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

UNIFIED FACILITIES CRITERIA (UFC)

SENSITIVE COMPARTMENTED INFORMATION FACILITIES PLANNING, DESIGN, AND CONSTRUCTION

\

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

UNIFIED FACILITIES CRITERIA (UFC)

SENSITIVE COMPARTMENTED INFORMATION FACILITIES 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.

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

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

Change No.	**Date**	**Location**
1	1 Oct 2013	Added paragraphs 3-5.6.4, 3-5.6.1 and 3-5.14 Added Figure 3-3 Modified paragraphs 1-4, 1-12, 1-13, 3-5.4.5, 3-5.6, 3-5.6.4, 3-5.6.5.1, 3-5.6.10, 3-5.7, 3-5.7.1, 3-5.8.1, 3-5.8.2, 3-5.8.3, 3-5.9, 3-5.9.1, 3-5.10, 3-5.12.1, 3-5.12.3, 3-5.12.3.2 3-5.12.3.3, and 3-5.13 Modified Figure 3-10 Modified References

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 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 Services' responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC) are responsible for administration of the UFC system. Defense agencies should contact the preparing service for document interpretation and improvements. Technical content of UFC is the responsibility of the cognizant DoD working group. Recommended changes with supporting rationale should be sent to the respective service proponent office by the following electronic form: Criteria Change Request. The form is also accessible from the Internet sites listed below.

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

- Whole Building Design Guide web site http://dod.wbdg.org/.

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

AUTHORIZED BY:

JAMES C. DALTON, P.E. Chief, Engineering and Construction U.S. Army Corps of Engineers	JOSEPH E. GOTT, P.E. Chief Engineer Naval Facilities Engineering Command
SCOTT HARTFORD, Colonel, USAF, P.E. Acting Director Facilities Engineering Center of Excellence AF Civil Engineer Center	MICHAEL McANDREW Director, Facilities Investment and Management Office of the Deputy Under Secretary of Defense (Installations and Environment)

UNIFIED FACILITIES CRITERIA (UFC)
REVISION DOCUMENT SUMMARY SHEET

Document: UFC 4-010-05, *Sensitive Compartmented Information Facilities Planning, Design, and Construction, with Change 1*

Superseding: UFC 4-010-05, *Sensitive Compartmented Information Facilities Planning, Design, and Construction*

Description: This change includes updates due to DoDM 5105.21, IC Tech Spec-for ICD/ICS 705 and added clarification on TEMPEST mitigation.

Reasons for Document:

Director of National intelligence issued policy for the planning, design, and construction of SCIF. There was no UFC document that prescribed facility criteria for SCIF. This UFC provides unified criteria for the planning, design, and construction of Sensitive Compartmented Information Facilities (SCIF).

- This document is one of a series of security engineering criteria documents covering physical countermeasures for the current threat environment.
- The design of physical security measures is a specialized technical area that does not fall in the normal skill record and resume of commanders, architects, engineers, and project managers. This document provides guidance to those parties tasked with implementing existing and emerging physical protection system requirements for SCIF.
- This document provides a unified approach for physical security measures for SCIF.

Impact:

- Implementation of Director of National Intelligence (DNI) policy for SCIF may have significant cost impacts for SCIF constructed overseas. This is primarily due to the security requirements for personnel and companies designing and constructing SCIF outside the United States and the access control measures that may have to be implemented during construction.

Unification Issues

There are no unification issues

.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION 1
1-1 BACKGROUND. 1
1-2 PURPOSE. 1
1-3 APPLICABILITY. 1
1-4 REFERENCES. 1
1-5 GLOSSARY. 1
1-6 POLICY. 1
1-7 IMPLEMENTATION. 2
1-8 GENERAL BUILDING REQUIREMENTS. 2
1-9 RISK MANAGEMENT. 2
1-9.1 Security in Depth (SID). 3
1-10 SCIF CLASSIFICATIONS. 4
1-10.1 Secure Working Area (SWA). 4
1-10.2 Temporary Secure Working Area (TSWA). 4
1-10.3 Temporary SCIF. 4
1-10.4 Closed Storage. 4
1-10.5 Open Storage. 4
1-10.6 Continuous Operation. 4
1-11 SCIF SECURITY REQUIREMENTS. 4
1-12 CONSTRUCTION SECURITY PLAN (CSP). 4
1-13 INFORMATION SECURITY. 5
1-14 SCIF DESIGN SECURITY. 5
1-15 SCIF CONSTRUCTION SECURITY. 5
1-15.1 SCIF Within the United States. 6
1-15.2 SCIF Outside the United States. 6
1-16 SCIF ACCREDITATION. 6
1-16.1 Accreditation Process. 6
1-16.2 Fixed Facility Checklist (FFC). 7
1-16.3 TEMPEST Review. 7
1-17 HISTORIC PRESERVATION COMPLIANCE. 7
1-17.1 Security and Stewardship. 7

1-17.2 Compliance with Laws. 7
1-17.3 Compliance with DoD Standards. 8
1-18 SECURITY ENGINEERING UFC SERIES. 8
1-18.1 DoD Minimum Antiterrorism Standards for Buildings. 8
1-18.2 DoD Security Engineering Facilities Planning Manual. 8
1-18.3 DoD Security Engineering Facilities Design Manual. 9
1-18.4 Security Engineering Support Manuals. 9
1-18.5 Security Engineering UFC Application. 9
CHAPTER 2 PLANNING 11
2-1 ESTABLISH PLANNING REQUIREMENTS. 11
2-1.1 Minimum and Enhanced Security. 11
2-1.2 Planning Team. 11
2-2 PLANNING DOCUMENTATION. 12
2-2.1 Configuration of SCIF Spaces. 12
2-2.2 SCIF and Historic Preservation. 12
2-2.3 Construction Security. 12
2-2.4 Project Documentation. 12
CHAPTER 3 DESIGN 15
3-1 VALIDATE PLANNING REQUIREMENTS. 15
3-2 MINIMUM AND ENHANCED SECURITY. 15
3-3 DESIGN APPROVAL. 15
3-4 GENERAL DESIGN STRATEGY. 15
3-4.1 Configuration of SCIF Spaces. 16
3-4.2 SCIF Perimeter. 16
3-4.3 Intrusion Detection System. 16
3-4.4 Sound Attenuation. 17
3-4.5 Electronic Emanations - TEMPEST. 17
3-5 SPECIFIC DESIGN STRATEGY. 17
3-5.1 Adjacent Space. 18
3-5.2 Vestibule. 18
3-5.3 Perimeter Construction. 18
3-5.4 Perimeter/Compartmented Areas Walls. 18

3-5.5 Ceiling and Floors. 21
3-5.6 Perimeter Doors. 21
3-5.7 Windows. 24
3-5.8 Perimeter Penetrations. 25
3-5.9 Vents, Ducts, and Pipes. 26
3-5.10 Access Port. 27
3-5.11 Flashing or Rotating Light. 27
3-5.12 Duress Alarm. 27
3-5.13 Electronic Security System (ESS). 29
3-5.14 Telecommunication Cabling System. 32
3-5.15 TEMPEST Countermeasures. 32
CHAPTER 4 CONSTRUCTION 35
4-1 DESIGN APPROVAL. 37
4-2 CONSTRUCTION SECURITY. 37
4-3 ACCREDITATION PROCESS. 37
4-4 INSPECTIONS. 37
4-5 PHOTOGRAPHIC CONSTRUCTION SURVEILLANCE RECORD. 39
APPENDIX A REFERENCES 41
APPENDIX B GLOSSARY 45
APPENDIX C MINIMUM CONSTRUCTION 49

FIGURES

Figure 1-1 Security-in-Depth 3
Figure 1-2 SCIF Drawings 5
Figure 1-3 Security Engineering UFC Application 10
Figure 3-1 Six Sided Approach 16
Figure 3-2 Wall Finish 19
Figure 3-3 Furred Out Wall for Utilities 21
Figure 3-4 Tamper Resistant Hinges 23
Figure 3-5 Emergency Exit Doors 24
Figure 3-6 Duct Penetrations 26
Figure 3-7 Sealing Penetrations 28
Figure 3-8 Bars on Penetration 28
Figure 3-9 Access Port 28
Figure 3-10 Notional IDS Layout 30

TABLES

Table C-1 Minimum SCIF Wall Construction and Alarm 49

This Page Intentionally Left Blank

CHAPTER 1 INTRODUCTION

1-1 BACKGROUND.

Sensitive Compartmented Information (SCI) is classified Confidential, Secret or Top Secret information that is derived from intelligence sources, methods or analytical processes which is required to be handled within formal control systems established by the Director of National Intelligence. Sensitive Compartmented Information (SCI) can only be handled, processed, discussed, or stored in an accredited Sensitive Compartmented Information Facilities (SCIF).

Sensitive Compartmented Information Facilities (SCIF) are accredited areas, room(s) or building(s) where Sensitive Compartmented Information (SCI), is stored, used, processed or discussed. SCIF are only required for SCI and not necessarily required for Secret or Top Secret information. When required, SCIF provide an operational capability that is critical to the supported command's mission.

1-2 PURPOSE.

Intelligence Community Directive (ICD) 705 established that all Intelligence Community (IC) SCIF comply with uniform IC physical and technical security requirements. Intelligence Community Standard (ICS) 705-1 and the IC Tech Spec-for ICD/ICS 705 provide the physical and technical security standards for all SCIF including existing and new construction, and renovation projects. This UFC is intended to make planning, design and construction communities aware of the published policy and ensure timely and appropriate implementation.

1-3 APPLICABILITY.

This document provides planning and design criteria for DoD components and participating organizations. This document applies to all construction, renovation, and repair projects for SCIF.

1-4 REFERENCES.

Appendix A contains a list of references used in this document. The publication date of the code or standard is not included in this document. \1\ The most recent edition of referenced publications applies, unless otherwise specified. /1/

1-5 GLOSSARY.

Appendix B contains acronyms, abbreviations, and terms.

1-6 POLICY.

Director of Central Intelligence Directive (DCID) No. 6/9 was rescinded by the issuance of ICD 705 by the Director of National Intelligence. ICD 705 replaces DCID No. 6/9 and all its annexes as the policy for SCIF. ICS 705-1 was issued by the Director of National

Intelligence (DNI) on 17 September 2010. ICS 705-1 and the IC Tech Spec-for ICD/ICS 705 provide the standards for the physical and technical security standards that apply to a SCIF, including existing, new construction, and renovation of SCIF. Refer to ICD 705, ICS 705-1, and IC Tech Spec-for ICD/ICS 705 for more information.

DoDM 5200.01 is the primary document associated with SCIF administration. The manual is composed of several volumes, each having its own purpose. It assigns responsibilities and prescribes procedures for the implementation of Director of Central Intelligence and Director of National Intelligence (DNI) policies for SCI.

1-7 IMPLEMENTATION.

Intelligence Community (IC) elements shall fully implement ICS 705-1 and IC Tech Spec-for ICD/ICS 705 within 180 days of signing. ICS 705-1 was signed on 17 Sep 2010 and IC Tech Spec-for ICD/ICS 705 was signed on 5 May 2011. Facilities under construction or renovation as of the effective date of ICS 705-1 shall be required to meet these standards or request a waiver to the standards. The Accrediting Official (AO) is responsible to request waiver approval.

Each SCIF must be planned, programmed, designed, and constructed on a project by project basis. Work closely with the supported command, designated Site Security Manager (SSM), and the Certified TEMPEST Technical Authority (CTTA) to determine the requirements for each SCIF.

1-8 GENERAL BUILDING REQUIREMENTS.

UFC 1-200-01, "General Building Requirements", provides applicability of model building codes and government-unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, sustainability, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

1-9 RISK MANAGEMENT.

Per ICS 705-1, the AO must ensure the application of analytical risk management in the SCIF planning, design and construction. Analytical risk management is the process of assessing threats against vulnerabilities and implementing security enhancements to protect assets at an acceptable level of risk, and within acceptable cost.

The CTTA will use a risk based approach outlined in CNSSI No. 7000 to determine applicable countermeasures for each SCIF. Supported command will provide the CTTA with a completed DNI TEMPEST Checklist for review. The TEMPEST Checklist is included in the IC Tech Spec-for ICD/ICS 705. Project Managers may need to provide site plans and building floor plans to assist CTTA in the determination of TEMPEST countermeasures.

1-9.1 Department of State (DoS) Security Environment Threat List (SETL).

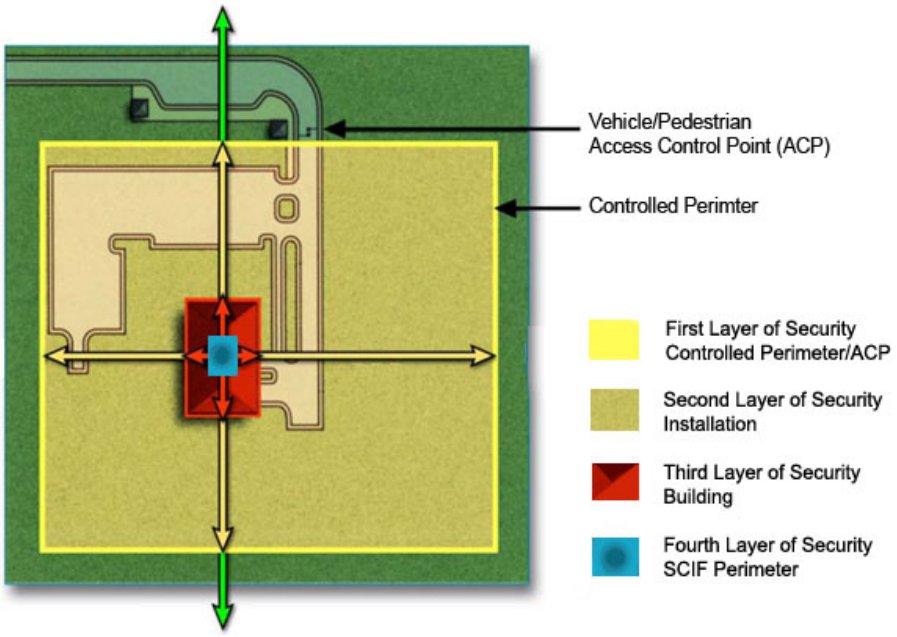
The SETL and its contents are classified information. The SETL reflects four categories of security threats for overseas locations. The AO will utilize the SETL category to determine security requirements for locations outside the United States.

1-9.2 Security in Depth (SID).

SID is desired for all SCIF and required for all SCIF located outside the United States. 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. The AO will assess the layers of security measures in place to determine if any security enhancements are required. The primary means to achieve SID include:

- Located on a Military installation or compound with a dedicated response force of U.S. citizens or U.S. persons.
- Located within a building or fenced compound that employs access control.
- Office areas adjacent to or surrounding the SCIF are controlled and are protected by alarm.

Figure 1-1 Security-in-Depth



1-10 SCIF CLASSIFICATIONS.

SCIF are classified based on operational requirements. Per ICS 705-1, there are six SCIF classifications.

1-10.1 Secure Working Area (SWA).

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

1-10.2 Temporary Secure Working Area (TSWA).

Secure working area is SCIF that is used less than 40 hours per month.

1-10.3 Temporary SCIF.

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

1-10.4 Closed Storage.

SCIF where SCI material is stored in GSA approved storage containers when not in use. This includes documents, computer hard drives, and storage media.

1-10.5 Open Storage.

SCIF in which SCI may be openly stored or processed.

1-10.6 Continuous Operation.

SCIF which is staffed and operated 24/7

1-11 SCIF SECURITY REQUIREMENTS.

ICS 705-1 and IC Tech Spec-for ICD/ICS 705 provide the minimum and enhanced security requirements. The minimum security requirements for a SCIF are based on classification and location. To implement security enhancements above the minimum, the AO must evaluate the threat, SID and balance the enhancements with risk at acceptable cost.

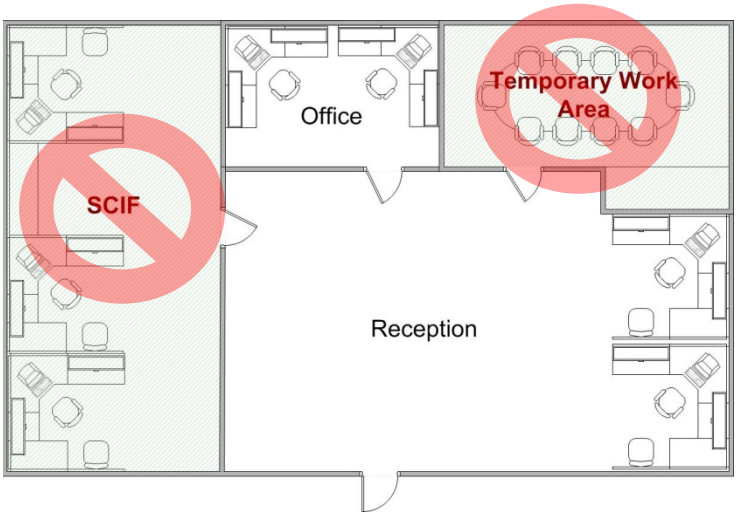
1-12 CONSTRUCTION SECURITY PLAN (CSP).

Per ICS 705-1, a Construction Security Plan (CSP) shall be developed by the SSM and approved by the AO to address the application of security to the SCIF planning, design, and construction. \1\ /1/

1-13 INFORMATION SECURITY.

Per ICS 705-1, construction plans and all related documents shall be handled and protected in accordance with the CSP. If classification guides dictate, plans and related documents may require classification. DoDM 5105.21 Vol 2 states the facility's location (complete address) and identity as a SCIF shall be protected at a minimum of FOR OFFICIAL USE ONLY (FOUO). Drawings or diagrams identified as a SCIF may not be posted on an UNCLASSIFIED website or transmitted over the Internet without some type of encryption. Therefore, do not identify SCIF locations on planning or construction documents; see Figure 1-2. With SSM's approval, areas may be identified as "Secure Area" or "Controlled Area". Under no circumstances shall plans or diagrams that are identified for SCI be sent or posted on unprotected information technology systems or Internet venue without encryption. Refer to DoDM 5200.01 \1\ /1/ and the Service's related policy documents for guidance on the handling of classified information.

Figure 1-2 SCIF Drawings



1-14 SCIF DESIGN SECURITY.

Per ICS 705-1, design of SCIF shall be performed by U.S. companies using U.S. citizens or U.S. persons. AO shall ensure mitigations are implemented when using non-U.S. citizens and these mitigations shall be documented in the CSP.

U.S. Person is defined as an individual who has been lawfully admitted for permanent residence as defined in 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by Title 8 U.S.C. 1324b (a)(3), and able to provide two forms of identification listed on Department of Homeland Security Form I-9, Employment Eligibility Verification.

1-15 SCIF CONSTRUCTION SECURITY.

Per ICS 705-1, construction security requirements are documented in the CSP. Depending on the location of the SCIF, the AO may impose procedures for the

procurement, shipping, and storing of construction materials at the site. These procedures must be documented in the CSP.

1-15.1 SCIF Within the United States.

General construction of SCIF shall be performed by U.S. companies using U.S. citizens or U.S. persons. The AO shall ensure mitigations are implemented when using non-U.S. citizens. These mitigations shall be documented in the CSP.

Intrusion Detection System (IDS) installation and testing shall be performed by U.S. companies using U.S. citizens.

1-15.2 SCIF Outside the United States.

General SCIF construction shall 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 of SCIF. In this situation, the SSM shall prescribe, with AO approval, mitigating strategies. These mitigations shall be documented in the CSP.
- U.S. Top Secret-cleared personnel shall perform finish work in Category I and II countries. U.S. Secret-cleared personnel shall perform finish work in Category III countries. Finish work includes closing up wall structures; installing, floating, taping and sealing wallboards; installing trim, chair rail, molding, and floorboards; painting, etc.
- Intrusion Detection System (IDS) installation and testing shall be performed by personnel who are U.S. TOP SECRET-cleared or U.S. SECRET-cleared and escorted by SCIF personnel.

1-16 SCIF ACCREDITATION.

A letter of accreditation is a formal statement on behalf of the IC element head that a facility has been designed, constructed, inspected, and certified for the protection of all Sensitive Compartmented Information (SCI) compartments, programs or special activities in accordance with the provisions of ICD 705. Refer to ISC 705-2 for the policy on SCIF accreditation.

1-16.1 Accreditation Process.

SCIF inspections and evaluations shall be performed by the AO, or designee, prior to initial accreditation. The accreditation process shall include a review of documents relating to SCIF design, construction, and operations. The SSM shall be responsible for assembling and submitting documents for AO approval. Documents shall include, but not be limited to:

- Fixed Facility Checklist
- Standard Operating Procedures
- Emergency Plans
- Construction Security Plan
- TEMPEST countermeasures evaluation from CTTA
- Waiver request packages and supporting documentation, if applicable.

1-16.2 Fixed Facility Checklist (FFC).

The FFC is a standardized document used in the process of accrediting a SCIF. It documents physical, technical, and procedural security information for obtaining an initial or subsequent accreditation.

To support the accreditation process, Designers of Record, Project Managers, and Construction mangers shall provide the AO/SSM site plans, building floorplans, IDS plans, and information related to perimeter and compartment area wall construction, doors, locks, deadbolts, IDS, telecommunication systems, acoustical protection, and TEMPEST countermeasure. See chapter 4 for additional information.

1-16.3 TEMPEST Review.

A TEMPEST review and evaluation shall be included in the accreditation documentation. TEMPEST review and verification of countermeasures by the appropriate Certified Technical TEMPEST Authority (CTTA) is a part of the accreditation process.

1-17 HISTORIC PRESERVATION COMPLIANCE.

1-17.1 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.

1-17.2 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 and the Archaeological Resources Protection Act. Installation personnel need to determine possible adverse effects upon an historic structure and/or archaeological resource 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.

1-17.3 Compliance with DoD Standards.

Conversely, historic preservation compliance does not negate the requirement to implement 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 not allow for prolonged consultations that conflict with the eminent need to implement security requirements. Preservation issues need to be quickly and effectively resolved.

1-18 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:

1-18.1 DoD Minimum Antiterrorism Standards for Buildings.

This UFC 4-010-01 and 4-010-02 establish standards that provide minimum levels of protection against terrorist attacks for the occupants of all DoD inhabited buildings. These UFCs are 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. They also include recommendations that should be, but are not required to be incorporated into all such buildings.

1-18.2 DoD 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.

1-18.3 DoD Security Engineering Facilities Design Manual.

UFC 4-020-02 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 4-020-02 is in sufficient detail to support concept level project development, and as such can provide a good basis for a more detailed design. The manual also provides a process for assessing the impact of protective measures on risk. The primary audience for the Security Engineering Design Manual is the design team, but it can also be used by security and antiterrorism personnel.

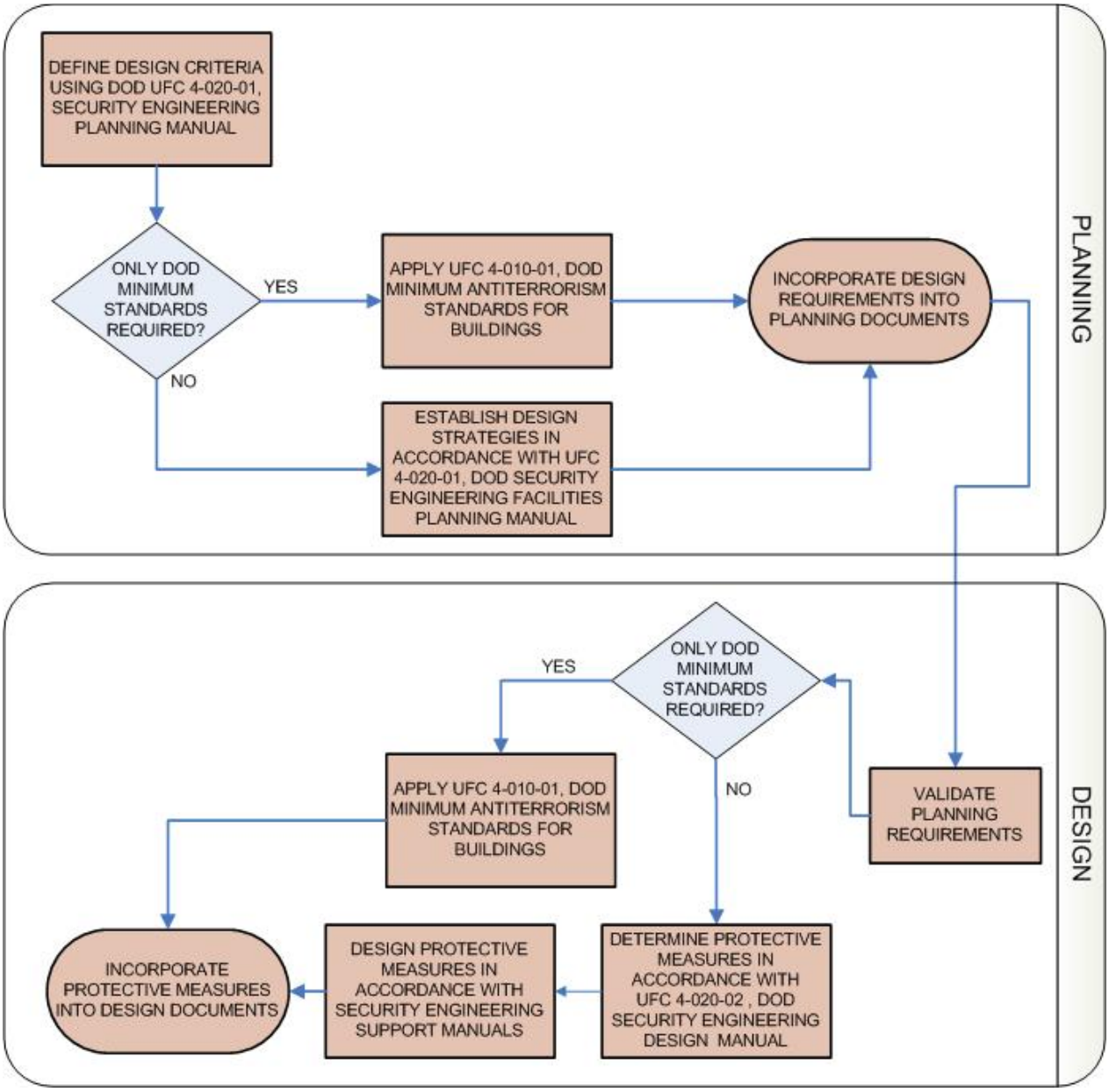
1-18.4 Security Engineering Support Manuals.

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 4-020-02. 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.

1-18.5 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. Even if only the minimum standards are required other UFCs may need to be applied if sufficient standoff distances are unavailable. Applying this series of UFCs in the manner illustrated in Figure 1-3 will result in the most efficient use of resources for protecting assets against security and antiterrorism related threats.

Figure 1-3 Security Engineering UFC Application



CHAPTER 2 PLANNING

2-1 ESTABLISH PLANNING REQUIREMENTS.

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

SCIF are established only when there are clear operational requirements which are critical to the supported command's mission. All SCIF projects begin with an Accrediting Official's Sponsorship. If a supported command requests a SCIF be included in a project, that SCIF has an Accrediting Official and a Site Security Manager (SSM).

2-1.1 Minimum and Enhanced Security.

ICS 705-1 and IC Tech Spec-for ICD/ICS 705 provide the minimum and enhanced security requirements for SCIF including construction details. The minimum security requirements are based on classification and location. Table C-1 in Appendix C provides an overview of the minimum SCIF construction requirements. To implement security enhancements above the minimum, the AO and CTTA will evaluate the threat, TEMPEST, SID and balance the security enhancements with cost at acceptable risk.

2-1.2 Planning Team.

Establish an interdisciplinary planning team with local considerations. The interdisciplinary planning team must work together to determine classification of SCIF 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
- Site Security Manager (SSM)
- Certified TEMPEST Technical Authority (CTTA)
- Communications
- Security
- Engineering
- Cultural resources (if historical building)

2-2 PLANNING DOCUMENTATION.

The SCIF classification, operation, TEMPEST countermeasures, and resulting facility related requirements must be determined, documented, and budgeted during the planning process.

2-2.1 Configuration of SCIF Spaces.

When a facility has more than one SCIF, serious consideration should be given to consolidate SCIF with Compartmented Areas within. Any consolidation of spaces will reduce initial and sustainment costs for infrastructure and electronic security systems and the associated accrediting requirements. This must be coordinated with the supported commands to insure the configuration will meet their operational (compartmented) requirements.

2-2.2 SCIF and Historic Preservation.

Preservation of Cultural Resources must be considered when converting a historical building into a SCIF or locating a SCIF within a historic building. In a SCIF, 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 shall be protected against forced entry and meet the standard for the SCIF 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 may allow the modification if the impact is minimized and the effect mitigated. Planners will 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.

2-2.3 Construction Security.

For locations outside the United States, 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 SCIF construction area. Since these additional security measures may have significant cost impacts on project, they must be determined during project development.

2-2.4 Project Documentation.

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

- Is the SCIF the entire facility or an area within the facility?
- Will there be more than one SCIF, if so how many?

- What is the classification of the SCIF?
- Will the SCIF perimeter wall be standard, enhanced, or vault construction?
- What is the required Sound Transmission Class (STC) rating for the SCIF perimeter?
- Will the SCIF have Compartmented Areas? If so, how many and what is the required STC rating for the Compartmented Areas?
- Will an Electronic Security System (ESS) be required?
- Is there equipment that will be processing National Security Information (NSI)?
- Has the supported command provided the CTTA with a completed TEMPEST Checklist for review? The TEMPEST Checklist is included in the IC Tech Spec-for ICD/ICS 705.
- Will there be a TEMPEST requirement? If so, what will be required TEMPEST countermeasures?
- Are there special procurement, shipping, and storing of SCIF construction materials at the site required? If so, what will be required?
- Are there access control requirements for the construction materials and the SCIF construction area?
- Will U.S. companies using U.S. citizens be required for construction and oversight?
- 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 U.S. SECRET-cleared personnel escorted by SCIF personnel.

Some of these requirements are documented in the approved CSP. Therefore, it is very important to obtain the approved CSP during project development to ensure appropriate security requirements are included in the project budget and scope.

This Page Intentionally Left Blank

CHAPTER 3 DESIGN

3-1 VALIDATE PLANNING REQUIREMENTS.

Work with the Supported Command, SSM, and the CTTA to validate planning requirements. Operation, classification, and threat classification of the SCIF may have changed since the project was planned. Validate and document the classification, operation, and resulting facility requirements for the SCIF. Include requirements in the Design Build RFP, design documents, and construction contracts to insure the SCIF can be accredited to meet the supported command's operational capabilities.

3-2 MINIMUM AND ENHANCED SECURITY.

ICS 705-1 and IC Tech Spec-for ICD/ICS 705 provide the minimum and enhanced security requirements for SCIF. The minimum security requirements are based on classification and location. Table C-1 in Appendix C provides an overview of the minimum SCIF construction requirements. To implement security enhancements above the minimum, the SSM and CTTA will evaluate the threat, SID and balance the security enhancements with cost at an acceptable risk.

3-3 DESIGN APPROVAL.

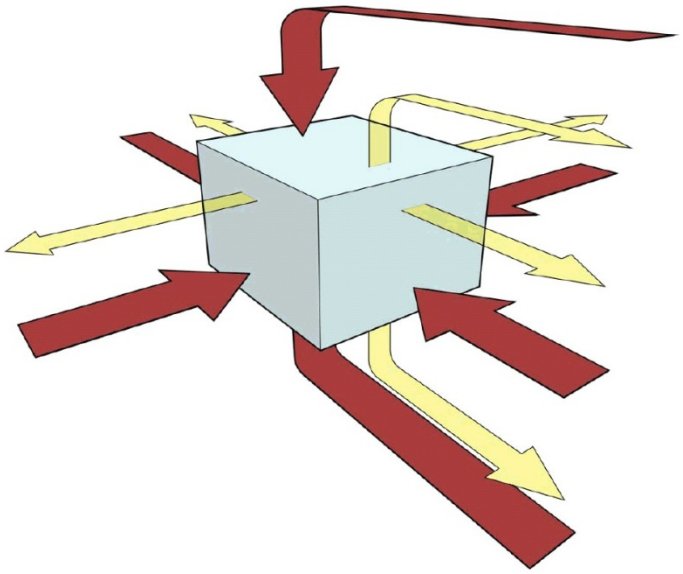
Per ICS 705-1, Concept and final design for each construction project must be reviewed and approved by the Accrediting Official prior to start of construction.

3-4 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.

SCIF design will vary depending on type of SCIF, location, SID, SCI discussion, and NSI processing requirements. Mitigation against forced entry, covert entry, visual surveillance, acoustic eavesdropping, and electronic emanations will dictate security requirements. Designers must take a six-sided approach when implementing SCIF requirements, see Figure 3-1. The floor, ceiling, walls and any penetrations must be designed to meet the performance requirements for the SCIF perimeter.

Figure 3-1 Six Sided Approach



3-4.1 Configuration of SCIF Spaces.

If a facility has more than one SCIF, serious consideration should be given to the consolidation SCIF spaces with Compartmented Areas within. Any consolidation of spaces will reduce accrediting requirements and the initial/sustainment costs for infrastructure and electronic security systems. This must be coordinated to insure configuration will meet operational (compartmented) requirements.

3-4.2 SCIF Perimeter.

The perimeter of the SCIF includes perimeter walls, windows, doors, ceiling, floor, and all penetrations. At a minimum, SCIF Perimeter shall provide:

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

This includes above the false ceilings and below raised floors.

3-4.3 Intrusion Detection System.

All Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, shall be protected by IDS, unless continuously occupied.

3-4.4 Sound Attenuation.

The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC). Architectural Graphics Standards (AGS) established Sound Groups I through 4, of which Groups 3 and 4 are considered adequate for specific acoustical security requirements for SCIF construction. Per AGS:

- Sound Group 3 – (STC of 45) or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.
- Sound Group 4 – (STC of 50) or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume, can be heard only faintly or not at all.

SCIF and compartmented area perimeters shall meet Sound Group 3, unless additional protection is required for amplified sound. 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 shall meet Sound Group 4 performance criteria.

3-4.5 Electronic Emanations - TEMPEST.

National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 7000, “TEMPEST Countermeasures for Facilities,” establish guidelines and procedures that shall be used by departments and agencies to determine the applicable TEMPEST countermeasures for national security systems. In general, TEMPEST countermeasures apply when the SCIF contains equipment that will be processing national security information (NSI). However, having equipment that will be processing NSI does not necessarily imply the need to implement TEMPEST countermeasures.

The Certified TEMPEST Technical Authority (CTTA) has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures. Failure to consult the CTTA could result in installation of unnecessary and/or expensive countermeasures or the omission of needed countermeasures. If required TEMPEST countermeasures are omitted, the facility will not be accredited and the Supported Command will not be mission capable.

3-5 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.

3-5.1 Adjacent Space.

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

3-5.2 Vestibule.

When practical, the entrance into a SCIF should incorporate a vestibule to preclude visual observation and enhance acoustic protection.

3-5.3 Perimeter Construction.

The SCIF and compartmented area perimeters and the penetrations in those perimeters are the primary focus of SCIF design. IC Tech Spec-for ICD/ICS 705 provides the minimum and enhanced construction requirements for SCIF perimeter and compartmented area 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 shall be provided as determined by the CTTA.

IC Tech Spec-for ICD/ICS 705 includes recommended 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 wall detail for Wall C - enhanced construction utilizing plywood. To meet UFC 1-200-01, the plywood must be Fire Retardant Treated (FRT) plywood.

3-5.4 Perimeter/Compartmented Areas Walls.

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

3-5.4.1 Wall Finish.

Walls must be uniformly finished on both sides from floor slab (true floor) to underside of floor or roof deck (true ceiling). See Figure 3-2.

Figure 3-2 Wall Finish

UNACCEPTABLE

- Wall not uniformly finished above false ceiling.
- Wall not sealed where wall abuts floor pan.
- Wall penetrations unsealed.

ACCEPTABLE

- Wall is uniformly finished above false ceiling
- Wall is sealed where wall abuts floor pan.
- Wall penetrations are sealed.

3-5.4.2 Sound Attenuation.

Provide acoustical protection to protect SCI against being inadvertently overheard by the casual passerby, not to protect against deliberate interception of audio.

3-5.4.3 Minimum Sound Attenuation.

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

- SCIF Perimeter shall meet Sound Group 3, unless additional protection is required for amplified sound. 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.
- Compartmented Area: If compartmented areas are required within the SCIF, the dividing office walls must meet Sound Group 3, unless additional protection is required for amplified sound.
- Conference rooms or other areas where amplified audio is used such as video teleconference (VTC) equipment, audio visual systems, and speakerphones shall meet Sound Group 4 performance criteria.

3-5.4.4 Sound Masking.

When normal construction and baffling measures have been determined to be inadequate to meet the sound attenuation requirement, sound masking shall be employed. A sound masking system may utilize a noise generator as a noise source with speakers or transducers located on the perimeter of the SCIF. When required, provide sound masking devices at penetrations to the SCIF perimeter such as doors and duct penetrations.

3-5.4.5 Utilities on Perimeter Wall.

Utilities such as power,\1\ telecommunications, /1/ signal, and plumbing on the interior of a perimeter/compartmented wall treated for acoustic or RF shall be surface mounted, contained in a raceway, or a furred out wall shall be constructed for routing of utilities. Utilities shall not be mounted in a manner that affects the acoustic or RF shielding performance. If a furred out wall is used, gypsum board may be 3/8 inch (10 mm) and shall terminate above the false ceiling. \1\ See Figure 3-3 for an example. /1/

3-5.4.6 Recessed Fire Extinguisher Cabinets.

Recessed fire extinguisher cabinets are prohibited on perimeter walls.

3-5.5 Ceiling and Floors.

Ceilings and floors shall 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 shall meet TEMPEST requirements when required by CTTA.

3-5.6 Perimeter Doors.

SCIF perimeter doors and frame assembles shall meet acoustic requirements (vestibule of two doors may be used) unless declared a non-discussion area. \1\ /1/ Provide dead bolts for perimeter doors with day access controls for SCIF residents. In addition, perimeter doors shall meet TEMPEST requirements when required by CTTA.

\1\

Figure 3-3 Furred Out Wall for Utilities

/1/

3-5.6.1 Acoustic Rated Doors.

Specify an acoustical assembly to include door, seals, hinges, frame, and threshold tested to ASTM-E336 to obtain a STC 45 or 50 rated door. Fill voids between frame and adjacent wall with sound deadening material. For STC 46 or higher rated door assemblies, fill voids between frame and adjacent wall with lightweight gypsum plaster, foam, or sealant. Seal both sides of the entire perimeter of the door assembly with acoustical caulk where it interfaces with wall.

3-5.6.2 Wood doors.

At a minimum, wood doors shall be 1 ¾ inch (45 mm) thick solid wood core (wood stave).

\1\

3-5.6.3 Steel Doors.

At a minimum, steel doors shall meet following specifications:

- 1 ¾ inch (45 mm) thick face steel equal to 18 gauge.
- Hinges reinforced to 7 gauge.
- Door closure reinforced to 12 gauge.
- Lock area predrilled and/or reinforced to 10 gauge.

3-5.6.4 Door Closers.

All perimeter SCIF doors shall be equipped with a heavy duty automatic non-hold door-closer installed internal to the SCIF.

/1/

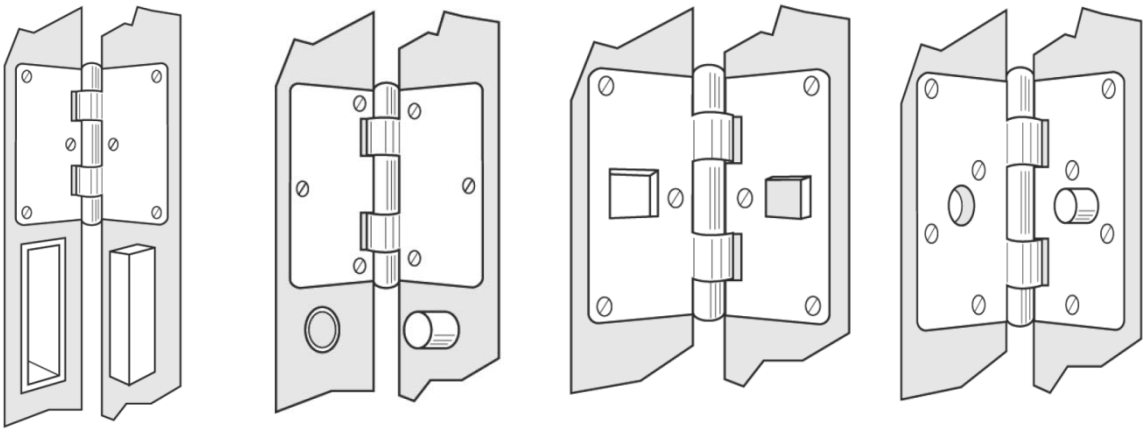
3-5.6.5 Hinges.

Hinges shall be full mortise, half mortise, full surface, or half surface design as recommended by the manufacturer for acoustical door assembly.

3-5.6.5.1 Hinge Pins.

Hinge pins on SCIF perimeter doors shall be tamper resistant unless mounted on the protected side of the door. Tamper resistant hinges shall have non-removable pins, security pins,\1\ set screws, welded, /1/ or equipped with a safety stud. \1\ See Figure 3-4. /1/

Figure 3-4 Tamper Resistant Hinges



3-5.6.6 Primary Entrance.

Unless approved by the AO, each SCIF shall have one primary SCIF entrance where visitor control is conducted. The primary entrance should incorporate a vestibule to preclude visual observation and enhance the acoustic protection. Primary entrance shall 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.

Federal Specification FF-L-2890 requires a combination lock that meets Federal Specification FF-L-2740. Therefore, only one locking device is provided on the door, that locking device shall meet Federal Specification FF-L- 2890.

3-5.6.7 Emergency Exit Doors.

Emergency exit doors shall meet perimeter door requirements and:

- Have no exterior hardware; see \1\ Figure 3-5. /1/
- Secured with deadlocking panic hardware.
- Alarmed 24/7 and equipped with a local annunciation.
- Delayed-egress is recommended with NFPA 101 compliance.

Figure 3-5 Emergency Exit Doors

3-5.6.8 Vault Doors.

All vaults shall be GSA-approved Class 5 vault door.

3-5.6.9 Roll-up Doors.

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

3-5.6.10 Double Doors.

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

- One side shall be secured top and bottom with deadbolts.
- Have an astragal strip attached to \1\ either /1/ door to prevent observation of the SCIF through the opening between the doors.
- Each door shall be alarmed (have a balanced magnetic switch).
- A GSA approved lock shall be installed on the moving door.

3-5.7 Windows.

SCIF perimeters should have no windows. Therefore, every effort should be made to minimize or eliminate windows, especially on the ground floor. If provided, \1\ windows shall be non-operable. /1/ Provide mitigation for visual surveillance, acoustic protection and meet TEMPEST requirements when required by CTTA. Large windows may require noise generator transducers to achieve acoustic protection. For visual surveillance protection, windows shall be made opaque or with SSM approval equipped with blinds, drapes or other coverings.

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 shall:

- Be fixed non-opening.
- Meet the standards of the SCIF perimeter.
- Be protected against forced entry.
- Be alarmed.

3-5.7.1 Windows greater than 18 feet (5.5 meters).

Windows located above 18 feet (5.5 meters) shall be fixed non-opening \1\ /1/

3-5.8 Perimeter Penetrations.

Penetrations of the perimeter shall be kept to a minimum. Ducts, conduits, pipes, or anything that penetrates the SCIF perimeter present a vulnerability that must be addressed. Ducts, conduits or pipes servicing areas other than SCIF shall not penetrate the SCIF Perimeter unless mitigation is provided. \1\ In addition, perimeter penetrations shall meet TEMPEST requirements when required by CTTA. /1/

3-5.8.1 Utility Penetrations.

Utilities (power and signal) should enter the SCIF at a single point. Seal all utility penetrations to mitigate acoustic emanations and covert entry. Spare conduits are allowed for future expansion \1\ provided the expansion conduit is filled with acoustic fill and capped. /1/

3-5.8.2 Metallic Penetrations.

All metallic penetrations through SCIF walls shall be considered carriers of compromising emanations (CE) and pose TEMPEST hazards that shall be addressed. Unless directed otherwise by the CTTA:

- Metal conduit or pipe: provide a dielectric union inside the SCIF 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 ground.
- Metallic sprinkler (fire suppression) pipe: provide a UL Listed dielectric union inside the SCIF 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 ground.
- 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 ground. 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 SCIF perimeter adjacent to the penetration; see \1\ Figure 3-6. When a waveguide-below-cutoff RF filter is required by CTTA, provide between the SCIF perimeter and the nonconductive break. /1/

In addition, the CTTA may require additional TEMPEST countermeasures.

Figure 3-6 Duct Penetrations

3-5.8.3 Penetration Seals.

Seal both sides of perimeter penetrations with an acoustical foam or sealant finished to match adjacent wall, floor, or ceiling. Fire Stop System may be required for fire rated assemblies, see \1\ Figure 3-7. In addition, penetration seals shall meet TEMPEST requirements when required by CTTA. /1/

3-5.9 Vents, Ducts, and Pipes.

All vents or duct openings exceeding 96 square inches (619 cm^2) that penetrate the perimeter shall be protected with permanently affixed bars, grills, metal sound baffles or wave forms. 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 them.

- Bars shall be a minimum of ½ inch (13 mm) diameter steel, 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 3-8.
- Grills shall be shall be of ¾ inch (20 mm) #9 (10 gauge) case hardened expanded metal. When used, metal sound baffles or wave forms shall be

permanently installed and set no farther apart than 6 inch (150 mm) in one dimension.

- Metal sound baffles or \1\ waveguide-below-cutoff RF filters /1/ permanently installed and set no farther apart than 6 inch (150 mm) in one dimension.

\1\

3-5.10 Access Port.

For vents or ducts that require bars or grill, provide an accessible access panel in the bottom within the perimeter of the SCIF to allow visual inspection of the bars ,grill, or waveguide-below-cutoff RF filter see Figure 3-9.

If the area outside the SCIF is controlled (SECRET or equivalent proprietary space), the inspection port may be installed outside the perimeter of the SCIF, and be secured with an AO approved high-security lock such as a GSA combination padlock meeting Federal Specification FF-P-110.

3-5.11 Flashing or Rotating Light.

Per DoDM 5105.21 Vol 2, SCIF personnel must be informed when non-SCI-indoctrinated personnel have entered and departed the SCIF. This may be accomplished either verbally or through visual notification methods. A flashing or rotating light is an excellent measure to indicate the presence of non-SCI-indoctrinated personnel in the SCIF. When used, lights shall be placed to ensure visual observation by SCIF personnel. Controls shall be provided within the SCIF at each door including emergency exit doors.

3-5.12 Duress Alarm.

When a duress alarm is required, duress alarm shall initiate an alarm condition at the central monitoring station and shall not result in an audible or visual signal in the protected area.

/1/

Figure 3-7 Sealing Penetrations

UNACCEPTABLE

- Wall penetration is not sealed around duct.
- Wall not uniformly finished around duct penetration.

Figure 3-8 Bars on Penetration

Figure 3-9 Access Port

3-5.13 Electronic Security System (ESS).

ESS is the integrated electronic system that encompasses one or more of the following subsystems; access control system (ACS), intrusion detection system (IDS), and closed circuit television (CCTV) systems for assessment of alarm conditions. For notional ESS layout, see \1\ Figure 3-10. /1/

ESS shall meet the requirements of ICS 705-1 and IC Tech Spec-for ICD/ICS 705 and designed in accordance with UFC 4-021-02NF.

3-5.13.1 Access Control System (ACS).

ACS function is to ensure only authorized personnel are permitted ingress and egress into the SCIF. At a minimum, provide card reader with keypad at the primary entrance. Unless otherwise directed, the default ACS identifier credential shall be the \1\ Common Access Card (CAC)[1]. /1/

- Equipment containing access-control software programs shall be located in the SCIF or a SECRET controlled area.
- System data that is carried on transmission lines (e.g., access authorizations, personal identification, or verification data) to and from equipment located outside the SCIF shall be protected using FIPS 140-2 certified encrypted lines. If this communication technology is not feasible, transmission lines shall be installed as approved by the AO.
- Electric door strikes installed in conjunction with an ACS shall have a positive engagement and be UL 1034 Listed for burglar resistance.

3-5.13.2 Closed Circuit television (CCTV).

Cameras are not allowed within the SCIF perimeter. A camera may be provided on the exterior of the SCIF to supplement the monitoring of a SCIF entrance for remote control of the door from within the SCIF. The system shall provide a clear view of the SCIF entrance and shall be monitored/operated by SCI-indoctrinated personnel within the SCIF.

3-5.13.3 Intrusion Detection System (IDS).

The IDS shall be independent of systems safeguarding other facilities and compatible with Installation's central monitoring system. All Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, shall be protected by IDS, unless continuously occupied. If the occupants of a continuously occupied SCIF cannot observe all potential entrances to the SCIF, the SCIF shall be equipped with a system to alert occupants of intrusions into the SCIF. Emergency exit doors shall be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication.

\1\ [1] Per DoD 5200.08-R /1/

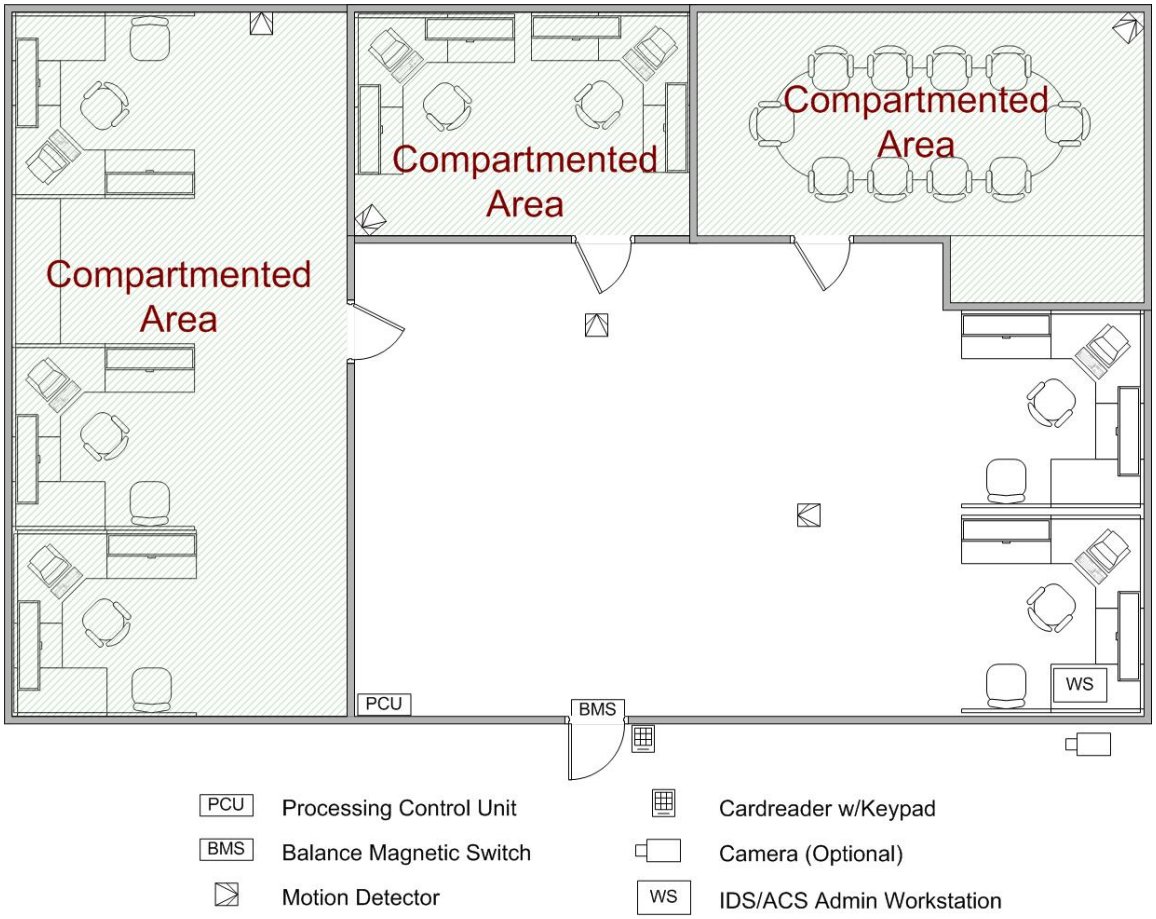
Provide point sensors on all \1\ /1/ doors, and man-passable openings. Provide motion sensors within SCIF to protect all windows, doors, and man-passable openings and detect movement within the SCIF to include compartmented areas. Motion detection sensors are not required above false ceilings or below false floors; however, these detectors may be required for critical and high threat facilities outside the U.S.

3-5.13.3.1 Intrusion Detection Installation and Components.

IDS installation, related components, and monitoring stations shall comply with Underwriters Laboratories (UL) 2050 Extent 3 standards. Systems developed and used exclusively by the U.S. Government do not require UL certification but shall comply with UL 2050 Extent 3 standards for installation. UL 2050 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 \1\ Figure 3-10 /1/ for a notional IDS layout.

\1\

Figure 3-10 Notional IDS Layout



/1/

Notes:

- Point sensor protect door
- Motion sensor monitoring door and space with access to SCI
- Camera (optional) monitors primary entrance - No cameras within SCIF
- Card reader with keypad located at primary entrance
- PCU and administrative workstation located within SCIF

3-5.13.3.2 Motion Detection Sensors.

\1\ Shall be 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). /1/

3-5.13.3.3 Point Sensors.

Shall be UL 634 high security switches (HSS) level 1 or 2. HSS Level 2 is preferred. \1\ Level 2 rated switches only include Balanced Magnetic Switches that pass additional performance testing. /1/

3-5.13.3.4 Sensor Cabling

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

3-5.13.3.5 Premise Control Unit (PCU).

PCU shall be located within the SCIF. System shall be configured to only allow cleared personnel located within the secure/protected area to initiate changes in access modes or alarm conditions.

3-5.13.3.6 External Transmission Line Security

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

3-5.13.3.7 Backup power.

Provide Twenty four hours of uninterruptible backup power. This may be provided by batteries, uninterruptible power supply (UPS), or generators, or any combination. Emergency backup power for IDS should not generate the requirement for a UPS or generator. If a generator or UPS is not available for backup, provide backup with batteries.

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

- Automatically transfer to an emergency electrical power source without causing alarm activation.
- Initiate an audible or visual indicator at the PCU to provide an indication of the primary or backup electrical 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.

3-5.13.3.8 IDS Approval.

The AO shall approve IDS proposals and plans prior to installation within a SCIF as part of the initial SCIF construction approval process.

\1\

3-5.14 Telecommunication Cabling System.

Cabling, patch panels, connector blocks, work area outlets, and cable connectors must be color coded[2] to distinguish their classification level. If color coding is not possible, cabling must be clearly marked to indicate their classification level. Cabling must enter a SCIF 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 requirement. Coordinate requirements with SSO, service provider, and CTTA. See TEMPEST Countermeasures.

/1/

3-5.14.1 Protected Distribution Systems (PDS).

A signal distribution system containing unencrypted NSI which enters an area of lesser classification, unclassified area, or uncontrolled (public) area must be protected according to the requirements of the current PDS standard. For a SCIF, that means a signal distribution system containing unencrypted NSI that leaves the SCIF must be protected according to the requirements of the NSTISSI No 7003. NSTISSI No. 7003 provides the minimum standards for PDS, refer to Service specific implementation policy or standards.

3-5.15 TEMPEST Countermeasures.

TEMPEST countermeasures and RF mitigation shall be provided at the direction of the CTTA. RF mitigation is recommended for all applications where RF interference from the outside of the SCIF is a concern inside the SCIF. \1\ /1/

3-5.15.1 Inspectable Space.

[2] Per DoDM 5105.21 Vol 1.

Inspectable space is the three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists. The CTTA shall determine the Inspectable Space for each facility.

Upon determination of the CTTA, the Inspectable space boundary may extend beyond the SCIF perimeter.

3-5.15.2 Radio Frequency (RF) Mitigation.

When directed by the CTTA, the SCIF shall be protected from compromising emanations. SCIF perimeter wall may have foil backed gypsum wall board or R-foil. Foil layer shall be placed inside the SCIF between the first and second layer of gypsum board. When directed, RF mitigation shall be provided for walls, ceilings, floors, and all penetrations including doors and windows. Doors shall be steel with RF gasket, and door frame shall be bonded to RF shield. Shielding shall be electrically bonded continuously at interfaces between, walls, floors, ceilings, doors, and windows. RF mitigation may include waveguides, power line and telecommunication line filters.

- Mounting apparatus shall not be connected to the RF shielding material in a manner that affects RF shielding performance.

3-5.15.3 RED/BLACK Telecommunication Systems.

All equipment, wirelines, components, and systems that process National Security Information (NSI) are considered RED. All 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 can be used to protect the signal line, the distribution system or other fortuitous conductors from conducting compromising signals beyond secure areas. The RED/BLACK concept is utilized to establish guidance for physical separation to decrease the probability that electromagnetic emissions from RED devices might couple to BLACK systems. Consult CTTA to determine TEMPEST countermeasures. Possible countermeasures may include:

- Red/Black separation.
- Distribution equipment must be designed with separate RED and BLACK connector blocks to prevent improper connection of RED and BLACK lines.
- Signal Line Isolators and Filters.

3-5.15.4 Paging, Intercom, and Public Address Systems.

- Systems should be totally contained within the SCIF. If not, for eavesdropping (using the speakers as microphones), a buffer amplifier is the standard

mitigation. For most systems, this is a simple amplifier in SCIF that takes the incoming audio signal and amplifies/distributes the signal to the speakers within the SCIF.

- In systems that require two-way communication, the system shall have electronic isolation. SCIF occupants must be alerted when the system is activated.
- Provide voice frequency, lowpass 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.
- When required, all electronic isolation components shall be installed within the SCIF as near to the point of SCIF penetration as possible.
- Equipment and signal lines should meet the separation recommendations

3-5.15.5 Fire Alarm and Mass Notification System (MNS).

The introduction of electronic systems that have components outside the SCIF should be avoided. TEMPEST concerns may require electronic isolation, validate requirements with CTTA. Speakers or other transducers, which are part of a system that is not wholly contained in the SCIF, may be required in the SCIF. Consult CTTA to determine TEMPEST countermeasures. Possible countermeasures may include:

- Separation of 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 in SCIF that takes the incoming audio signal and amplifies/distributes the signal to the speakers within the SCIF. 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 1711, the Standard for Amplifiers for Fire-Protective Signaling Systems. Therefore, any amplifier used in a MNS must meet UL 1711.
- Provide a MNS/Fire alarm subpanel within the SCIF with optical fiber backbone to the building system. Optical fiber shall have no metallic shielding, cladding, or strength members.
- In systems that require two-way communication, the system shall have electronic isolation. SCIF occupants should be alerted when the system is activated.
- When required, all electronic isolation components shall be installed within the SCIF as near to the point of SCIF penetration as possible.

3-5.15.6 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 plain text information 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. Consult CTTA to determine TEMPEST countermeasures. Possible countermeasures may include:

\1\

- Separation of Black power lines from RED telecommunication lines and processors.
- Power line Filters.

/1/

This Page Intentionally Left Blank

CHAPTER 4 CONSTRUCTION

4-1 DESIGN APPROVAL.

Per ICS 705-1, Final design for each construction project must be reviewed and approved by the Accrediting Official prior to start of construction.

4-2 CONSTRUCTION SECURITY.

Per ICS 705-1, construction plans and all related documents shall be handled and protected 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 be sent or posted on unprotected information technology systems or Internet venue without encryption.

A Site Security Manager (SSM) shall be the single point of contact regarding SCIF security and the individual responsible for all security aspects of the SCIF construction. SSM shall conduct periodic security inspections for the duration of the project to ensure compliance with the CSP.

4-3 ACCREDITATION PROCESS.

In support of the accreditation process, Project/Construction mangers shall provide the AO/SSM site plans, building floorplans, IDS plans, and information related to perimeter and compartment area wall construction, doors, locks, deadbolts, IDS, telecommunication systems, acoustical protection, and TEMPEST countermeasure.

4-4 INSPECTIONS.

Coordinate preliminary walkthrough with the SSM prior to substantial completion of SCIF space. Conduct periodic inspections of SCIF area to document and validate:

- Perimeter and Compartmented Area construction
    - Wall goes from floor slab (true floor) to underside of floor or roof deck (true ceiling)
    - Top and bottom sealed (both sides) with acoustical foam or sealant
    - Wall finished and uniform from true floor to true ceiling
    - Acoustic batting installation
    - Gypsum Wallboard installation
    - Floor and Ceiling construction
- Perimeter Penetrations
    - Sealed (both sides) with acoustical foam or sealant
    - Finished to match wall.
    - Metallic penetrations at perimeter (non-conductive break (e.g., canvas, rubber) installed at the interior perimeter.

- Perimeter Doors
    - Acoustical rating
    - Door assemblies sealed with acoustical foam or sealant (both sides) and finished to match wall
    - Door hardware (locks, closers, and hinges)
- Man-bar installation.
- Inspection ports.
- Tempest Countermeasures (as applicable)
    - RF shielding including penetrations
    - Waveguides
    - Doors including RF gaskets
    - Power Line Filters
    - Signal Line Isolators and Filters

Prior to walk through; assemble required documents for accreditation process and equipment providers. Requirements vary depending on project but in general assemble the following documents:

- Drawings:
    - Civil Site Plan
    - Architectural
        - Floor and Reflective Ceiling Plans
        - Wall sections (floor to ceiling)
        - Floor and Ceiling section
        - Door Schedule
        - Door head, jamb, and threshold details
        - Window schedule and details
    - Fire Protection
        - Sprinkler piping including penetration details
        - Fire Alarm system
        - Mass Notification System
    - Mechanical
        - HVAC plans, sections and details of SCIF penetrations, ductwork details sheets
        - Plumbing floor plans, detail for SCIF penetrations
    - Electrical
        - Site plan

        - Lighting, Power, Telecommunications, ESS plans. Plans must indicate device and panel location and include strobe lights and controls.
        - One-line diagrams for Power, Telecommunications, and ESS including RED/Black separation when required.
        - ESS Door wiring details
        - SCIF penetration details

- Submittals
    - Doors
    - Door Hardware (locks, closers, and hinges)
    - Acoustical ratings
    - Electronic Security Systems
    - Sound masking equipment
    - Tempest Countermeasures (as applicable)
        - RF shielding
        - RF sealant
        - Waveguides
        - Doors including RF gasketing
        - Power Line Filters
        - Signal Line Isolators and Filters

- As-Built drawings

4-5 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 shall include the SCIF and CA perimeters and should capture:

- Wall construction
    - Stud walls
    - Acoustic installation
    - Enhanced wall construction (9 gauge expanded metal)
    - R-foil or aluminum foil backed gypsum installation
    - Wall finishes (true floor to true ceiling)
    - Wall penetrations
- Duct construction including inspection ports and acoustic baffles
- Man-bar construction
- Sound masking devices

This Page Intentionally Left Blank

APPENDIX A REFERENCES

THE AMERICAN INSTITUTE OF ARCHITECTS

Architectural Graphics Standards

DEPARTMENT OF DEFENSE

Manuals:
http://www.dtic.mil/whs/directives/corres/pub1.html

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

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

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

\1\

Directives

http://www.dtic.mil/whs/directives/

DoD 5200.8-R (DTM) 08-004, *Physical Security Program*, Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division

/1/

Federal Specifications:
http://dodssp.daps.dla.mil/

FF-L-2740, *Locks, Combination*

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

\1\ FF-P-110, Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack) /1/

DIRECTOR OF NATIONAL INTELLIGENCE

Director of Central Intelligence Directive (DCID) No. 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities (superseded)*

Intelligence Community Directive (ICD) 705, *Sensitive Compartment Information Facilities*. http://www.ncix.gov/publications/policy/docs/ICD_705-Sensitive_Compartmented_Information_Facilities.pdf

Intelligence Community Standard Number 705-1 (ICS 705-1), *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities* http://www.ncix.gov/publications/policy/docs/ICS_705-01_Physical_and_Technical_Security_Standards_for_Sensitive_Compartmented_Information_Facilities.pdf

Intelligence Community Standard Number 705-2 (ICS 705-2), *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information* http://www.ncix.gov/publications/policy/docs/ICS_705-02_Standards_for_the_Accreditation_and_Reciprocal_Use_of_Sensitive_Compartmented_Information_Facilities.pdf

IC Tech Spec-for ICD/ICS 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* http://www.ncix.gov/publications/policy/docs/Technical_Specifications_for_SCIF_Construction-V1.2.pdf

COMMITTEE ON NATIONAL SECURITY SYSTEMS INSTRUCTION (CNSSI)

CNSSI No. 7000, *TEMPEST Countermeasures for Facilities (Confidential)*

NATIONAL SECURITY TELECOMMUNICATION AND INFORMATION SYSTEMS SECURITY (NSTISS)

NSTISSI No.7003, *Protective Distribution Systems (PDS)*

http://www.cnss.gov/instructions.html

NATIONAL FIRE PROTECTION ASSOCIATION
http://www.nfpa.org

NFPA 101, *Life Safety Code*

UNDERWRITER'S LABORATORIES, Inc.
http://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 1711*, Amplifiers for Fire Protective Signaling Systems*

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

UNIFIED FACILITIES CRITERIA
http://www.wbdg.org/ccb/browse_cat.php?o=29&c=4

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

UFC 4-010-02, *DoD Minimum Antiterrorism Standoff Distances for Buildings (FOUO)*

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

UFC 4-020-02, *DoD Security Engineering: Facilities Design Manual*, currently in Draft and unavailable

UFC 4-021-02NF, *Security Engineering: Electronic Security Systems*

This Page Intentionally Left Blank

APPENDIX B GLOSSARY

ACRONYMS

ACS	Access Control System
AO	Accrediting Official
BIA	Bilateral Infrastructure Agreements
CA	Compartmented Area
CSP	Construction Security Plan
CTTA	Certified TEMPEST Technical Authority
DNI	Director of National Intelligence
FFC	Fixed Facility Checklist
HNFA	Host Nation Funded Construction Agreements
HSS	High Security Switch
IC	Intelligence Community
IDS	Intrusion Detection System
MNS	Mass Notification System
NSI	National Security Information
PCU	Premise Control Unit
RF	Radio frequency
SETL	Security Environment Threat List
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SID	Security-in-depth
SOFA	Status of Forces Agreements
SSM	Site Security Manager

STC Sound Transmission Class

SWA Secure Working Area

TSWA Temporary Secure Working Areas

VTC Video teleconference

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.

Black LAN: A term applied to equipment, cables, or fiber that processes or carries only unclassified and/or encrypted information.

Certified TEMPEST Technical Authority (CTTA): U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a U.S. Government department or agency.

Closed Storage: The storage of SCI material in properly secured GSA approved security containers within an accredited SCIF.

Cognizant Security Authority (CSA): The single Principal designated by a SOIC (see definition of SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.

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

Construction Security Plan (CSP): A plan developed by the Site Security Manager (SSM) and approved by the AO, which outlines security measures to be followed to ensure security of the construction site and compliance with the SCIF construction requirements.

Continuous Operation: This condition exists when a SCIF is staffed 24 hours every day.

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.

Open Storage: The storage of SCI material within a SCIF in any configuration other than within GSA approved security containers.

Red Equipment: A term applied to equipment that processes unencrypted NSI that requires protection during electrical/electronic processing.

Red LAN: A term applied to equipment, cables, or fiber that processes or carries unencrypted National Security Information (NSI) that requires protection during electrical/electronic processing.

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

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

Site Security Manager (SSM): Person designated by the Accrediting Official (AO) that is responsible for all aspects of SCIF management and operations to include security policy implementation and oversight.

Sensitive Compartmented Information (SCI): Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

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

Sound Transmission Class (STC): The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value.

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

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

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 facilities 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.

U.S. Person: An individual who has been lawfully admitted for permanent residence as defined in 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by Title 8 U.S.C. 1324b (a)(3), and able to provide two forms of identification listed on Department of Homeland Security Form I-9, Employment Eligibility Verification.

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

APPENDIX C MINIMUM CONSTRUCTION

Table C-1 Minimum SCIF Wall Construction and Alarm

	CLASSIFICATION	WALL CONSTRUCTION[1]	IDS[3]	ACS[4]	DURESS
INSIDE UNITED STATES	Open Storage without SID[5]	Wall B - Enhanced Wall (Expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	NO
	Open Storage with SID[5]	Wall A - Standard Wall[2]	YES	YES	NO
	Closed Storage	Wall A - Standard Wall[2]	YES	YES	NO
	Continuous Operations	Wall A - Standard Wall[2]	YES	YES	NO
	Secure Working Area (SWA)	Wall A - Standard Wall[2]	YES	YES	NO
OUTSIDE UNITED STATES	SETL Cat I				
	Open Storage	Vault [2]	YES	YES	RECOMMENDED
	Closed Storage	Wall B - Enhanced Wall (Expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	NO
	Continuous Operation	Wall B - Enhanced Wall (expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	YES
	SETL Cat II & III				
	Open Storage	Wall B - Enhanced Wall (expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	RECOMMENDED
	Closed Storage	Wall B - Enhanced Wall (Expanded Metal)[2] Wall C - Enhanced Wall (Fire Retardant Plywood)[2]	YES	YES	NO
	Continuous Operation	Wall A - Standard Wall[2]	YES	YES	RECOMMENDED
	Secure Working Area (SWA)	Wall A - Standard Wall[2]	YES	YES	RECOMMENDED

Notes:

1. Table indicates the minimum wall construction, Accrediting Official shall determine construction requirements based on Risk Assessment.
2. Refer to IC Tech Spec-for ICD/ICS 705 for wall construction definitions and details. Include Radio Frequency (shielding) protection and sound attenuation as required.
3. IDS - Intrusion Detection System
4. ACS - Access Control System: Automated ACS is not required.
5. SID - Security In Depth