	DoD Minimum Antiterrorism Standards for Buildings. ....	9
1-21.2	Security Engineering Facilities Planning Manual. ....	10
1-21.3	Security Engineering Facilities Design Manual. ....	10
1-21.4	Security Engineering Support Manuals.....	10
1-21.5	Security Engineering UFC Application. ....	10
<b>CHAPTER 2</b>	<b>PLANNING</b> .....	<b>13</b>
<b>2-1</b>	<b>ESTABLISH PLANNING REQUIREMENTS.</b> .....	<b>13</b>
<b>2-2</b>	<b>CONCEPT APPROVAL.</b> .....	<b>13</b>
2-2.1	SCIF Concept Approval. ....	13
2-2.2	SAPF Concept Approval. ....	13
<b>2-3</b>	<b>MINIMUM AND ENHANCED SECURITY.</b> .....	<b>13</b>
<b>2-4</b>	<b>PLANNING TEAM.</b> .....	<b>14</b>



<b>2-5</b>	<b>PLANNING DOCUMENTATION.</b>	<b>14</b>
<b>2-6</b>	<b>CONSOLIDATION OF SPACES.</b>	<b>14</b>
<b>2-7</b>	<b>VISITOR CONTROL.</b>	<b>14</b>
<b>2-8</b>	<b>PRIMARY ENTRANCE VESTIBULE.</b>	<b>15</b>
<b>2-9</b>	<b>TELECOMMUNICATION SPACES.</b>	<b>15</b>
2-9.1	Temperature and Humidity Control.	15
<b>2-10</b>	<b>RESILIENCY.</b>	<b>15</b>
2-10.1	Redundant Utilities.	15
2-10.2	Standby Power Systems (SPS).	16
2-10.3	Redundancy.	16
<b>2-11</b>	<b>HISTORIC PRESERVATION.</b>	<b>16</b>
<b>2-12</b>	<b>CONSTRUCTION SECURITY.</b>	<b>16</b>
<b>2-13</b>	<b>PROJECT DOCUMENTATION.</b>	<b>17</b>
<b>CHAPTER 3</b>	<b>DESIGN</b>	<b>19</b>
<b>3-1</b>	<b>VALIDATE PLANNING REQUIREMENTS.</b>	<b>19</b>
<b>3-2</b>	<b>MINIMUM AND ENHANCED SECURITY.</b>	<b>19</b>
<b>3-3</b>	<b>GENERAL DESIGN STRATEGY.</b>	<b>19</b>
3-3.1	Consolidation of Spaces.	19
3-3.2	Perimeter.	19
3-3.3	Building Layout.	20
<b>3-4</b>	<b>SPECIFIC DESIGN STRATEGY.</b>	<b>22</b>
3-4.1	Perimeter Construction.	22
3-4.2	Compartmented Area.	23
3-4.3	Acoustic Protection.	23
3-4.4	Perimeter Walls.	25
3-4.5	Ceilings and Floors.	29
3-4.6	Perimeter Doors.	29
3-4.7	Personal Electronic Device (PED) Cabinets.	33
3-4.8	Windows.	33
3-4.9	Daylighting.	33
3-4.10	Visual Protection of Windows and Daylighting Fenestration.	34
3-4.11	Perimeter Penetrations.	34
3-4.12	Vents and Ducts.	36

3-4.13	Acoustic Protection for Ducts.....	37
3-4.14	Access Port.....	38
3-4.15	Flashing or Rotating Light.....	38
3-4.16	Duress Alarm.....	38
3-4.17	Electronic Security System (ESS).....	39
3-4.18	Telecommunications Space.....	41
3-4.19	Telecommunication Cabling System.....	42
3-4.20	Protected Distribution Systems (PDS).....	42
3-4.21	RESILIENCE.....	43
3-4.22	TEMPEST.....	44
<b>CHAPTER 4</b>	<b>CONSTRUCTION.....</b>	<b>49</b>
<b>4-1</b>	<b>CONSTRUCTION AWARD.....</b>	<b>49</b>
<b>4-2</b>	<b>CONSTRUCTION PLANS SECURITY.....</b>	<b>49</b>
<b>4-3</b>	<b>CONSTRUCTION SITE SECURITY.....</b>	<b>49</b>
<b>4-4</b>	<b>ACCREDITATION PROCESS.....</b>	<b>49</b>
<b>4-5</b>	<b>INSPECTIONS.....</b>	<b>49</b>
<b>4-6</b>	<b>CONSTRUCTION DRAWINGS AND SUBMITTALS.....</b>	<b>50</b>
<b>4-7</b>	<b>PHOTOGRAPHIC CONSTRUCTION SURVEILLANCE RECORD.....</b>	<b>52</b>
<b>APPENDIX A</b>	<b>MINIMUM CONSTRUCTION.....</b>	<b>53</b>
<b>A-1</b>	<b>MINIMUM CONSTRUCTION.....</b>	<b>53</b>
<b>APPENDIX B</b>	<b>GLOSSARY.....</b>	<b>55</b>
<b>B-1</b>	<b>ACRONYMS.....</b>	<b>55</b>
<b>B-2</b>	<b>DEFINITION OF TERMS.....</b>	<b>56</b>
<b>APPENDIX C</b>	<b>REFERENCES.....</b>	<b>61</b>

## FIGURES

<b>Figure 1-1</b>	<b>Security Engineering UFC Applicability.....</b>	<b>11</b>
<b>Figure 3-1</b>	<b>Access Layers.....</b>	<b>20</b>
<b>Figure 3-2</b>	<b>Security Zones.....</b>	<b>21</b>
<b>Figure 3-3</b>	<b>STC 45 Assembly.....</b>	<b>26</b>
<b>Figure 3-4</b>	<b>STC 50 Assembly.....</b>	<b>26</b>
<b>Figure 3-5</b>	<b>Sealing Tracks.....</b>	<b>27</b>
<b>Figure 3-6</b>	<b>Wall Finish.....</b>	<b>28</b>

Figure 3-7 Furred Out Wall for Utilities ..... 29  
Figure 3-8 Tamper Resistant Hinges..... 31  
Figure 3-9 Emergency Exit Doors..... 32  
Figure 3-10 PED Cabinets ..... 33  
Figure 3-11 Duct Penetrations ..... 35  
Figure 3-12 Sealing Penetrations ..... 36  
Figure 3-13 Bars on Penetration..... 37  
Figure 3-14 Double Wall Acoustic Duct ..... 37  
Figure 3-15 Access Port ..... 38  
Figure 3-16 ABA Non-Compliant RF Door ..... 46

**TABLES**

Table A-1 Minimum Construction and Alarm..... 53

*This Page Intentionally Left Blank*

## CHAPTER 1 INTRODUCTION

### 1-1 PURPOSE AND SCOPE.

This UFC is intended to provide unified criteria to make the planning, design and construction communities aware of the published regulatory requirements to ensure timely, consistent, and appropriate implementation.

### 1-2 REISSUES AND CANCELS.

This UFC reissues and cancels UFC 4-010-05, Change 1, 1 October 2013.

### 1-3 APPLICABILITY.

This document applies to all construction, renovation, and repair projects for DoD Sensitive Compartmented Information Facility (SCIF) or Special Access Program Facility (SAPF). This UFC applies to each phase of a project, from planning through construction.

#### 1-3.1 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.

#### 1-3.2 SAPF.

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.

### 1-4 GLOSSARY.

APPENDIX B contains acronyms, abbreviations, and terms.

### 1-5 REFERENCES.

APPENDIX C contains a list of references used in this document. The publication date of the code or standard is not included in this document. Unless otherwise specified, the most recent edition of referenced publications applies.

### 1-6 POLICY.

There are multiple policy documents that establish the baseline requirements for planning, design, construction and accreditation of DoD facilities.

### **1-6.1 Office of the Director of National Intelligence.**

Intelligence Community Directive (ICD) 705 was issued by the Director of National Intelligence (DNI) on May 26, 2010. Intelligence Community Standard (ICS) 705-1, ICS 705-02, and the Intelligence Community (IC) Tech Spec-for ICD/ICS 705 provides the physical and technical security standards for SCIFs, including existing, new construction, and renovations. Refer to ICS 705-1, ICS 705-02, and IC Tech Spec-for ICD/ICS 705 for additional information.

### **1-6.2 Department of Defense.**

- DoDM 5105.21 (Volumes 1-3) are the primary documents associated with SCIFs for the DoD. The manuals are composed of several volumes, each having its own purpose. DoDM 5105.21 volume 2 concerns the physical security of a SCIF and it requires the implementation of Director of National Intelligence (DNI) policies for the protection of SCI and additional requirements.
- DoDM 5205.07 (Volumes 1-4) are the primary documents associated with SAPFs for the DoD. The manual is composed of several volumes, each having its own purpose. DoDM 5205.07 Vol 3 concerns the physical security of a SAPF and it establishes the construction of a SAPF will conform to the equivalent SCIF requirements, as defined in IC Tech Spec-for ICD/ICS 705.
- DoDM 5200.01 volumes 1-3 are the primary document associated with the protection of classified information for the DoD. The manual is composed of several volumes, each having its own purpose. DoDM 5200.01 volume 3 concerns the physical security of a classified information.
- DoDI 5200.48 is the primary document associated with the protection of Controlled Unclassified Information (CUI).

## **1-7 REGULATORY AUTHORITY.**

### **1-7.1 DoD SCIF Authorities.**

The DoDM 5105.21 manuals define the regulatory authorities for DoD SCIF.

### **1-7.2 Non-DoD SCIF Authorities.**

In some cases, the DoD may build a SCIF for Non-DoD agencies. These projects will have an IC designated AO sponsor for each construction or renovation project for the Non-DoD agency.

### **1-7.3 DoD SAPF Authorities.**

The DoDM 5205.07 manuals define the regulatory authorities for DoD SAPF. The special access program facility accrediting official (SAO) is defined as the AO for SAPF.

## **1-8 IMPLEMENTATION.**

Note that this UFC was based on IC Tech Spec-for ICD/ICS 705 Version 1.5.1. When the National Counterintelligence and Security Center adopts a newer version, it will have precedence over the requirements contained in this UFC.

### **1-8.1 Department of Navy.**

Refer to NAVFAC INST 4700.1 for additional policy for Department of Navy projects that include a SCIF. The NAVFAC instruction details various steps accomplished in the planning, design and construction phase of a SCIF including roles and responsibilities.

### **1-8.2 Department of the Army.**

Department of the Army projects that include a SCIF, refer to *SCIF Security, Planning, Design, and Construction Tasks* downloadable at: <https://www.wbdg.org/ffc/army-coe/policies-and-guidance-army-design-and-construction/scif-tasks>. The task list details various steps accomplished in the planning, design, and construction of a SCIF, including the roles and responsibilities, Per USACE Engineering Regulation 1110-1-8158 Engineering and Design Centers of Expertise Program, for projects containing SCIFs completed by USACE, inclusion of representative(s) from the USACE Protective Design Center as part of the project delivery team is mandatory. For projects executed by any other services, inclusion of the USACE Protective Design Center is optional. Contact information can be found at: <https://www.nwo.usace.army.mil/pdc/home/>

### **1-8.3 Department of the Air Force.**

Department of the Air Force projects that include a SCIF, the Construction Agency acting on behalf of the AF must utilize their respective task list for the planning, design, construction of SCIFs including the roles and responsibilities. In the rare case where the AF is acting as the DoD Construction Agent, either the NAVFAC or the USACE task list may be used.

## **1-9 GENERAL BUILDING REQUIREMENTS.**

Comply with UFC 1-200-01, *DoD Building Code*. UFC 1-200-01 provides applicability of model building codes and government unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, high performance and sustainability requirements, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

## **1-10 CYBERSECURITY.**

All facility-related control systems (including systems separate from a utility monitoring and control system) must be planned, designed, acquired, executed, and maintained in accordance with UFC 4-010-06, and as required by individual Service Implementation Policy.

### **1-10.1 Mission Critical Facility-Related Control Systems.**

Determine facility-related control system categorization in coordination with supported command and mission owner. Incorporate cybersecurity into the mission critical facility-related control systems with a minimum Confidentiality/Integrity/Availability Categorization of Moderate/Moderate/Moderate as indicated in IC Standard 706-02.

### **1-11 FACILITY CLASSIFICATION.**

SCIF and SAPF are classified based on operational requirements. There are various classifications.

#### **1-11.1 Secure Working Area (SWA) or SAP Working Area (SAPWA).**

Area where SCI or SAP is handled, discussed, and/or processed but not stored.

#### **1-11.2 Temporary Secure Working Area (TSWA) or Temporary SAP Working Area (TSAPWA).**

An accredited area used for the handling, discussing or processing of SCI or SAP information, when use is limited to less than 40 hours per month.

#### **1-11.3 Temporary SCIF (T-SCIF) or Temporary SAPF (T-SAPF).**

Established for a limited time to meet tactical, emergency, or immediate operational requirements.

#### **1-11.4 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 all classified materials, equipment and information.

#### **1-11.5 Open Storage.**

An accredited facility in which SCI or SAP information may be openly stored or processed without using a GSA-approved storage container.

#### **1-11.6 Continuous Operation.**

An accredited facility staffed and operated 24/7.

### **1-12 SECURITY IN DEPTH.**

Security in Depth (SID) is desired for all SCIF or SAPF and required for locations outside the United States, its possessions or territories. SID is a multilayered approach, which effectively employs human and other physical security measures throughout the installation or facility to create a layered defense against potential threats. The intent of SID is to increase the possibility of detection of potential aggressors prior to



compromising the SCI or SAP materials. Per IC Tech Spec for ICD/ICS 705, the primary means to achieve SID include one of the following:

- Located on a Military installation, embassy compound, U.S. Government (USG) compound, or contractor compound with a dedicated response force of U.S. persons.
- Located within a controlled building with separate building access controls, alarms, elevator controls, stairwell controls required to gain access to the buildings or elevators.
- Controlled office areas adjacent to or surrounding the secure area that are protected by an Intrusion Detection System (IDS).
- Located within a fenced compound with access controlled vehicle gate and/or pedestrian gate.

### **1-13 SECURITY REQUIREMENTS.**

ICS 705-1 and IC Tech Spec-for ICD/ICS 705 provide the security standards. Per IC Tech Spec-for ICD/ICS 705, exceeding or not meeting a standard, even when based upon risk, requires an approved waiver.

Waivers are processed and approved in accordance with DoDM 5105.21 Vol 2 for SCIF and DoDM 5205.07 Vol 3 for SAPF.

### **1-14 SITE SECURITY MANAGER (SSM).**

The SSM is responsible for the security aspects of project planning, design and construction. The SSM is also responsible to ensure compliance of all regulatory requirements for the accreditation of the facility. Planners, Project Managers, Design Managers, Designers, and Construction Managers must work closely with the supported command and their designated SSM to determine the requirements for each project and ensure the implementation of the policy based requirements.

Projects with a SCIF and a SAPF may have two different SSMs reporting to two different AOs.

### **1-15 CONSTRUCTION SECURITY PLAN (CSP).**

The CSP documents the security requirements from planning through construction for each project. Per IC Tech Spec-for ICD/ICS 705, a CSP is developed by the SSM and approved by the AO for each project.

Per IC Tech Spec – for ICD/ICS 705, do not award a construction contract without an approved CSP. See DoDM 5105.21 Vol 2 for SCIF and DoDM 5205.07 Vol 3 for SAPF for additional information and for Navy and Marine Corps projects, refer to NAVFAC INST 4700.01.

## **1-16 INFORMATION SECURITY.**

Per ICS 705-1, construction plans and related documents are to be handled and protected in accordance with the CSP. Construction plans and related documents may be publicly releasable, CUI, or if Classification Guide dictates, plans and related documents may require classification. Refer to DoDM 5200.01 Vol 3 for the handling of classified information and DoDI 5200.48 for the handling of Controlled Unclassified Information (CUI).

### **1-16.1 SCIF Location and Identity.**

DoDM 5105.21 Vol 2 states the facility's location (complete address) and identity of a SCIF must be protected at a minimum of CUI. Drawings or diagrams identified as a SCIF may not be posted on an UNCLASSIFIED website, transmitted over the Internet without some type of encryption or included on public releasable documents.

Therefore, do not identify SCIF locations on planning or construction documents. With SSM's approval, areas may be identified as "Restricted Area", "Controlled Space", "Secure Area", "Controlled Area" or some other non-identifiable name.

### **1-16.2 SAPF Location and Identity.**

Similar to SCIF, coordinate with the SSM on how to identify SAPF locations on planning or construction documents. With the SSM's approval, areas may be identified as "Restricted Area", "Controlled Space", "Secure Area", "Controlled Area" or some other non-identifiable name.

### **1-16.3 TEMPEST Vulnerabilities and Recommended Countermeasures.**

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<sup>1</sup>.

### **1-16.4 Security Environment Threat List (SETL) Information.**

The SETL and its contents including a country's threat category is classified Secret.

## **1-17 DESIGN SECURITY.**

Per IC Tech Spec – for ICD/ICS 705, design must be performed by U.S. companies using U.S. citizens or U.S. persons. AO must ensure mitigations are implemented when using non-U.S. citizens and these mitigations are documented in the CSP.

## **1-18 CONSTRUCTION SECURITY.**

Depending on the location of the facility, the AO may impose procedures for the procurement, shipping, selection, and secure storage of construction materials. In

---

<sup>1</sup> DoDM 5105.21 Vol 2

addition, there may be site security and access control that may include vehicle and personnel inspections. The CSP documents the security requirements for each project. For reference, DoDM 5105.21-Volume 2 and DoD M5205.07 Volume 3 provide additional information on security requirements for DoD SCIF and SAPF construction projects.

### **1-18.1 Within the United States.**

For facilities located within the U.S., its possessions or territories, general construction of the SCIF or SAPF must be performed by U.S. companies using U.S. citizens or U.S. persons. The AO must ensure mitigations are implemented when using non-U.S. citizens. These mitigations must be documented in the CSP.

Per IC Tech Spec – for ICD/ICS 705, Intrusion Detection System (IDS) installation and testing must be performed by U.S. companies using U.S. citizens. However, 5200.01, Volume 3 requires that the alarm installation and maintenance for IDS that protect classified information be accomplished by U.S. citizens who have been subjected to a trustworthiness determination.

### **1-18.2 Outside the United States.**

For facilities located outside the U.S., its possessions or territories, general construction of the SCIF or SAPF must be performed using U.S. companies using U.S. citizens.

- On military facilities, the AO may authorize foreign national citizens or companies to perform general construction. In this situation, the SSM must prescribe, with AO approval, mitigating strategies. These mitigations must be documented in the CSP.
- U.S. Top Secret-cleared personnel must perform finish work in Category I and II countries. U.S. Secret-cleared personnel must perform finish work in Category III countries. Finish work includes activities such as closing up wall structures; installing, floating, taping and sealing wallboards; installing trim, chair rail, molding, flooring; acoustical ceiling tile, light fixtures, device plates, diffusers, registers, grilles, and painting.
- IDS installation and testing must be performed by personnel who are U.S. Top Secret-cleared or U.S. Secret-cleared and escorted by SCIF or SAPF personnel.

### **1-19 ACCREDITATION.**

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 for the DoD policy on accreditation.

### **1-19.1 Accreditation Process.**

Inspections and evaluations are typically performed by the SSM, or designee, prior to initial accreditation. The accreditation process includes, site inspections and a review of documents relating to design, construction, and testing. The SSM is responsible for assembling and submitting documents for AO approval. The forms for these documents are included in the IC Tech Spec – for ICD/ICS 705. These documents include, but are not limited to the following:

- Construction Security Plan
- Fixed Facility Checklist
- TEMPEST Addendum
- Pre-Construction Checklist

Planners, Designers of Record, Project Managers, and Construction Managers must provide the SSM the project information needed to develop these documents to support the accreditation process. Information may include, site plans, floorplans, IDS plans, and information related to construction methods and materials.

### **1-19.2 Fixed Facility Checklist (FFC).**

The FFC is a standardized form that documents the physical, technical, and procedural security information to obtain accreditation. This document may be CUI or Classified depending on contents.

### **1-19.3 TEMPEST Addendum.**

The requesting command's Special Security Officer (SSO) or SSM will use the TEMPEST addendum to the FFC, sometimes referred to as the TEMPEST Checklist to request the TEMPEST Countermeasures Review (TCR) by the Certified Technical TEMPEST Authority (CTTA). For an initial TCR, the addendum will be submitted to AO during the planning phase<sup>2</sup>. 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.

The CTTA will provide the TCR based on the TEMPEST addendum and recommend countermeasures to the AO as part of the accreditation process.

### **1-19.4 Pre-Construction Checklist.**

The Pre-Checklist provides the AO with project information, points of contact and information required to assist in the determination of the security requirements for the project and final accreditation.

## **1-20 HISTORIC PRESERVATION COMPLIANCE.**

---

<sup>2</sup> DoDM 5105.21 Vol 2

### **1-20.1 Security and Stewardship.**

The Department of Defense remains the lead federal agency in balancing security threats with the protection of historic properties. The Department of Defense abides by federal legislation on protecting cultural resources, and issues its own complementary policies for stewardship.

### **1-20.2 Compliance with Laws.**

Implementation of ICD 705 will not supersede DoD's obligation to comply with federal laws regarding cultural resources to include the National Historic Preservation Act (NHPA) and the Archaeological Resources Protection Act (ARPA). Installation personnel must determine possible adverse effects to historic structures and/or archaeological resources during project development and consult accordingly. Personnel at installations outside the United States should coordinate with the applicable host nation regarding possible adverse effects to cultural resources.

### **1-20.3 Compliance with DoD Standards.**

Conversely, historic preservation compliance does not negate the requirement to implement other Department of Defense policy. Federal agencies are always the decision-maker in the Section 106 process of the National Historic Preservation Act. An agency should seek to avoid prolonged consultations that conflict with the imminent need to implement security requirements. Preservation considerations and security standards are not mutually exclusive, and any compliance conflicts should be quickly and effectively resolved in consultation with appropriate stakeholders.

## **1-21 SECURITY ENGINEERING UFC SERIES.**

This UFC is one of a series of security engineering unified facilities criteria documents that cover minimum standards, planning, preliminary design, and detailed design for security and antiterrorism. The manuals in this series are designed to be used sequentially by a diverse audience to facilitate development of projects throughout the design cycle. The manuals in this series include the following:

### **1-21.1 DoD Minimum Antiterrorism Standards for Buildings.**

UFC 4-010-01 establishes standards that provide minimum protection against terrorist attacks for the occupants of all DoD inhabited buildings. This UFC is intended to be used by security and antiterrorism personnel and design teams to identify the minimum requirements that must be incorporated into the design of all new construction and major renovations of inhabited DoD buildings and inhabited tenant buildings on DoD installations. They also include recommendations that should be, but are not required to be incorporated into all such buildings.

### **1-21.2 Security Engineering Facilities Planning Manual.**

UFC 4-020-01 presents processes for developing the design criteria necessary to incorporate security and antiterrorism into DoD facilities and for identifying the cost implications of applying those design criteria. Those design criteria may be limited to the requirements of the minimum standards, or they may include protection of assets other than those addressed in the minimum standards (people), aggressor tactics that are not addressed in the minimum standards, or levels of protection beyond those required by the minimum standards. The cost implications for security and antiterrorism are addressed as cost increases over conventional construction for common construction types. The changes in construction represented by those cost increases are tabulated for reference, but they represent only representative construction that will meet the requirements of the design criteria. The manual also addresses the tradeoffs between cost and risk. The Security Engineering Facilities Planning Manual is intended to be used by planners as well as security and antiterrorism personnel with support from planning team members.

### **1-21.3 Security Engineering Facilities Design Manual.**

UFC 4-020-02FA provides interdisciplinary design guidance for developing preliminary systems of protective measures to implement the design criteria established using UFC 4-020-01. Those protective measures include building and site elements, equipment, and the supporting manpower and procedures necessary to make them all work as a system. The information in UFC 4-020-02FA is in sufficient detail to support concept level project development, and as such can provide a good basis for a more detailed design. The primary audience for the Security Engineering Design Manual is the design team, but it can also be used by security and antiterrorism personnel.

### **1-21.4 Security Engineering Support Manuals.**

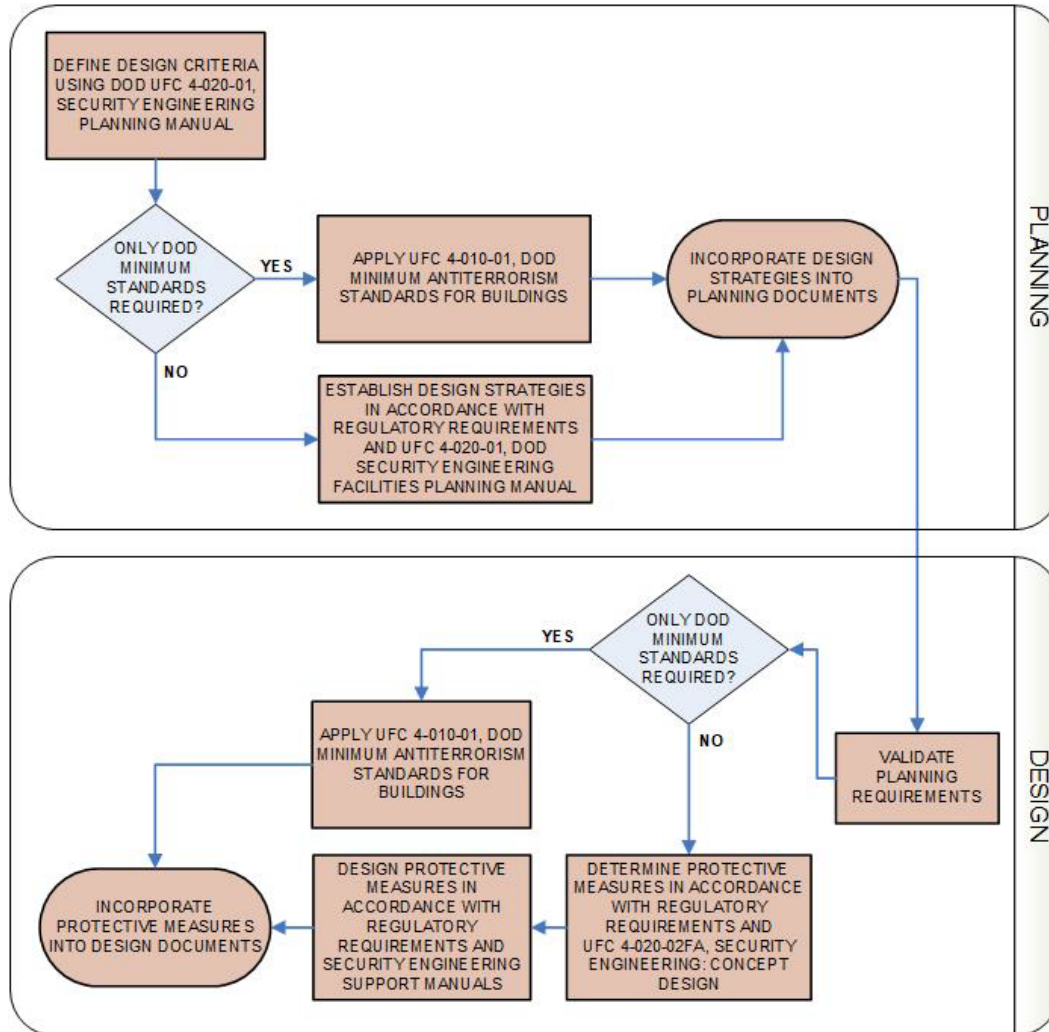
In addition to the standards, planning, and design UFCs mentioned above, there is a series of additional UFCs that provide detailed design guidance for developing final designs based on the preliminary designs developed using UFC 4-020-02FA. These support manuals provide specialized, discipline specific design guidance. Some address specific tactics such as direct fire weapons, forced entry, or airborne contamination. Others address limited aspects of design such as resistance to progressive collapse or design of portions of buildings such as mail rooms. Still others address details of designs for specific protective measures such as vehicle barriers or fences. The Security Engineering Support Manuals are intended to be used by the design team during the development of final design packages.

### **1-21.5 Security Engineering UFC Application.**

The application of the security engineering series of UFCs is illustrated in Figure 1-1. UFC 4-020-01 is intended to be the starting point for any project that is likely to have security or antiterrorism requirements. By beginning with UFC 4-020-01, the design criteria will be developed that establishes which of the other UFCs in the series will need to be applied. The design criteria may indicate that only the minimum standards

need to be incorporated, or it may include additional requirements, resulting in the need for application of additional UFCs. Applying this series of UFCs in the manner illustrated in Figure 1-1 will result in the most efficient use of resources for protecting assets against security and antiterrorism related threats.

Figure 1-1 Security Engineering UFC Applicability



*This Page Intentionally Left Blank*



## CHAPTER 2 PLANNING

### 2-1 ESTABLISH PLANNING REQUIREMENTS.

This chapter is intended to make planners aware of requirements that may affect the facility scope and budget. It is not intended to document the standard planning processes related to project development.

### 2-2 CONCEPT APPROVAL.

SCIFs and SAPFs are established when there are clear operational requirements that are critical to the supported command's mission. All projects begin with an AO's sponsorship. This sponsorship is formalized for SCIF and some SAPFs with the Concept Approval.

#### 2-2.1 SCIF Concept Approval.

Per DoDM 5105.21 Vol 2, to establish a SCIF, the supported command must have Concept Approval. The Concept Approval is the first critical element in the establishment of a SCIF. For approval, the commander must submit a request for SCI to the Service Cognizant Security Authority (CSA), their designee, or DoD Component senior intelligence official (SIO). This is referred to as the request for Concept Approval. Concept Approval certifies that a clear operational requirement exists for the SCIF and there is no existing SCIFs to support the requirement. Proof of sponsorship in the form of a SCIF number or written documentation of Concept Approval from the supported command is required to establish a SCIF.

#### 2-2.2 SAPF Concept Approval.

DoDM 5205.07 Vol 3 does not require Concept Approval for SAPF. Sponsorship for most SAPFs is formalized at the program level.

##### 2-2.2.1 Navy SAPF Concept Approval.

Per DONSAPCO/0779-22 Memo, Director, Department of the Navy Special Program Central Office requires Concept Approval for the establishment of a SAPF. The organization with the requirement for the SAPF submits a concept request endorsed by the leadership of the organization via the Program Security Officer (PSO) and the Government Program Manager (GPM). The concept request must clearly define the operational requirement and identify why existing SAPFs do not meet the need. In addition, the organization is required to identify a Site Security Manager (SSM) for the project.

### 2-3 MINIMUM AND ENHANCED SECURITY.

ICS 705-1 and IC Tech Spec-for ICD/ICS 705 provide the minimum security standards. The security requirements are based on classification, location, and risk assessment of the facility. APPENDIX A provides an overview of the minimum construction requirements. To implement security enhancements above the minimum, the AO will

evaluate the threat, SID and balance the security enhancements with cost at acceptable risk.

#### **2-4 PLANNING TEAM.**

Establish an interdisciplinary planning team with local considerations. The interdisciplinary planning team must work together to determine classification of the space and establish the minimum/enhanced security requirements. The planning team may consider user constraints such as operations, manpower requirements or limitations, and sustainment costs when determining the requirements for the overall security solution. The planning team should include the following:

- Planning
- Supported Command
- SSM(s)
- Communications
- Security
- Engineering
- Cultural resources (if historical building)

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

#### **2-5 PLANNING DOCUMENTATION.**

The classification, operation, security requirements, TEMPEST countermeasures, and resulting facility related requirements must be scoped, documented, and budgeted during the planning process. Concept Approval, Preliminary CSP, FFC and TEMPEST Addendum 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 NAVFAC INST 4700.01 for additional information.

#### **2-6 CONSOLIDATION OF SPACES.**

When a facility has more than one SCIF or SAPF, serious consideration must be given to consolidating the multiple spaces into one with Compartmented Areas within. Any consolidation of spaces will reduce initial infrastructure and electronic security systems, associated accreditation requirements, and sustainment. Coordinate consolidation with the supported command to ensure the configuration meets command's operational (compartmented) requirements.

#### **2-7 VISITOR CONTROL.**

Some larger facilities may require additional space at the entrance for processing and visitor control. Program adequate space for processing un-indoctrinated personnel and visitors, issuing badges and space for personnel awaiting escorts.

## **2-8 PRIMARY ENTRANCE VESTIBULE.**

Program space for a vestibule at the primary entrance. Vestibules enhance the security of the space by precluding visual observation into the space and enhancing acoustic protection.

## **2-9 TELECOMMUNICATION SPACES.**

Per UFC 3-580-01, the minimum size for a Telecommunications Room (TR) is 10 feet x 8 feet (3m x 2.4m). This and the normal net to gross calculation may be inadequate if the TR contains equipment racks for multiple networks such as Secret Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS), Non-classified Internet Protocol Router Network (NIPRNet) and voice services. Depending on the number of workstations served, this could generate a larger space requirement when considering RED/BLACK separation requirements.

UFC 3-580-01 allows the use of Equipment Room in lieu of a TR for buildings that house substantial Information Technology (IT) electronics. A telecommunication space that contains equipment for multiple classified networks such as SIPRNet, JWICS and NIPRNet all requiring RED/BLACK separation is considered as substantial Information Technology (IT) electronics which would allow for the use of the larger Equipment Rooms.

### **2-9.1 Temperature and Humidity Control.**

Substantial Information Technology (IT) equipment generate a significant amount of heat. In these environments, the heat densities can be up to five times higher than in a typical office load. Traditional HVAC systems cannot remove enough heat to protect this equipment. Instead, these areas require dedicated computer room air conditioner (CRAC) units with higher cooling capabilities. The smallest high-powered CRACs require a minimum 10 ft. x 3 ft. (3m×1m) footprint for equipment and clearances. This area must be included in the equipment room area calculation.

## **2-10 RESILIENCY.**

Some critical operations or communication systems may require redundant utilities, standby power, and redundant systems to ensure continuous operation in the event of utility or equipment failure. Coordinate system and the associated resiliency requirements with the mission commander.

### **2-10.1 Redundant Utilities.**

Critical operations or communication systems may require redundant utilities such as telecommunication system connectivity and utility power services. To be redundant, they must be two separate utilities that are not routed together.

## **2-10.2 Standby Power Systems (SPS).**

Critical operations or Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) systems may require an SPS designed to ensure continuity of electrical power to essential and uninterruptible loads upon loss of normal power sources.

### **2-10.2.1 Engine-Driven Generator.**

When a SPS is required, provide a standby engine-driven generator sized for essential and uninterruptible loads to ensure continued operation upon loss of utility power.

### **2-10.2.2 Uninterruptible Power System (UPS).**

When a SPS is required, provide UPS for the uninterruptible loads to filter commercial power and to support the uninterruptible loads during transitions to and from the standby generator.

## **2-10.3 Redundancy.**

Some critical operations may require a minimum of N+1 redundancy to ensure system availability in the event of component failure. In this configuration, components (N) have at least one independent backup component (+1). An example would be chillers, CRACs, or generators.

## **2-11 HISTORIC PRESERVATION.**

Preservation of Cultural Resources must be considered when converting a historical building into a secure facility or locating a secure space or room within a historic building. For instance, every effort should be made to minimize or eliminate windows, especially on the ground floor. Windows less than 18 feet above the ground or from the nearest platform affording access to the window (measured from the bottom of the window) and doors must be protected against forced entry and meet the standard for the perimeter, which may include acoustic and TEMPEST mitigation. State Historic Preservation Officers (SHPO) may consider window and door modifications to have an adverse effect but allow the modification if the impact is minimized and the effect mitigated. Planners need to explore options and 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.

## **2-12 CONSTRUCTION SECURITY.**

For locations outside the United States, its possessions or territories, the AO may impose procedures for the procurement, shipping, and storing of construction materials at the site. In addition, the AO may require access control to the construction materials and the construction area. These requirements and others are documented in the CSP. Since these additional security measures may have significant cost impacts on a project, they must be determined during project development and documented in the CSP, project planning documents, and the costs must be included in the project budget.

## 2-13 PROJECT DOCUMENTATION.

Work with the Supported Command, and the SSM to determine and document the classification, operation, and resulting facility requirements for the project. Projects in higher threat areas (outside the United States, its possessions or territories) may have additional security requirements. Determine and document the following during project development:

- 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?
- Are there any Electronic Security System (ESS) requirements above that required by IC Tech Spec-for ICD/ICS 705?
- 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 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?

- Has the supported command provided the CTTA with a completed TEMPEST Addendum for the TCR?
  - If so, what will be the required TEMPEST countermeasures? RED/BLACK separation, 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?
- 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.

## CHAPTER 3 DESIGN

### 3-1 VALIDATE PLANNING REQUIREMENTS.

Work with the Supported Command and the SSM to validate the requirements established in the planning phase. Operation, classification, and threat classification may have changed since the project was planned. Validate and document the classification, operation, and resulting facility requirements documented in the CSP. Include requirements in the Design Build RFP, design documents, and construction contracts.

### 3-2 MINIMUM AND ENHANCED SECURITY.

ICS 705-1 and IC Tech Spec-for ICD/ICS 705 provide the minimum and enhanced security standards. APPENDIX A provides an overview of the minimum construction requirements. Per IC Tech Spec-for ICD/ICS 705, exceeding a standard, even when based upon risk, requires a waiver. Planners may have to provide the cost associated with exceeding a standard to include in the evaluation process.

Waivers are processed and approved in accordance with DoDM 5105.21 Vol 2 for SCIF and DoDM 5205.07 Vol 3 for SAPF.

### 3-3 GENERAL DESIGN STRATEGY.

The general design strategy for any tactic is the basic approach to developing a protective system to mitigate the effects of that tactic. It governs the general application of construction, building support systems, equipment, manpower, and procedures.

The design will vary depending on type, location, SID, risk assessment, and National Security Information (NSI) processing, storage and discussion requirements. Designers must take a six-sided approach when designing a secure space. Design the floor, ceiling, walls and any penetrations to meet the performance requirements for the perimeter.

#### 3-3.1 Consolidation of Spaces.

When a facility has more than one SCIF or SAPF, serious consideration must be given to consolidate the multiple spaces into one. Any consolidation of spaces will reduce initial infrastructure, electronic security systems, associated accreditation requirements, and sustainment costs. Coordinate consolidation with the supported command to ensure the configuration meets command's operational and compartmented requirements.

#### 3-3.2 Perimeter.

The perimeter includes perimeter walls, ceiling, floor, and all penetrations in the perimeter such as windows, doors, ducts and utilities. At a minimum, the perimeter provides:

- Resistance to forced entry
- Resistance to covert entry
- Visual evidence of surreptitious penetration
- Resistance to visual observation
- Sound Attenuation for acoustic eavesdropping
- Countermeasures for Electronic Emanations -TEMPEST (when required)

This includes above the false ceilings and below raised floors.

### 3-3.3 Building Layout.

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

#### 3-3.3.1 Zoning.

Zoning is the concept of grouping functional areas by security or access levels to enhance security. If configured correctly, having multiple zones within a facility can enhance the security of the higher security zones. This is accomplished by requiring personnel to transition through increasingly secure access control layers (zones) prior to accessing the highest security zone. Zones may include public access, controlled access, and 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. See Figure 3-1 for access layers and Figure 3-2 for a bubble diagram example.

**Figure 3-1 Access Layers**

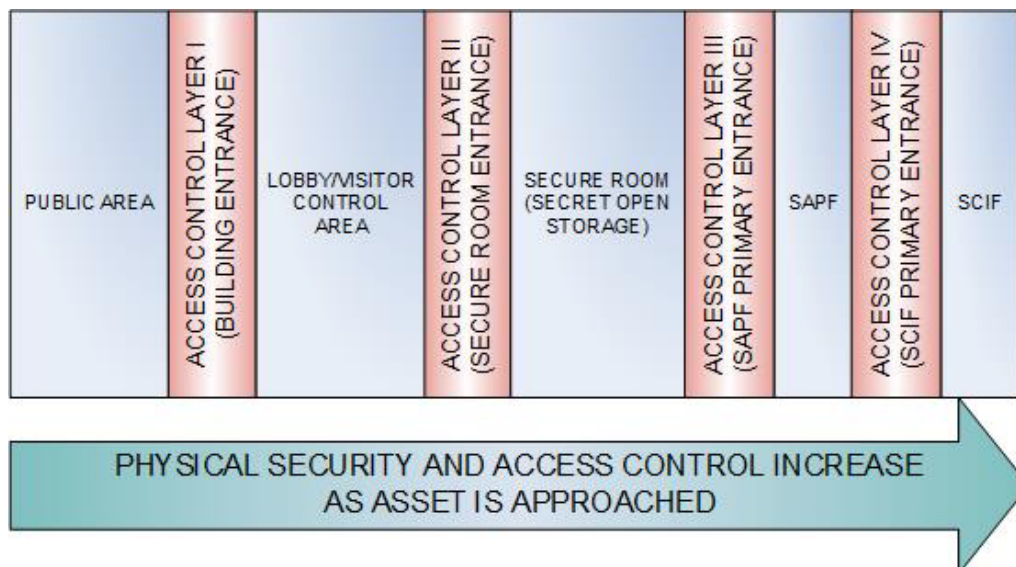
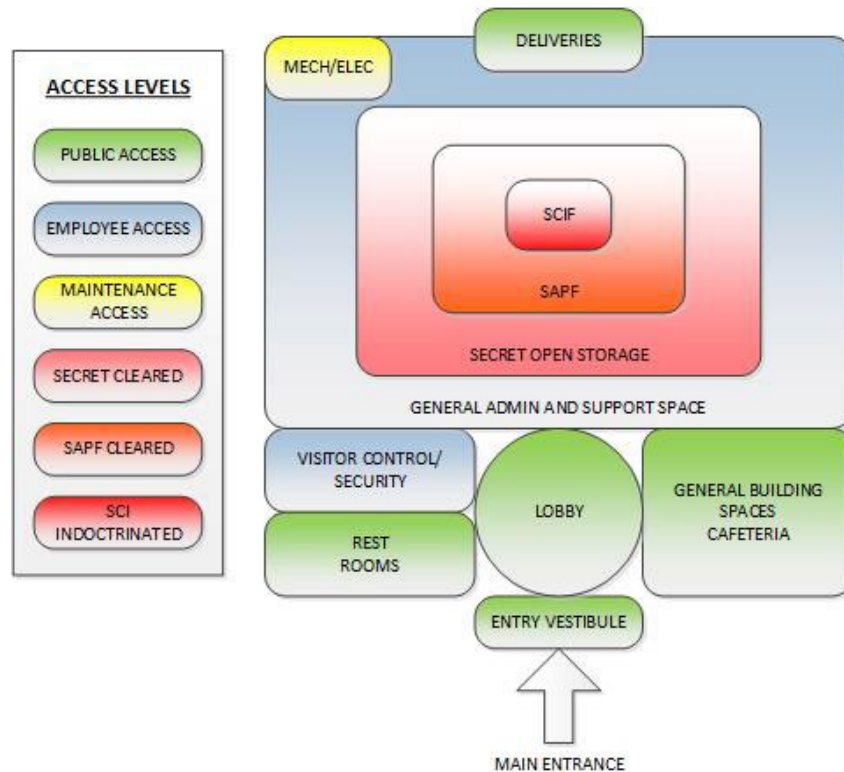




Figure 3-2 Security Zones



### 3-3.3.2 Layout Criteria.

In developing the 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, 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 access to the SCIF through a SAPF or secret open storage area.
- Are foreign nationals allowed in the facility to work or participate in training given at the facility? If so, building layout should consolidate high security areas and provide the appropriate separation to minimize the technical threat and escort requirements.
- Utilities and general building support spaces should remain outside of the secure areas.

- Locate telecommunication spaces that contain the encryption equipment within or adjacent (shared wall) to the secure area to enhance security and minimize or eliminate Protected Distribution System (PDS) requirements.
- Entry into a lower security area cannot be through a higher security area. This would require escorts.
- Egress paths from the lower security areas must not pass through a higher security area.
  - Egress stairs intended for use as communicating stairs between secure areas must have appropriate access control at each floor level without compromising safe egress to grade from all floor levels.
  - Vertical circulation elements that are entirely within the secure area may not require additional controls at each landing.

### **3-3.3.3 Adjacent Space.**

To increase SID, locate other areas that require access control adjacent to or surrounding the SCIF or SAPF.

### **3-3.3.4 Visitor Control.**

Some larger facilities may require additional space at the entrance for processing and visitor control. For these facilities, provide adequate space for processing un-indoctrinated personnel and visitors, issuing badges and space for personnel awaiting escorts.

## **3-4 SPECIFIC DESIGN STRATEGY.**

The specific design strategy for any tactic governs how the general design strategy varies for different levels of protection or threat severity. They may vary by the sophistication of the protective measures and the degree of protection provided. The specific design strategies reflect the degree to which assets will be left vulnerable after the protective system has been employed.

### **3-4.1 Perimeter Construction.**

The secure area perimeters and the penetrations in those perimeters are the primary focus of the design and construction. IC Tech Spec-for ICD/ICS 705 provides the minimum and enhanced construction requirements for the perimeter with regard to forced entry, covert entry, visual evidence of surreptitious penetration, and sound attenuation. In addition, radio frequency (RF) shielding and other TEMPEST mitigation must be provided as documented in the TCR. Refer to Best Practices Guidelines for Architectural Radio Frequency Shielding for standard construction for RF shielding.

IC Tech Spec-for ICD/ICS 705 includes suggested construction details for acoustic wall construction and duct penetrations. Designers must ensure that details used from IC

Tech Spec-for ICD/ICS 705 comply with UFC 1-200-01. For example, IC Tech Spec-for ICD/ICS 705 has a suggested wall detail for Wall C - enhanced construction utilizing plywood. However, plywood used for construction of interior partitions must be Fire Retardant Treated (FRT) in buildings required to be of noncombustible construction.

### **3-4.1.1 Inspectable Perimeter.**

Secure space perimeters, including the perimeter above the ceiling or below raised floors may need to be inspected for surreptitious penetration once a space becomes operational. The design should facilitate future inspections by minimizing the above ceiling obstructions on the controlled and uncontrolled side of the secure perimeter. Where hard ceilings are located adjacent to the perimeter, coordinate inspection methods with the SSM and SSO to ensure the capability of above ceiling or below raised floors inspections.

### **3-4.2 Compartmented Area.**

A Compartmented Area may be an area, room, or a set of rooms within the accredited space that provides controlled separation between control systems, compartments, sub-compartments, or Controlled Access Programs. There are three types of compartmented areas. Type I is an area where discussion is not authorized so there is no sound rated construction required. Type II & III are a room, or set of rooms are constructed the same and require acoustic protection.

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.

### **3-4.3 Acoustic Protection.**

The perimeter of the space must provide acoustic protection. The acoustic protection is intended to protect conversations from being inadvertently overheard outside the secure space, not to protect against deliberate interception of audio.<sup>3</sup>

#### **3-4.3.1 Sound Transmission Class (STC).**

The ability of an assembly to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC). Architectural Graphics Standards (AGS) established Sound Groups 1 through 4, of which Groups 3 and 4 are

---

<sup>3</sup> IC Tech Spec – for ICD/ICS 705

considered adequate for specific acoustical security requirements for 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.

IC Tech Spec – for ICD/ICS 705 provides definitions for Sound Group 3 and 4 based on the above descriptions from AGS.

### **3-4.3.2 Sound Attenuation Descriptions.**

The amount of sound energy reduction may vary according to individual facility requirements. However, Sound Group ratings will be used to describe the effectiveness of acoustical security measures afforded by various wall materials and other building components.

- A minimum of Sound Group 3 (STC 45 or better) for the perimeter unless additional protection is required for amplified sound<sup>3</sup>. This applies to the entire perimeter of the space to include walls, ceilings and floors and perimeter penetrations such as conduit, pipe, ducts, doors, and windows.
- Conference rooms or other areas where amplified audio is used such as video teleconference (VTC) equipment, audio visual systems, and speakerphones must meet Sound Group 4 (STC 50 or better)<sup>3</sup>.

### **3-4.3.3 Minimum Perimeter STC Rating.**

The SSM develops the CSP and recommends the STC rating for the perimeter with approval by the AO. The STC ratings for the perimeter should be either STC 45 or STC 50. When factory tested in accordance with ASTM E90, provide 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. This will ensure the assemblies meet the minimum STC requirement when installed correctly. Most factory tests are conducted on assemblies with framing members spaced at 24" (607 mm) on center (o.c.). The spacing of the framing member may be reduced to 16" (406 mm) o.c. without compromising the STC rating<sup>4</sup>.

### **3-4.3.4 Sound Masking.**

When normal construction and baffling measures have been determined to be inadequate to meet the sound attenuation requirement, utilize sound masking. See IC Tech Spec for more information on the use of sound masking systems and devices.

---

<sup>4</sup> GA-600

### **3-4.4 Perimeter Walls.**

SSM, with AO approval, will determine if the perimeter walls are Standard (Wall A), Enhanced (Wall B or C) or vault construction. Walls must go from floor slab (true floor) to underside of floor or roof deck (true ceiling). Perimeter walls, floor and ceiling must be permanently and solidly constructed and attached to each other. 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.

Exception: When an existing wall is constructed with substantial material such as brick, concrete, masonry, the existing wall may be utilized to satisfy the specification<sup>5</sup>.

#### **3-4.4.1 Perimeter Wall Variations.**

The IC Tech Spec-for ICD/ICS 705 included suggested wall drawings for Standard (Wall A), Enhanced (Wall B or C) and construction criteria for STC 45 and 50 walls. These are suggested and allow variations in wall construction techniques to meet the security standards.

There are criteria beyond the scope of the IC Tech Spec-for ICD/ICS 705 that require walls that may exceed the IC Tech Spec-for ICD/ICS 705. For example, the size of stud and gauge of the metal stud will vary depending on if this is a load bearing, non-load bearing or exterior wall. In some cases, walls may have to span heights greater than normal. For these cases, the stud size or gauge may be increased to reduce wall deflection. For exterior walls, the stud thickness is typically a minimum of 6" (152mm) depending on the thermal insulation requirements of the building envelope. These designs will exceed the IC Tech Spec-for ICD/ICS 705 required STC rating but should not require a waiver since the design exceeds the standard based on other criteria.

#### **3-4.4.2 Gypsum Board.**

IC Tech Spec-for ICD/ICS 705 indicates 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) of the protected area to meet STC 45, see Figure 3-3. The STC 50 wall in IC Tech Spec-for ICD/ICS 705 indicates four layers. Two layers on the outside and two layers on the inside, see Figure 3-4.

- 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.

---

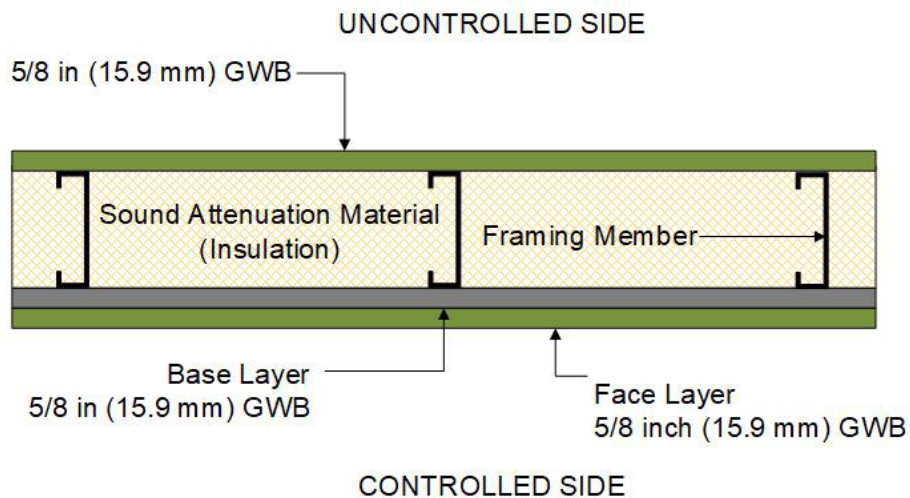
<sup>5</sup> IC Tech Spec – for ICD/ICS 705

Exception: When using adhesive between the layers, joints in the face layer do not have to occur over the framing member

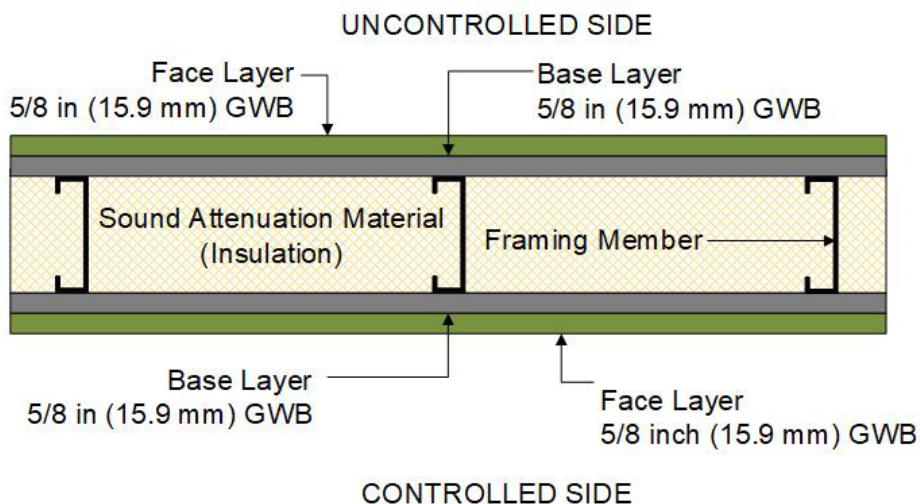
### 3-4.4.3 Factory-Laminated GWB.

To enhance the sound attenuation of the assembly, one layer of factory laminated GWB meeting ASTM C1766 may be used. GWB meeting ASTM C1766 is designed for sound control systems and is composed of two layers of gypsum panels factory-laminated into a composite panel.

**Figure 3-3 STC 45 Assembly**



**Figure 3-4 STC 50 Assembly**



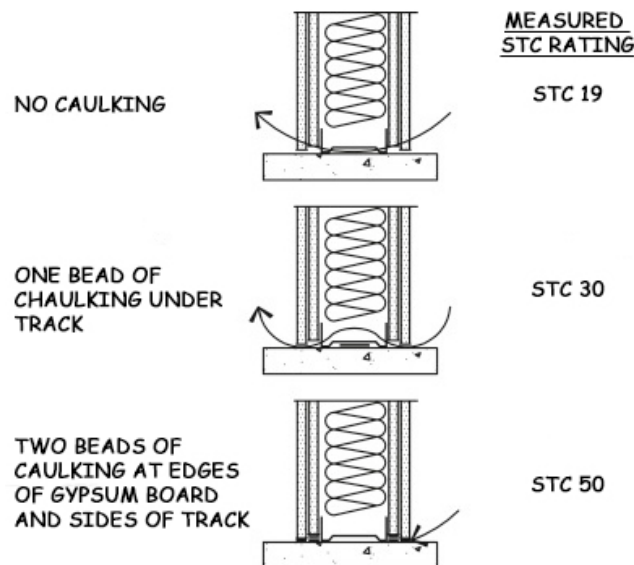
#### 3-4.4.4 Insulation.

Use fibrous insulation to improve the sound isolating performance of the system. Over-packing the cavity may decrease the performance. In addition, the use of spray foam or other hardening insulations may decrease the sound performance.

#### 3-4.4.5 Sealing Gaps.

Gypsum board panels are lifted into place during construction using a spacer under their bottom edge, so there is a 1/8 inch to 1/4 inch (3 mm to 6 mm) gap at the bottom. Sealing openings in partitions is critical to acoustical performance. Seal gaps on both sides with a non-hardening caulk so the acoustical rating of the wall is maintained. Figure 3-5 shows how sealing the gaps effect the STC ratings of the connection.

**Figure 3-5 Sealing Tracks**



#### 3-4.4.6 Wall Finish.




Walls must be uniformly finished and painted from floor slab (true floor) to underside of floor or roof deck (true ceiling). See Figure 3-6.

#### 3-4.4.7 Utilities on Perimeter Wall.

Utilities such as power, telecommunications, signal, and plumbing on the perimeter or compartmented wall treated for acoustic or RF must be surface mounted or construct a furred out wall for routing of utilities. This include recessed outlet boxes, recessed panels for power, telecommunications, ESS, fire alarm and other systems. Do not mount utilities in a manner that will affect the acoustic or RF shielding performance.

If a furred out wall is used, provide a minimum 3/8 inch (10 mm) gypsum board. The gypsum board only needs to go above the false ceiling. Figure 3-7 shows an example of a furred out wall prior to the installation of the 3/8 inch (10 mm) gypsum board.

Figure 3-6 Wall Finish

	<p><b><u>UNACCEPTABLE</u></b></p> <ul style="list-style-type: none"><li>• Wall not uniformly finished and painted.</li><li>• Wall assembly does not meet acoustic rating<ul style="list-style-type: none"><li>- Wall not continuous and sealed where wall abuts floor pan.</li></ul></li><li>• Wall penetrations not sealed.</li></ul>
	<p><b><u>UNACCEPTABLE</u></b></p> <ul style="list-style-type: none"><li>• Not uniformly finished and painted.</li><li>• Gap between finished and unfinished GWB</li><li>• Gap between unfinished GWB and duct penetration</li><li>• Not finished and painted and the penetrations are not sealed and finished.</li></ul>
	<p><b><u>ACCEPTABLE</u></b></p> <ul style="list-style-type: none"><li>• Wall is true floor to true ceiling</li><li>• Wall is sealed where wall abuts floor pan.</li><li>• Wall is uniformly finished and painted from true floor to true ceiling</li><li>• Wall penetrations are sealed.</li></ul>



**Figure 3-7 Furred Out Wall for Utilities**



#### **3-4.4.8 Recessed Fire Extinguisher Cabinets.**

Recessed fire extinguisher cabinets are prohibited on perimeter or sound rated compartmented area walls.

#### **3-4.5 Ceilings and Floors.**

Ceilings and floors must meet the same requirements as walls with regard to forced entry, covert entry, visual evidence of surreptitious penetration, and sound attenuation. In addition, ceilings, floors and all penetrations must meet TEMPEST requirements when recommended by the TCR

#### **3-4.6 Perimeter Doors.**

Perimeter doors and frame assemblies must meet acoustic requirements unless declared a non-discussion area and protected by IDS. Provide dead bolts for perimeter doors with day access controls for occupants. In addition, perimeter doors must meet TEMPEST requirements when recommended by the TCR. All perimeter doors must be solid with no lites or sidelites.

##### **3-4.6.1 Acoustic Rated Doors.**

Use UFGS 08 34 73 to specify acoustical rated door assemblies to include door, seals, hinges, door closer, frame and threshold. Provide door assemblies that are factory tested in accordance with ASTM E90 to no less than STC 50 when a STC 45 perimeter is required and no less than STC 55 when STC 50 perimeter is required. This will help ensure the door assemblies meet the minimum STC requirement when installed correctly.

Acoustical rated door assemblies are much heavier than typical doors and require heavy-duty hardware and structurally adequate support. For acoustics, utilize structural C or U channel in lieu of tubing. Coordinate design of structural support with a Structural Engineer and install in door assembly in accordance with UFGS 08 34 73 and manufacturer's instructions.

#### **3-4.6.2 Wood doors.**

When used, wood doors must meet following minimum specifications:

- 1 ¾ inch (45 mm) thick solid wood core (wood stave, structural composite lumber).
- Lock area predrilled.

#### **3-4.6.3 Steel Doors.**

At a minimum, steel doors must meet following specifications:

- 1 ¾ inch (45 mm) thick face steel equal to 18 gauge.
- Lock area predrilled and reinforced to 10 gauge.

#### **3-4.6.4 Door Closers.**

Equip perimeter doors with a heavy-duty automatic non-hold door-closer installed internal to the perimeter the installation area reinforced to a minimum of 12 gauge for a steel door and at the top rail for a wood door.

#### **3-4.6.5 Electric Locks.**

Electric door strikes or electrified mortise locks installed with an access control system (ACS) must have a positive engagement, fail secure, and approved under UL 1034 for burglar resistance.

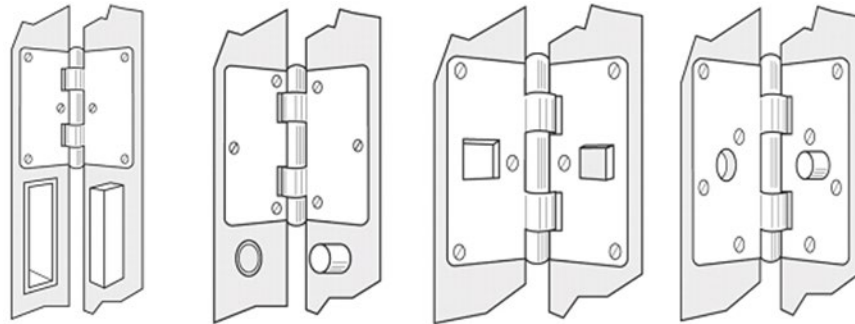
#### **3-4.6.6 Hinges.**

Hinges must be reinforced to a minimum of 7 gauge, and be cam-lift for acoustical door assemblies.

##### **3-4.6.6.1 Hinge Pins.**

Hinge pins on perimeter doors must be tamper resistant unless mounted on the protected side of the door. Tamper resistant hinges must have non-removable pins, security pins, set screws, welded, or equipped with a safety stud. See Figure 3-8.

**Figure 3-8 Tamper Resistant Hinges**



### **3-4.6.7 Primary Entrance.**

Unless approved by the AO, provide one primary entrance where visitor control is conducted. Primary entrance must be:

- Equipped with an approved automated access control device.
- Equipped with a GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890.
- Equipped with combination lock meeting Federal Specification FF-L-2740.
- Equipped with a key override in the event of a malfunction or loss of power to the ACS.

### **3-4.6.8 Secondary Entrance.**

In addition to the primary entrance, a secondary entrance may be allowed with AO approval. As with the primary entrance, the secondary entrance should incorporate a vestibule to preclude visual observation and enhance the acoustic protection. Secondary entrance must be:

- Equipped with an approved automated access control device.
- Equipped with a GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890. Additional standalone and flush mounted deadbolts are prohibited.

### **3-4.6.9 Primary and Secondary Entrance Vestibule.**

When practical, the primary and secondary entrance should incorporate a vestibule to preclude visual observation and enhance acoustic protection. Primary entrance vestibule may have to accommodate space for visitor check-in and badging. In most applications, the interior door of the vestibule will be sound rated and the secure perimeter. To improve acoustic protection, provide acoustic treatments in vestibules to help absorb and diffuse sound.

### **3-4.6.10 Emergency Exit Doors.**

Emergency exit doors must meet perimeter door requirements and:

- Have no exterior hardware; see Figure 3-9.
- Equipped with a GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890. Additional standalone flush-mounted deadbolts are prohibited.
- Alarmed 24/7 and equipped with a local annunciation.
- Delayed-egress is recommended with NFPA 101 compliance.

**Figure 3-9 Emergency Exit Doors**



### **3-4.6.11 Vault Doors.**

General Services Administration (GSA)-approved Class 5 vault door equipped to meet Architectural Barriers Act (ABA) Standards. General Services Administration (GSA) has authorized the use of federal specification AA-D-600D for vault doors.

### **3-4.6.12 Roll-up Doors.**

Roll-up doors can only be located in an area of non-discussion due to the inability to treat for acoustics. Roll-up doors must be 18 gauge or greater and secured with dead bolts on each side of the door.

### **3-4.6.13 Double Doors.**

Double doors should not be used on the perimeter. If double doors are used:

- Secure one side with deadbolts at the top and bottom.
- Provide an astragal strip attached to either door to prevent observation into the space through the opening between the doors.
- Provide an independent high security switch (HSS) level 2 on each door.

### 3-4.7 Personal Electronic Device (PED) Cabinets.

Provide lockable metal cabinets outside the primary entrance for the storage of PEDs, see Figure 3-10. PED cabinets cannot be located within 10 ft. (3 m)<sup>6</sup> of equipment processing unencrypted NSI. Recessed PED cabinets are prohibited on perimeter walls.

**Figure 3-10 PED Cabinets**



### 3-4.8 Windows.

Every effort should be made to minimize windows, especially on the ground floor. When used, windows must be non-opening, be provide visual and acoustic protection and include TEMPEST requirements when recommended by the TCR.

#### 3-4.8.1 Windows less than 18 feet (5.5 meters).

Windows less than 18 feet (5.5 meters) (measured from the bottom of the window) above the ground or from the nearest platform; such as lower roof, canopy or mechanical equipment, which affords access to the window must:

- Meet the standards of the perimeter
- Monitored by IDS

Large glazing panels may require noise generator transducers to achieve acoustic protection.

### 3-4.9 Daylighting.

Secure facilities are not exempt from the high performance building requirements of UFC 1-200-02. Promote access to daylight in breakrooms and other common spaces.

---

<sup>6</sup> DoDM 5105.21-V2 and CNSSAM TEMPEST/1-13

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.

#### **3-4.9.1 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 fenestration) above the ground or from the nearest platform; such as lower roof, canopy or mechanical equipment, which affords access to the fenestration or accessible from the roof must:

- Meet the standards of the perimeter
- Monitored by IDS

#### **3-4.10 Visual Protection of Windows and Daylighting Fenestration.**

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 light transmission. Specify a maximum of 75% diffuse transmittance and a minimum haze of 90% when tested in accordance with ASTM D1003.

For existing windows, blinds, drapes or other coverings may be used with SSM/SSO approval.

#### **3-4.11 Perimeter Penetrations.**

Keep penetrations of the perimeter to a minimum. Ducts, conduits, pipes, or anything that penetrates the perimeter presents a vulnerability that must be addressed. All penetration must meet the acoustic requirements of the perimeter. In addition, perimeter penetrations may require TEMPEST countermeasures when recommended by TEMPEST Countermeasure Review.

Ducts, conduits or pipes servicing other areas cannot penetrate the perimeter unless mitigated with AO approval.

##### **3-4.11.1 Utility Penetrations.**

Utilities (power and signal) should enter at a single point. Seal all utility penetrations 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 or a Fire Stop System may be required for fire rated assemblies.

##### **3-4.11.2 Metallic Penetrations.**

All metallic penetrations through the perimeter are considered carriers of compromising emanations (CE) and pose TEMPEST hazards that must be addressed. Unless directed otherwise by the TEMPEST Countermeasure Review:

- Metal conduit or pipe: provide a nonconductive union inside the perimeter adjacent to the penetration, or ground the conduit within 6 inch (150 mm) of the perimeter penetration using a no. 4 wire (0.2043-diameter copper wire) to the building grounding system.
- Metallic sprinkler (fire suppression) pipe: ground the pipe within 6 inch (150 mm) of the perimeter penetration using a no. 4 wire (0.2043-diameter copper wire) to the building grounding system.
- Mechanical system refrigerant lines: ground the line within 6 inch (150 mm) of the perimeter penetration using a no. 4 wire (0.2043-diameter copper wire) to the building grounding system. Maintain integrity of refrigerant line insulation.
- HVAC ducts: provide a nonconductive break (flex connection) using material appropriate for the climate, for a 2- to 6-inch (50 to 150 mm) section of the duct inside the perimeter adjacent to the penetration, see Figure 3-11. When a waveguide is recommended by TEMPEST Countermeasure Review, provide between the perimeter and the nonconductive break.

In addition, the TEMPEST Countermeasure Review may require additional countermeasures.

**Figure 3-11 Duct Penetrations**



### **3-4.11.3 Penetration Seals.**

Seal both sides of perimeter penetrations with an acoustical foam or sealant finished to match adjacent wall, floor, or ceiling see Figure 3-12. Fire Stop System may be required for fire rated assemblies. In addition, penetration seals must meet TEMPEST requirements when recommended by the TEMPEST Countermeasure Review.

**Figure 3-12 Sealing Penetrations**



### **3-4.12 Vents and Ducts.**

Protect all vents or duct openings exceeding 96 square inches (619 cm<sup>2</sup>) that penetrate the perimeter with permanently affixed bars, grills, diamond mesh, welded wire fabric, metal sound baffles or waveguides. If one dimension of the penetration measures less than 6 inch (150 mm), protection is not required. One of the following can be used to secure openings 6-inches (150 mm) or more in any dimension.

- A minimum of ½ inch (13 mm) diameter steel bars welded vertically and horizontally 6 inch (150 mm) on center. A deviation of ½ inch (13 mm) in vertical and/or horizontal spacing is permissible, see Figure 3-13.
- ¾ inch (20 mm) #9 (10 gauge) case hardened expanded metal grills.
- Carbon steel standard expanded metal diamond mesh, 1-1/2" (38 mm) #10 (13 gauge). With a maximum design size of 1-3/8" by 3" (35 mm x 76 mm), strand size thickness of 0.093" (2.36 mm), with at least 80% open design).
- Welded wire fabric (WWF) 4x4-W2.9xW2.9 (6 gauge) smooth steel wire welded vertically and horizontally four inches on center.
- Metal sound baffles or waveguide permanently installed and set no farther apart than 6 inch (150 mm) in one dimension.

Coordinate material selection with Mechanical Engineer to ensure proper airflow and fan sizing.



**Figure 3-13 Bars on Penetration**

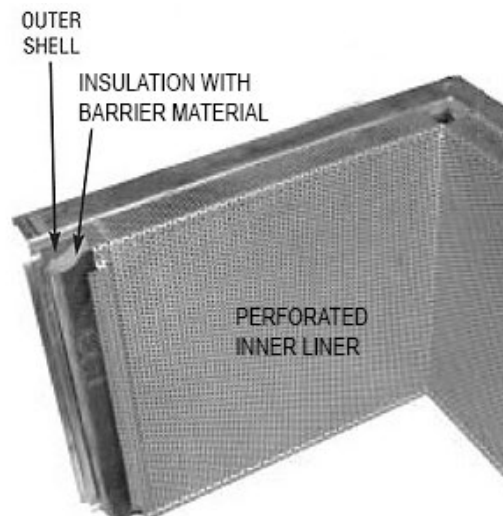


**3-4.13 Acoustic Protection for Ducts.**

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 the mechanical engineer. Backpressures created by the baffles may significantly impact the HVAC system design.

Be aware, (Z) Duct Penetration in 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, see Figure 3-14. For contamination protection, include a barrier material between the perforated liner and the insulation designed to prevent air quality issues caused by bacteria and other contaminants that can embed in the insulation.

**Figure 3-14 Double Wall Acoustic Duct**

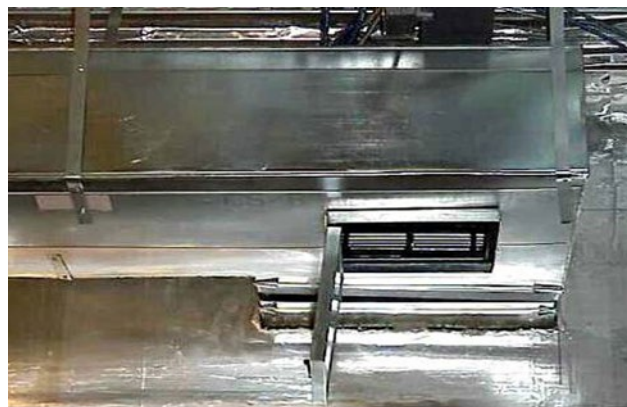


### 3-4.14 Access Port.

For vents or ducts that require bars or grill, provide an accessible access panel in the bottom within the perimeter to allow visual inspection of the bars, grill, or waveguide, see Figure 3-15.

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 an AO approved high-security lock such as a GSA combination padlock meeting Federal Specification FF-P-110.

**Figure 3-15 Access Port**



### 3-4.15 Flashing or Rotating Light.

Per DoDM 5105.21 Vol 2 and DoDM 5205.07 Vol 2, personnel must be informed when non-indoctrinated personnel have entered and departed the space. Per IC Tech Spec, Lights, signs, or other alerting mechanisms or procedures must be used to alert occupants of the presence of uncleared personnel. This may be accomplished either verbally or through visual notification methods. A flashing or rotating light is an approved method to indicate the presence of non-indoctrinated personnel in the area. This can be hand held or installed.

Coordinate use of flashing or rotating notification lights with mission requirements. There may be light-sensitive or simulation equipment that preclude use of such light during ongoing operations. When installed, place lights to ensure visual observation by the occupants of the space. At a minimum, provide controls within the perimeter at each entrance into the space or compartmented area.

### 3-4.16 Duress Alarm.

When a duress alarm is required, duress alarm must initiate an alarm condition at the central monitoring station and no audible or visual signal in the protected area.

### **3-4.17 Electronic Security System (ESS).**

An ESS is comprised of three primary subsystems; intrusion detection system (IDS), access control system (ACS), and video system along with a supporting data transmission network and electrical power system.

ESS systems must meet the requirements of ICS 705-1 and IC Tech Spec-for ICD/ICS 705 and be designed in accordance with UFC 4-021-02. UFC 4-021-02 provides notional layouts for typical ESS systems.

#### **3-4.17.1 Access Control System (ACS).**

At a minimum, provide card reader with keypad at the primary entrance and when provided, the secondary entrance. Unless otherwise directed, the default ACS identifier credential is the Common Access Card (CAC)<sup>7</sup>.

- Locate equipment containing access-control software programs within the perimeter or a SECRET controlled area.
- Protect system data that is carried on transmission lines (e.g., access authorizations, personal identification, or verification data) to and from equipment located outside the perimeter using FIPS AES certified encrypted lines. If this communication technology is not feasible, provide transmission lines as approved by the AO.
- Provide electric locks with positive engagement, fail secure, and approved under UL 1034 for burglar resistance.

#### **3-4.17.2 Video System.**

Cameras are not allowed within the perimeter or enable observation within the perimeter. A camera may be provided on the exterior to supplement the monitoring of a primary entrance for remote control of the door from within the space. A Video Intercom System may provide this capability. The system must provide a clear view of the primary entrance that is monitored and operated by indoctrinated personnel.

#### **3-4.17.3 Intrusion Detection System (IDS).**

Protect the space with IDS when not occupied. Protect all Interior areas through which reasonable access to the asset could be gained with IDS.

- The IDS must be independent of systems safeguarding other facilities and compatible with Installation's central monitoring system.
- Provide point sensors on perimeter doors and man-passable openings such as roof hatches.
- Provide motion sensors within the perimeter to protect perimeter windows, doors, daylight fenestrations, and man-passable openings.

---

<sup>7</sup> Per DoD 5200.08-R

- Strategically place motion sensors within the space to detect movement where assets are stored or where assets are stored or in pathways leading to the asset. One hundred percent coverage is not required.
- Motion sensors are not normally 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.
- Monitor emergency exit doors 24 hours a day. Provide local annunciation to alert occupants when the door opened with identification of the appropriate door when there is an alarm indication.

#### **3-4.17.3.1 Intrusion Detection Installation and Components.**

Per IC Tech Spec – for ICD/ICS 705, IDS installation, related components, and monitoring stations must 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 must comply with UL 2050 Extent 3 standards for installation. UL 2050 materials are restricted and only distributed to those demonstrating relevant national industrial security involvement. However, UL 2050 implements UL 681, Installation and Classification of Burglar and Holdup Alarm Systems for alarm system installation. See UFC 4-021-02 for additional information and a notional ESS layout.

#### **3-4.17.3.2 Motion Detection Sensors.**

UL 639 Listed. Dual-technology sensors may be used when authorized and when each technology transmits alarm conditions independent of the other technology (“or” configuration).

#### **3-4.17.3.3 Point Sensors.**

UL 634 HSS level 2. Level 2 rated switches only include Balanced Magnetic Switches that pass additional performance testing.

#### **3-4.17.3.4 Sensor Cabling.**

Cabling between sensors and the PCU must be dedicated to the system, contained within the perimeter, and comply with Committee for National Security Systems (CNSS) standards. If the wiring cannot be contained within the perimeter, meet the requirements for External Transmission Line Security.

#### **3-4.17.3.5 Premise Control Unit (PCU).**

Locate PCU within the Perimeter. Configure system to only allow cleared personnel located within the secure/protected area to initiate changes in access modes or alarm conditions.

PCUs certified under UL 1610 must meet FIPS 197 or FIPS 140-2 encryption certification and methods. For PCUs certified under UL1076, only FIPS 140-2 is the acceptable encryption certification and method.

#### **3-4.17.3.6 External Transmission Line Security.**

IDS transmission lines to the central monitoring station, must meet National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) certified encrypted lines.

All lines employing line supervision require certification of the algorithm by the National Institute of Standards and Technology (NIST) (a NIST certificate). An alternate form of line supervision may be approved on a case-by-case basis.

#### **3-4.17.3.7 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.

In the event of primary power failure, the IDS must:

- Automatically transfer to the backup power source without causing alarm activation.
- Initiate an audible or visual indicator at the PCU to provide an indication of the primary or backup power source in use.
- Initiate an audible or visual indicator at the monitoring station indicating a failure in a power source or a change in power source.

#### **3-4.17.3.8 IDS Approval.**

The AO must approve IDS proposals and plans prior to installation as part of the pre-construction approval process.

#### **3-4.18 Telecommunications Space.**

Per UFC 3-580-01, the minimum size for Telecommunications Room (TR) is 10 feet x 8 feet (3m x 2.4m). This will be inadequate if the telecommunications space contains equipment racks for multiple networks such as Secret Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS), Non-classified Internet Protocol Router Network (NIPRNet), voice services, and other equipment or services. Depending on the number of workstations served, this could generate a larger space requirement when considering the equipment racks and RED/BLACK separation requirements.

UFC 3-580-01 allows the use of an Equipment Room in lieu of a TR for buildings that house substantial Information Technology (IT) electronics. A telecommunication space that contains equipment for multiple networks such as SIPRNet, JWICS and NIPRNet all requiring RED/BLACK separation is considered as substantial Information Technology (IT) electronics which would allow for the use of a larger Equipment Room.

#### **3-4.18.1 Telecommunications Expansion.**

Design the telecommunication spaces to accommodate future equipment expansion. At a minimum, UFC 3-580-01 requires one spare rack for every four utilized racks with the minimum of one spare rack. Future operational capability for these types of facilities may require additional expansion space. Coordinate future expansion capabilities with mission commander and the C5ISR equipment provider. Provide additional power, environmental support, and floor space for the future expansion.

#### **3-4.18.2 Temperature and Humidity Control.**

Substantial Information Technology (IT) equipment generate a significant amount of heat. In these environments, the heat densities can be up to five times higher than in a typical office load. Traditional HVAC systems cannot remove enough heat to protect IT equipment. Instead, these areas require systems with higher cooling capabilities such as a computer room air conditioner (CRAC). The smallest high-powered CRACs require a minimum 10 ft. x 3 ft. (3m×1m) footprint for equipment and clearances.

Design air-conditioning systems for year-round cooling with very high cooling intensity. The high sensitivity of electronic components in such facilities requires that temperature, humidity, air movement and air cleanliness must be kept consistent and within specific limits to prevent premature equipment failures and costly downtime.

#### **3-4.19 Telecommunication Cabling System.**

Cabling, patch panels, connector blocks, work area outlets, and cable connectors must be color coded<sup>8</sup> to distinguish their classification level. If color-coding is not possible, cabling must be clearly marked to indicate their classification level. Cabling must enter the protected area from a single location and must 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 requirements. Coordinate requirements with SSM and service provider. See TEMPEST Countermeasures.

#### **3-4.20 Protected Distribution Systems (PDS).**

Protect signal distribution systems containing unencrypted NSI that enters an area of lesser classification, unclassified area, or uncontrolled (public) area with a PDS in accordance with CNSSI No 7003.

---

<sup>8</sup> Per DoDM 5105.21 Vol 1

Avoid the use of PDS whenever possible due to inspection requirements. To avoid PDS, keep cabling transmitting unencrypted NSI within the protected perimeter.

### **3-4.21 RESILIENCE.**

Some facilities must continue to operate effectively or recover rapidly to support the mission in the event of severe weather, earthquake, loss of utility, or equipment failure. Defining the appropriate International Building Code (IBC) Risk Category is critical in determining the earthquake, flood, snow and wind load requirements that will apply to the building. Some critical operations or C5ISR systems require redundant utilities, standby power systems, and redundant support systems to ensure continuous operation in the event of utility or equipment failure.

Coordinate resiliency requirements with the mission commander.

#### **3-4.21.1 Redundant Utilities.**

Critical operations or C5ISR systems may require redundant utilities such as telecommunication system connectivity or utility power service. To be redundant, the utilities providing connectivity or power to the facility must be two separate utilities that are not routed together.

#### **3-4.21.2 Standby Power System (SPS).**

Critical operations or C5ISR systems may require an SPS designed to ensure continuity of electrical power to essential and uninterruptible loads upon loss of normal power sources. Design SPS in accordance with NFPA 70 and NFPA 110. The SPS must have the capacity and rating to meet the maximum demand likely to be produced by the essential and uninterruptible loads and be consistent with the facilities emergency operations plan.

##### **3-4.21.2.1 Engine-Driven Generator.**

When a SPS is required, provide a standby engine-driven generator for essential and uninterruptible loads to ensure continued operation upon loss of utility power. Design the standby generator in accordance with UFC 3-540-01.

##### **3-4.21.2.2 UPS Systems.**

When a SPS is required, provide UPS for the uninterruptible loads to filter commercial power and to support the uninterruptible loads during transitions to and from the standby generator.

#### **3-4.21.3 Redundant Support Systems.**

Some critical operations may require support systems with a minimum of N+1 redundancy to ensure continuous operation in the event of component failure. In this configuration, components (N) have at least one independent backup component (+1). For a critical communication system, the N+1 redundancy would be applied to support

systems such as the air-conditioning systems and SPS required to support continuous operation. For example, if the essential and uninterruptible loads required two 250 kW generators, N+1 would result in three 250 kW generators.

### **3-4.22 TEMPEST.**

TEMPEST is a short name referring to investigation, study and control of compromising emanations from telecommunications and automated information systems equipment. In general, TEMPEST countermeasures apply when there is equipment that will be processing national security information (NSI). The intent is to minimize the likelihood that these emanations will be intercepted.

#### **3-4.22.1 TEMPEST Countermeasures Review (TCR).**

Each project requires a TEMPEST countermeasures review (TCR), performed or verified by the Certified TEMPEST Technical Authority (CTTA). The SSO or SSM will request a TCR by submitting a TEMPEST addendum to the FFC. For an initial TCR, the TEMPEST addendum will be submitted to AO during the preliminary design phase. 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. Based on the results of the TCR, the CTTA will determine the most cost-effective countermeasures and will document these requirements in writing<sup>9</sup>.

#### **3-4.22.2 TEMPEST Countermeasures.**

TEMPEST-suppressed equipment, radio frequency (RF) shielded enclosures, filters (power, signal, telephone, etc.), nonconductive conduit or duct sections, or other potentially expensive TEMPEST countermeasures must not be applied without AO approval. Normally, facilities located on military installations within the United States do not require additional countermeasures beyond implementing RED/BLACK separation guidance depending on threat and mission requirements. However, facilities that are located outside the U.S., off a military installation, in close proximity with a foreign entity; or facilities that share a common wall, floor, or ceiling with a non-government element may require additional measures beyond implementing RED/BLACK separation<sup>9</sup>. These additional measures are determined through the TCR process and approved by the AO.

#### **3-4.22.3 RED/BLACK Telecommunication Systems.**

All equipment, wirelines, components, and systems that process National Security Information (NSI) are considered RED. Equipment, wirelines, components, and systems that process encrypted NSI and non-NSI are considered BLACK. 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 such as separation and filtering are

---

<sup>9</sup> DoDM 5105.21 Vol 2 and DoDM 5205.07 Vol 3



used to protect the signal line, the distribution system or other fortuitous conductors from conducting compromising signals beyond secure areas.

Apply fundamental RED/BLACK mitigations in accordance with CNSSAM TEMPEST/01-13 to prevent the inadvertent transmission of classified data over telephone lines, power lines, signal lines, and electrical components, circuits, and communication media. The application of RED/BLACK separation establishes areas where equipment processing classified information (RED) are isolated from areas where equipment processing unclassified (BLACK) are located.

#### **3-4.22.4 Radio Frequency (RF) Mitigation.**

As documented in the TCR, protect the space from compromising emanations. When directed, provide RF mitigation for perimeter walls, ceilings, floors, doors, windows, skylights and penetrations with RF shielding, non-conductive breaks, and grounding. RF mitigations for penetrations may include waveguides.

When required, place foil layer on the secure side of the perimeter wall between the first and second layer of gypsum board. When required, place RF shielding material on floor and ceiling. Doors must be steel with RF gasket, and door frame must be electrically bonded continuously to RF shield. Entire window or skylight assembly must be RF shielded and window or skylight frame and must be electrically bonded continuously to RF shield. Shielding must be electrically bonded continuously, with no gaps or discontinuities at any point, at interfaces between, walls, floors, ceilings, doors, windows, and skylights and penetrations. Power and low voltage systems may include power line and telecommunication line filters. Refer to *Best Practices Guidelines for Architectural Radio Frequency Shielding* for standard construction for RF shielding.

- Do not connect mounting apparatus to the RF shielding material in a manner that affects RF shielding performance.
- Consider providing furred out walls to protect RF shielding from future compromise.

#### **3-4.22.5 RF Door ABA Compliance.**

RF doors that utilize a knife-edge may not meet ABA Standards without modification due to accessibility requirements at the sill, see Figure 3-16. The use of temporary ramps will not meet ABA Standards.

#### **3-4.22.6 Paging, Intercom, and Public Address Systems.**

Systems should be totally contained within the perimeter. Refer to the TCR to determine TEMPEST countermeasures. Possible countermeasures may include:

- Separation of equipment and signal lines from RED telecommunication lines and processors.
- Provide a local buffer amplifier to prevent speakers or earphones from functioning as microphone. For most systems, this is a simple amplifier

within the perimeter that takes the incoming audio signal and amplifies/distributes the signal to the speakers within the perimeter.

- Provide electronic isolation for systems that require two-way communication. The system must alert occupants when the system is activated.
- Provide voice frequency, bandpass filters if they are not totally contained within the inspectable space. This protects against TEMPEST signals on the cables but does not protect against voice modulation of the speakers.
- Provide a subpanel within the perimeter with optical fiber backbone to the building system or convert the electrical signal to an optical signal before penetration of the perimeter. Provide optical fiber with no metallic shielding, cladding, or strength members.
- When required, provide electronic isolation components within the perimeter as near to the point of penetration as possible.

**Figure 3-16 ABA Non-Compliant RF Door**



#### **3-4.22.7 Fire Alarm and Mass Notification System (MNS).**

The introduction of electronic systems that have components outside the perimeter should be avoided. TEMPEST concerns may require electronic isolation. Speakers or other transducers, which are part of a system that is not wholly contained within the perimeter, may require mitigation. Refer to the TCR to determine TEMPEST countermeasures. Possible countermeasures may include:

- Separation of equipment and signal lines from RED telecommunication lines and processors.
- For eavesdropping (using the speakers as microphones), a simple buffer amplifier is the standard mitigation. For most systems, this is a simple amplifier within the perimeter that takes the incoming audio signal and amplifies/distributes the signal to the speakers within the space. However, equipment such as pre-amplifiers, amplifiers and products translating or converting live voice signals for use in mass notification systems must comply with the applicable requirements in UL 864, the Standard for Amplifiers for Fire-Protective Signaling Systems. Therefore, any amplifier used in a MNS must meet UL 864.
- Provide a MNS/Fire alarm subpanel within the perimeter with optical fiber backbone to the building system or convert the electrical signal to an optical signal before penetration of the perimeter. Provide optical fiber with no metallic shielding, cladding, or strength members.
- Provide electronic isolation for systems that require two-way communication. The system must alert the occupants when the system is activated.
- When required, provide electronic isolation components within the perimeter as near to the point of penetration as possible.

#### **3-4.22.8 Power Systems.**

The power requirements are divided into two groups -- power for the mission equipment (technical) and power for the supporting services (nontechnical). Supporting services include lighting, heating, ventilating, air conditioning, etc. Provide a separate service feeder dedicated to the sensitive equipment and control its distribution reducing the opportunity for unauthorized detection of compromising signals on those lines. Power line conduction occurs when data is transferred onto the power line by RED equipment, or radiated through free space and coupled onto the power lines. If a facility is processing NSI, power is sometimes divided into RED and BLACK power. RED power provides isolation for those non-TEMPEST approved equipment processing NSI. BLACK power is provided for equipment processing non-NSI because power isolation is not required. This separation prevents conducted emissions from RED equipment being coupled through BLACK equipment to BLACK lines that might egress the inspectable space. Refer to the TCR to determine TEMPEST countermeasures. Possible countermeasures may include:

- Separation of BLACK power lines from RED telecommunication lines and processors.
- Power line Filters. UPS within the perimeter may eliminate power line filters.

### **3-4.22.9 RF Communications Systems.**

Facilities that require large RF communications systems (combat net radios, microwave systems, air to ground, or ship to shore) should be designed to place RF communications systems as far away from RED processors as possible.<sup>10</sup>

---

<sup>10</sup> DoDM 5105.21 Vol 2

## CHAPTER 4 CONSTRUCTION

### 4-1 CONSTRUCTION AWARD.

Per IC Tech Spec – for ICD/ICS 705, prior to awarding a construction contract, a CSP for each project must be approved by the AO. The CSP documents the security requirements for the project. For Navy and Marine Corps projects, refer to NAVFAC INST 4700.01 for additional information.

### 4-2 CONSTRUCTION PLANS SECURITY.

Per ICS 705-1, protect and handle construction plans and related documents in accordance with the CSP. If classification guides dictate, plans and related documents may require classification. Under no circumstances should plans, diagrams, etc. that are identified for a SCIF or SAPF be sent or posted on unprotected information technology systems, networks or Internet venue without encryption.

### 4-3 CONSTRUCTION SITE SECURITY.

The SSM is the single point of contact regarding security and the individual responsible for the security aspects of the construction. The SSM will have 24-hour unrestricted access to the site to conduct periodic security inspections for the duration of the project. DoDM 5105.21 Vol 2 defines the minimum security requirements for the SCIF construction site. DoDM 5205.07 does not identify minimum security requirements for the SAPF construction site.

Refer to the CSP for the project specific security requirements.

### 4-4 ACCREDITATION PROCESS.

In support of the accreditation process and the updating of the FFC, and other required documentation, Project/Construction managers will provide the SSM site plans, building floorplans, IDS plans, and information related to the perimeter's construction, penetrations, doors, locks, deadbolts, IDS, telecommunication systems, acoustical protection, low voltage systems, electrical power systems, and TEMPEST countermeasures. For SCIFs, refer to DoDM 5105.21 Vol 2, and for SAPFs, refer to DoDM 5205.07 Vol 3.

### 4-5 INSPECTIONS.

Coordinate preliminary walkthrough with the SSM prior to substantial completion of the space. SSM conducts periodic inspections of the area to validate and document elements for accreditation. Inspection elements may include:

- Perimeter construction
  - 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

- Top and bottom of walls are sealed (both sides) with acoustical foam or sealant
- Acoustic insulation is securely fastened
- Gypsum Wallboard installation
- Floor and Ceiling construction
- Perimeter Penetrations
  - Sealed (both sides) with acoustical foam or sealant
  - Finished to match wall
- Perimeter Doors
  - Door assemblies sealed with acoustical foam or sealant (both sides) and finished to match wall
  - Door hardware (locks, closers, sweeps and hinges)
  - ASTM E90 laboratory Test Report
  - ASTM E336 field Test Report
- HVAC Systems
  - Man-bar installation
  - Inspection Ports
  - Nonconductive break
  - Acoustic mitigation
    - Z-duct installation or sound baffle installation
- ESS installation
- TEMPEST Countermeasures (as applicable)
  - RED/BLACK LAN separation
  - Metallic penetrations at perimeter (non-conductive break or grounded at the interior perimeter)
  - RF shielding including penetrations
  - Waveguides
  - Doors including RF gaskets
  - Power Line Filters
  - Signal Line Isolators and Filters

#### **4-6 CONSTRUCTION DRAWINGS AND SUBMITTALS.**

Prior to walk through; assemble required documents in support of the accreditation process. Requirements vary depending on project but in general assemble the following documents:

- Drawings:
  - Civil Site Plan
  - Architectural
    - Floor and Reflective Ceiling Plans
    - Perimeter wall sections (floor to ceiling)
    - Floor and Ceiling section
    - Door Schedule
    - Perimeter Door head, jamb, and threshold details
    - Window schedule and details
  - Fire Protection
    - Sprinkler piping grounding and penetration details
    - Low voltage cabling penetrations
    - Fire Alarm system
    - Mass Notification System
  - Mechanical
    - HVAC plans, sections and details of perimeter penetrations, ductwork details sheets
    - Plumbing floor plans, detail for perimeter penetrations
  - Electrical
    - Site plan
    - Lighting, Power, Telecommunications, Grounding, and ESS plans. Plans must indicate device and panel locations and when provided, include strobe lights and controls
    - One-line diagrams for Power, Telecommunications including RED/BLACK separation, and ESS
    - ESS door wiring details
    - Perimeter penetration details
- Submittals
  - Doors
  - Door Hardware (locks, closers, and hinges)
  - Acoustical rated assemblies
    - ASTM E90 Test Reports
  - Electronic Security Systems
  - TEMPEST Countermeasures (as applicable)

- Non-metallic breaks
- RF shielding
- RF sealant
- Waveguides
- RF Shielded Doors including RF gaskets
- RF Shielded Windows
- Power Line Filters
- Signal Line Isolators and Filters
- RF Shielding Test Reports (as applicable)
- As-Built drawings

#### **4-7 PHOTOGRAPHIC CONSTRUCTION SURVEILLANCE RECORD.**

Photographic Construction Surveillance Record may be accomplished by the SSM or approved personnel to expedite the accreditation process. It is important to capture areas which will be covered up during construction. Pictures should capture:

- Wall construction
  - Stud walls
  - Acoustic insulation
  - Enhanced wall layer (when applicable)
  - Initial GWB layer installation
  - RF shielding installation
  - Wall penetrations
  - Wall finishes (true floor to true ceiling)
- Duct construction including inspection ports, Z-Ducts, Sound baffles and man-bars.



**APPENDIX A MINIMUM CONSTRUCTION**

**A-1 MINIMUM CONSTRUCTION.**

Table A-1 is provided as a synopsis of the construction and alarm requirements based on the IC Tech Spec-for ICD/ICS 705. Construction is determined on a project-by-project basis by the Commander or their designated SSM working with the AO.

**Table A-1 Minimum Construction and Alarm**

	CLASSIFICATION	TYPE OF CONSTRUCTION <sup>1</sup>	IDS <sup>3</sup>	ACS <sup>4</sup>	DURESS
INSIDE UNITED STATES, ITS POSSESSIONS OR TERRITORIES	Open Storage without SID <sup>5</sup>	Wall B - Enhanced Wall (Expanded Metal) <sup>2</sup> Wall C - Enhanced Wall (Plywood) <sup>2</sup>	YES	YES	NO
	Open Storage with SID <sup>5</sup>	Wall A - Standard Wall <sup>2</sup>	YES	YES	NO
	Closed Storage	Wall A - Standard Wall <sup>2</sup>	YES	YES	NO
	Continuous Operations	Wall A - Standard Wall <sup>2</sup>	YES	YES	NO
	Secure Working Area (SWA)	Wall A - Standard Wall <sup>2</sup>	YES	YES	NO
OUTSIDE UNITED STATES, ITS POSSESSIONS OR TERRITORIES	SETL Cat I <sup>6</sup>				
	Open Storage	Vault <sup>2</sup>	YES	YES	RECOMMENDED
	Closed Storage	Wall B - Enhanced Wall (Expanded Metal) <sup>2</sup> Wall C - Enhanced Wall (Plywood) <sup>2</sup>	YES	YES	NO
	Continuous Operation	Wall B - Enhanced Wall (expanded Metal) <sup>2</sup> Wall C - Enhanced Wall (Plywood) <sup>2</sup>	YES	YES	YES
	SETL Cat II & III <sup>6</sup>				
	Open Storage	Wall B - Enhanced Wall (expanded Metal) <sup>2</sup> Wall C - Enhanced Wall (Plywood) <sup>2</sup>	YES	YES	RECOMMENDED
	Closed Storage	Wall B - Enhanced Wall (Expanded Metal) <sup>2</sup> Wall C - Enhanced Wall (Plywood) <sup>2</sup>	YES	YES	NO
	Continuous Operation	Wall A - Standard Wall <sup>2</sup>	YES	YES	RECOMMENDED
	Secure Working Area (SWA)	Wall A - Standard Wall <sup>2</sup>	YES	YES	RECOMMENDED

Notes:

1. Table indicates the minimum construction from IC Tech Spec-for ICD/ICS 705.
2. Refer to IC Tech Spec-for ICD/ICS 705 for construction definitions and suggested details. Include Radio Frequency (shielding) protection, enhanced construction and sound attenuation as required.
3. IDS - Intrusion Detection System
4. ACS - Access Control System at Primary and secondary (if provided) entrance.
5. SID - Security in Depth
6. Security Environment Threat List (SETL). SETL Categories are classified.

*This Page Intentionally Left Blank*

## APPENDIX B GLOSSARY

### B-1 ACRONYMS.

<b>ACS</b>	Access Control System
<b>AO</b>	Accrediting Official
<b>BIA</b>	Bilateral Infrastructure Agreements
<b>C5ISR</b>	Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance
<b>CA</b>	Compartmented Area
<b>CSA</b>	Cognizant Security Authority
<b>CSP</b>	Construction Security Plan
<b>CTTA</b>	Certified TEMPEST Technical Authority
<b>DNI</b>	Director of National Intelligence
<b>ER</b>	Equipment Room
<b>ESS</b>	Electronic Security System
<b>FFC</b>	Fixed Facility Checklist
<b>HNFA</b>	Host Nation Funded Construction Agreements
<b>HSS</b>	High Security Switch
<b>IC</b>	Intelligence Community
<b>IDS</b>	Intrusion Detection System
<b>JWICS</b>	Joint Worldwide Intelligence Communications System
<b>MNS</b>	Mass Notification System
<b>NIPRNET</b>	Non-classified Internet Protocol Router Network
<b>NSI</b>	National Security Information
<b>PDS</b>	Protected Distribution System
<b>PCU</b>	Premise Control Unit
<b>RF</b>	Radio frequency

<b>SAO</b>	Special Access Program Facility Accrediting Official
<b>SAP</b>	Special Access Program
<b>SAPF</b>	Special Access Program Facility
<b>SCI</b>	Sensitive Compartmented Information
<b>SCIF</b>	Sensitive Compartmented Information Facilities
<b>SETL</b>	Security Environment Threat List
<b>SID</b>	Security-in-depth
<b>SIO</b>	Senior intelligence Official
<b>SIPRNET</b>	Secret Internet Protocol Router Network
<b>SOFA</b>	Status of Forces Agreements
<b>SPS</b>	Standby Power System
<b>SSM</b>	Site Security Manager
<b>SSO</b>	Special Security Officer
<b>STC</b>	Sound Transmission Class
<b>SWA</b>	Secure Working Area
<b>TCR</b>	TEMPEST Countermeasure Review
<b>TR</b>	Telecommunications Room
<b>TSWA</b>	Temporary Secure Working Areas
<b>UFGS</b>	Unified Facilities Guide Specification
<b>VTC</b>	Video teleconference

**B-2**                    **DEFINITION OF TERMS.**

**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 Equipment:** A term applied to equipment that processes only unclassified and/or encrypted information. (CNSSAM TEMPEST/1-13)

**BLACK LAN:** A term applied to equipment, cables, or fiber that processes or carries only unclassified and/or encrypted information. (CNSSAM TEMPEST/1-13)

**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.

**Classification Guide:** A documentary form of classification guidance issued by an Original Classification Authority (OCA) that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. (ODNI 80.16)

**Cleared American Guard:** A U.S. Secret cleared guard that performs access control functions to screen all non-cleared workers, vehicles, and equipment entering or exiting the site and conducts random inspections of site areas. (IC Tech Spec – for ICD/ICS 705)

**Closed Storage:** The storage of sensitive material in properly secured GSA approved security containers within an accredited space.

**Cognizant Security Authority (CSA):** The single Principal designated to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods.

**Compartmented Area (CA):** An area, room, or a set of rooms within the accredited space that provides controlled separation between control systems, compartments, sub-compartments, or Controlled Access Programs. (IC Tech Spec – for ICD/ICS 705)

**DoD Construction Agent.** The U.S. Army Corps of Engineers, the Naval Facilities Engineering Systems Command, or such other approved DoD activity assigned the design or construction execution responsibilities associated with the military construction program. (DoDD 4270.5)

**Construction Security Plan (CSP):** The plan developed by the SSM and approved by the AO, which outlines security protective measures that will be applied to each phase of the construction project. (IC Tech Spec – for ICD/ICS 705)

**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. (IC Tech Spec – for ICD/ICS 705)

**Continuous Operation:** This condition exists when the secure space is staffed 24 hours every day.

**Duress Alarm:** A silent alarm signal generated by the manual activation of a device requiring a security force response.

**Equipment Room (ER):** An environmentally controlled, centralized space for telecommunications equipment that usually houses a main or intermediate cross-connect. (UFC 3-580-01)

**Essential Loads:** Loads that require standby power, but can be de-energized until they can be supplied from an engine generator system. Loads in this category usually include HVAC loads to vital facilities or other load types that can be de-energized for short periods without severe consequence. (UFC 3-540-01)

**Fixed Facility Checklist (FFC):** Checklist used by CSAs to determine whether construction requirements have been met.

**Inspectable Space.** The three-dimensional space surrounding equipment that processes classified or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists. Inspectable space may include parking areas around the facility which are owned or randomly inspected daily by the organization, public roads along which parking is not allowed, heavily wooded or other undeveloped areas with restricted vehicular access, and any areas where U.S. security personnel have unannounced 24-hour access. (DoD 5105.21-M Vol 2)

**Open Storage:** Storage of classified information within an approved facility where securing classified information in GSA approved storage containers while the facility is not occupied by authorized personnel is not required. (DoD 5105.21-M Vol 2)

**Protected Distribution System (PDS):** Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information through an area of lesser classification or control. (CNSSAM TEMPEST/01-13)

**RED Equipment:** A term applied to equipment that processes unencrypted NSI that requires protection during electrical/electronic processing. (CNSSAM TEMPEST/1-13)

**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. (CNSSAM TEMPEST/1-13)

**Secure Working Area (SWA):** 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.

**Site Security Manager (SSM):** Person designated for the construction project that is responsible for all aspects of security 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 National Intelligence.

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

**Sound Transmission Class (STC):** An integer rating of how well a building partition attenuates airborne sound.

**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. (DoDM 5205.07, Volume 3)

**Special access program facility accrediting official (SAO):** A properly trained SAP facility accrediting official designated by the CA SAPCO to physically inspect and review and approve or disapprove physical security preconstruction plans for a SAPF, T-SAPF, SAPCA, and SAPWA or SAPSWA before accreditation. (DoDM 5205.07, Volume 3)

**Special Security Officer (SSO):** The SSO designated by the Senior Intelligence Official for any activity that is accredited for and authorized to receive, use, and store SCI. The activity SSO is responsible, IAW DoDM 5105.21, Volumes 1-3 and ICD 703 for the day-to-day security management, operations, implementation, use and dissemination of SCI within the activity. (DoDM 5200.01, Vol 1)

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

**TEMPEST:** A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. (CNSSI No. 4009)

**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. (DoD 5105.21-M Vol 2)

**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.

**Telecommunications Room (TR):** An architectural space designed to contain telecommunications equipment, cable terminations, and cross connect cabling. (UFC 3-580-01)

**Telecommunications System:** Any system that transmits an analog or digital signal over a physical (cable or wire) or non-physical (wireless) connection. This includes

systems such as information technology, control, cable television, electronic security, fire alarm, paging, intercom, public address, and mass notification.

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

**United States and its territories:** The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the United States Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands. (DoDM 5200.01, Volume 3)

**Uninterruptible Load:** Loads that require continuous power and cannot experience even momentary power disruptions. Loads in this category usually involve life safety or include hazardous or industrial process equipment, command, control, computer, data center, and communications systems. (UFC 3-540-01)

**U.S. Person:** An individual who has been lawfully admitted for permanent residence as defined in 8U.S.C. § 1101(a)(20) or who is a protected individual as defined by Title 8 U.S.C. §1324b (a)(3)). (IC Tech Spec – for ICD/ICS 705)

**Vault:** A room(s) used for the storing, handling, discussing, and/or processing of SCI and constructed to afford maximum protection against unauthorized entry. (IC Tech Spec – for ICD/ICS 705)

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



## APPENDIX C REFERENCES

### C-1 GOVERNMENT.

#### COMMITTEE ON NATIONAL SECURITY SYSTEMS

<https://www.cnss.gov/cnss/>

Committee on National Security Systems Advisory Memorandum (CNSSAM)  
TEMPEST/01-13, *RED/BLACK Installation Guidance* (For Official Use Only)

Committee on National Security Systems Instruction (CNSSI) No.4009, *Committee on National Security Systems (CNSS) Glossary*

Committee on National Security Systems Instruction (CNSSI) No.7003, *Protective Distribution Systems (PDS)*

#### DEPARTMENT OF DEFENSE

<https://www.esd.whs.mil/dd/dod-issuances/>

##### Manuals:

DoDM 5105.21-Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*

DoDM 5105.21-Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*

DoDM 5105.21-Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*

DoDM 5200.01 Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*

DoDM 5200.01 Volume 2, *DoD Information Security Program: Marking of Information*

DoDM 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*

DoDM 5205.07 Volume 1, *DoD Special Access Program (SAP) Security Manual: General Procedures*

DoDM 5205.07 Volume 2, *DoD Special Access Program (SAP) Security Manual: Personnel Security*

DoDM 5205.07 Volume 3, *DoD Special Access Program (SAP) Security Manual: Physical Security*

DoDM 5205.07 Volume 4, *DoD Special Access Program (SAP) Security Manual: Marking*

**Directives:**

DoD 5200.08-R (DTM) 08-004, *Physical Security Program*

DoDD 4270.5, *Military Construction*

**Instructions:**

DoDI 5200.48, *Controlled Unclassified Information (CUI)*

**DEPARTMENT OF THE NAVY**

DONSAPCO/0779-22, *Department of Navy Special Access Program Facilities Way Ahead*

**DEPARTMENT OF STATE**

*Best Practices Guidelines for Architectural Radio Frequency Shielding (FOUO)*

**DIRECTOR OF NATIONAL INTELLIGENCE**

<https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-ci-security-governance-regulations>

Office of the Director of National Intelligence Instruction 80.16, *Category 80 - Information and Records Management*

Intelligence Community Directive (ICD) 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*

Intelligence Community Directive (ICD) 705, *Sensitive Compartment Information Facilities*

Intelligence Community Standard Number 705-1 (ICS 705-1), *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*

Intelligence Community Standard Number 705-02, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities*

Intelligence Community Standard Number 706-02, *Protecting Mission Critical-Facility Related Control Systems (MC-FRCS) in Mission Critical Facilities (MCF)*

IC Tech Spec-for ICD/ICS 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*

## **FEDERAL SPECIFICATIONS**

<https://quicksearch.dla.mil/qsSearch.aspx>

AA-D-600D, *Federal Specification Door, Vault, Security*

FF-L-2740, *Locks, Combination*

FF-L-2890, *Lock Extension (Pedestrian Door, Deadbolt)*

FF-P-110, *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)*

## **NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY**

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*

Federal Information Processing Standard (FIPS) 197, *Advanced Encryption Standard (AES)*

## **NAVAL FACILITIES ENGINEERING COMMAND**

NAVFAC INSTRUCTION 4700.01, *Planning, Design, and Construction of Navy Sensitive Compartmented Information Facilities*

## **UNIFIED FACILITIES CRITERIA**

<https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc>

UFC 1-200-01, *DoD Building Code*

UFC 1-200-02, *High Performance and Sustainable Building Requirements*

UFC 3-410-01, *Heating, Ventilating, and Air Conditioning Systems*

UFC 3-540-01, *Engine-Driven Generator Systems for Prime and Standby Power Applications*

UFC 3-580-01, *Telecommunications Interior Infrastructure Planning and Design*

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*

UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*

UFC 4-020-01, *DoD Security Engineering: Facilities Planning Manual*

UFC 4-020-02FA, *Security Engineering: Concept Design (FOUO)*

UFC 4-021-02, *Electronic Security Systems*

## **UNIFIED FACILITIES GUIDE SPECIFICATIONS**

<https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs>

UFGS 08 34 73, *Sound Control Door Assemblies*

## **UNITED STATES ACCESS BOARD**

<https://www.access-board.gov/aba/>

*Architectural Barriers Act (ABA) Standards*

## **C-2 NON-GOVERNMENT.**

### **THE AMERICAN INSTITUTE OF ARCHITECTS**

*Architectural Graphics Standards*

### **ASTM INTERNATIONAL (ASTM)**

ASTM C1766, *Factory-Laminated Gypsum Board*

ASTM D1003, *Standard Test Method for Haze and Luminous Transmittance of Transparent Plastics*

ASTM E336, *Standard Test Method for Measurement of Airborne Sound Attenuation between Rooms in Buildings*

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

### **GYPSUM ASSOCIATION**

GA-600, *Fire Resistance and Sound Control Design Manual*

### **INTERNATIONAL CODE COUNCIL**

<https://www.iccsafe.org/>

*International Building Code (IBC)*

### **NATIONAL FIRE PROTECTION ASSOCIATION**

<http://www.nfpa.org>

NPFA 70, *National Electric Code*

NFPA 101, *Life Safety Code*

NFPA 110, *Standard for Emergency and Standby Power Systems*

**UNDERWRITER'S LABORATORIES, INC. (UL)**

<https://www.ul.com/>

UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*

UL 639, *Standard for Intrusion-Detection Units*

UL 681, *Installation and Classification of Burglar and Holdup Alarm Systems for Alarm System Installation*

UL 864, *Standard for Control Units and Accessories for Fire Alarm Systems*

UL 1034, *Standard for Safety for Burglary-Resistant Electric Locking Mechanisms*

UL 1076, *Standard for Safety Proprietary Burglar Alarm Units and Systems*

UL 1610, *Standard for Safety Central-Station Burglar-Alarm Units*

UL 2050, *National Industrial Security Systems*; UL 2050 materials are restricted and only distributed to those demonstrating relevant national industrial security involvement