NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Advancing Counterintelligence and Security Excellence

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities

VERSION 1.5.1

IC Tech Spec – for ICD/ICS 705

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

July 26, 2021

This page intentionally left blank.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
WASHINGTON, DC

NCSC-2021-00068

MEMORANDUM FOR: Distribution

SUBJECT: Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.5.1, Chapter 13, Second Party Integree and Second Party Liaison Spaces within U.S. Sensitive Compartmented Information Facilities

REFERENCES:
A. Technical Specifications, Version 1.5, 13 Mar 20 (U)
B. ICD 705, Sensitive Compartmented Information Facilities, 26 May 10 (U)
C. ICS 705-01, Physical and Technical Standards for Sensitive Compartmented Information Facilities, 27 Sep 10 (U)
D. ICS 705-02, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities, 22 Dec 16 (U)

This memorandum promulgates modifications to Chapter 13 of the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (SCIF) Version 1.5, dated 13 Mar 2020 (Ref A) to the Intelligence Community (IC), which are effective upon signature of this memorandum.

This Chapter establishes general guidance to our stakeholders for implementing personnel, physical, and technical security standards prior to assigning and placing Second Party officers within United States SCIFs in accordance with authorized agreements.

The Technical Specifications are designed to be a living document that enables periodic updates to keep pace with changes that significantly impact protection of SCIFs from compromising emanations, inadvertent observations, and disclosure by unauthorized persons. To this end, guidance described in this addendum was developed in tandem with physical and technical experts from IC elements and with our industrial partners to arrive at robust security practices that will further supplement and bolster standards identified in ICS 705-01, Physical Security Standards for Sensitive Compartmented Information Facilities and ICS 705-02, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities.

SUBJECT: Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.5.1, Chapter 13, Second Party Integree and Second Party Liaison Spaces within U.S. Sensitive Compartmented Information Facilities

Please contact the National Counterintelligence and Security Center's Special Security Directorate at DNI-NCSC-SSD-CSG-PTSP-Mailbox@cia.ic.gov.

Michael J Orlando

JUL 26 2021

Michael J. Orlando
Acting Director

Date

Attachment:
Chapter 13 Modification_Version 1.5.1

Distribution:
Secretary of State, Department of State
Secretary of the Treasury, Department of the Treasury
Secretary of Defense, Department of Defense
Attorney General, Department of Justice
Secretary of the Interior, Department of the Interior
Secretary of Agriculture, Department of Agriculture
Secretary of Commerce, Department of Commerce
Secretary of Labor, Department of Labor
Secretary of Health and Human Services, Department of Health and Human Services
Secretary of Housing and Urban Development, Department of Housing and Urban Development
Secretary of Transportation, Department of Transportation
Secretary of Energy, Department of Energy
Secretary of Education, Department of Education
Secretary of Veterans Affairs, Department of Veterans Affairs
Secretary of Homeland Security, Department of Homeland Security
Administrator, Executive Office of the President
Administrator, Environmental Protection Agency
Director, Office of Management and Budget
United States Trade Representative
Administrator, Small Business Administration
Director, National Drug Control Policy
Director, Central Intelligence Agency
Administrator, Equal Employment Opportunity Commission
Chairman, Federal Communications Commission
Chairman, Federal Maritime Commission
Chairman, Federal Reserve System
Chairman, Federal Trade Commission
Administrator, General Services Administration

SUBJECT: Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.5.1, Chapter 13, Second Party Integree and Second Party Liaison Spaces within U.S. Sensitive Compartmented Information Facilities

Administrator, National Aeronautics and Space Administration
Archivist, National Archives and Records Administration
Director, National Science Foundation
Chairman, Nuclear Regulatory Commission
Director, Office of Government Ethics
Chairman, Privacy and Civil Liberties Oversight Board
Chairman, Security and Exchange Commission
Director, Selective Service System
Commissioner, Social Security Administration
Administrator, United States Agency for International Development
United States Postal Service
Chairman, United States International Trade Commission
Director, United States Peace Corps
Office of the Chief Administrative Officer

Change History

Rev. #	Date	Page	Changes	Approver
1.2	04/23/12	Cover	Banner Graphic, Version, Date	PTSEWG
1.2	04/23/12	4	Added note to warn users of classification when associating threat information and facility location.	PTSEWG
1.2	04/23/12	5	Re-worded approval of CAs to designate the AO as the primary approval authority of Compartmented Areas within SCIFs.	PTSEWG
1.2	04/23/12	9-10	Changed "Type X Gypsum" to "wallboard" to remove the standard of fire resistant gypsum and permit use of other wallboard types.	PTSEWG
1.2	04/23/12	9-10	Changed references to wall design drawings to "suggested" wall types to enable variety of wall construction techniques to meet the security standards.	PTSEWG
1.2	04/23/12	10	Added explanation to glue and screw plywood to ceiling and floor to clarify standard. Stud placement changed to 16 on center to match drawing and correct error.	PTSEWG
1.2	04/23/12	11	Added statement to finish wall and paint from true floor to true ceiling in Walls B and C to clarify and equal Type A Wall.	PTSEWG
1.2	04/23/12	9-10	Replaced drawings to reflect "suggested" wall construction methods and remove references to "Type X gypsum wallboard".	PTSEWG
1.2	04/23/12	17-19	Replaced drawings to reflect "suggested" wall construction methods and remove references to "Type X gypsum wallboard".	PTSEWG
1.2	04/23/12	56	Updated Federal Information Processing Standards (FIPS) encryption standards and certification to remove a standard that could not be met by commercial alarm systems.	PTSEWG
1.2	04/23/12	64	Replaced FIPS 140-2 with Advanced Encryption Standard (AES) to remove	PTSEWG

			a standard that could not be met by commercial alarm systems.	

Rev. #	Date	Page	Changes	Approver
1.2	04/23/12	TEMPEST Checklist	Removed references to "inspectable space" as requested by the TEMPEST Advisory Group (TAG).	PTSEWG
1.2	04/23/12	TEMPEST Checklist	Removed references to "Red-SCI" information.	PTSEWG
1.2	04/23/12	TEMPEST Checklist	Removed parenthetical reference to cell phones and Bluetooth.	PTSEWG
1.2	04/23/12	CA Checklist	Replaced Compartmented Area Checklist to reflect IC standards.	PTSEWG
1.2	04/23/12	SCIF Co-Use Request and MOA Form	Replaced Co-Use and MOA Form to include "joint-use" statements.	PTSEWG
1.3	03/26/15	Cover	Banner change, version, date	PTSEWG
1.3	03/26/15	B-C	Appended "D/NCSC Memorandum"	PTSEWG
1.3	03/26/15	D-G	"Appended Change History"	PTSEWG
1.3	03/26/15	3	Chapter 2.A (2)(a) Added: "NOTE" regarding prefabricated modular SCIFs.	PTSEWG
1.3	03/26/15	9	Chapter 3.C Corrected wording to match wall drawings on p.21.	PTSEWG
1.3	03/26/15	14	Chapter 3.G (7)(c.4) Correction and addition of guidance on vents and ducts perimeter protection.	PTSEWG
1.3	03/26/15	17-19	Reformatted wall types to reflect correct architectural graphics for prescribed materials.	PTSEWG
1.3	03/26/15	53	Chapter 7.A (2)(d) Added requirement for HSS switches.	PTSEWG
1.3	03/26/15	54	Chapter 7.A (2)(k) Changed to reflect restrictions on dissemination of installation plans.	PTSEWG
1.3	03/26/15	54	Chapter 7.A (3)(a.2) Added exception that sensors must be located within SCIF perimeter.	PTSEWG
1.3	03/26/15	55	Chapter 7.A (3)(b.7.e) Replaced "Zones" with "IDE sensor points".	PTSEWG
1.3	03/26/15	56	Chapter 7.A (3)(c.1) Added language for approval authority.	PTSEWG

1.3	03/26/15	56	Chapter 7.A (3)(c.2) Added language for integrated IDS and Remote Access.	PTSEWG
1.3	03/26/15	56-57	Chapter 7.A (3)(c.2) Added system application software requirements.	PTSEWG
1.3	03/26/15	58-59	Replaced "access/secure" with "arm/disarm" throughout.	PTSEWG
Rev. #	**Date**	**Page**	**Changes**	**Approver**
1.3	03/26/15	58	Chapter 7.B (2) Added "A record shall be maintained that identifies the person responsible for disarming the system".	PTSEWG
1.3	03/26/15	87	Chapter 12.G (2) Changed Section header to read "Inspections/Reviews, added same where the term "inspection" or "review" used. The responsibility to perform as such was changed from "IC element head" to the AO, or designee.	PTSEWG
1.3	03/26/15	SCIF Co-Use Request and MOA Form	Appended Co-Use Request and MOA Form	PTSEWG
1.4	06/27/17	Cover	Banner change, version, date	PTSEWG
1.4	06/27/17	i-iii	Appended "D/NCSC Memorandum"	PTSEWG
1.4	06/27/17	iv-vii	"Appended Change History"	PTSEWG
1.4	06/27/17	1	Chapter 1.B.2 Added SAPF Language	PTSEWG
1.4	06/27/17	12	Chapter 3.E.1.b Added egress device language	PTSEWG
1.4	06/27/17	60	Chapter 7.C.1.c Added, "…IAW UL 2050 requirements (60 minutes)"	PTSEWG
1.4	06/27/17	71-74	Chapter 10 Revised	PTSEWG
1.4	06/27/17	75-76	Chapter 11.B.5 Added sub-bullets to address CNSSI 5002	PTSEWG
1.4	06/27/17	90-91	Chapter 12.L1/2/7 Added clarification language	PTSEWG
1.4	06/27/17	91-92	Chapter 12.M.4 Synchronized bullets	PTSEWG
1.5	11/13/19	3-4	Chapter 2.A.3.a Added clarification language	PTSEWG
1.5	11/13/19	5-6	Chapter 2.C.2	PTSEWG

			Defined CA Types	
1.5	11/13/19	8	Chapter 3. Added Pre-Construction Checklist language	PTSEWG
1.5	11/13/19	13-15	Chapter 3.E Expanded SCIF Door Criteria	PTSEWG
1.5	11/13/19	30	Chapter 4.E.2 Added reference to Inspectable Materials Checklist	PTSEWG
1.5	11/13/19	35	Chapter 5.A Added language in Applicability	PTSEWG
1.5	11/13/19	46	Chapter 6.A.1.a Added exception language	PTSEWG
1.5	11/13/19	74-77	Chapter 10 Changed “CSA” to “AO” where appropriate	PTSEWG
1.5	11/13/19	90	Chapter 12.G.8 Added TSCM language to Inspections/Reviews	PTSEWG
1.5	11/13/19	95-97	Chapter 12.N/O/P Added CUA instructions	PTSEWG
1.5	11/13/19	98	Chapter 13 Updated FFC and added CUA Guide and Cancellation Forms, Inspectable Materials Checklist, Pre-construction Checklist,	PTSEWG
1.5.1	07/26/21	Cover	Version and Date Change	PTSEWG
1.5.1	07/26/21	i-iii	Appended “D/NCSC Memorandum”	PTSEWG
1.5.1	07/26/21	iv-vii	Appended “Change History”	PTSEWG
1.5.1	07/26/21	104/113	Chapter 13, FVEY Chapter inserted. Changing Original Chapter 13, Forms & Plans to Chapter 14, Forms & Plans	PTSEWG

This page intentionally left blank.

Table of Contents

Chapter 1. Introduction ……..…….... 1
A. Purpose ……...…….....……..…...…. 1
B. Applicability...…….……..... 1
Chapter 2. Risk Management…….…..... 4
A.Analytical Risk Management Process…….……...…….....… 4
B.Security in Depth (SID)……...…….……..... 5
C. Compartmented Area (CA) ……...……..... 6
Chapter 3. Fixed Facility SCIF Construction…….. 10
A. Personnel……..... 10
B.Construction Security……...…….…….…… 11
C.Perimeter Wall Construction Criteria……...…….…….……..... 12
D.Floor and Ceiling Construction Criteria……...….…….…….…….... 15
E.SCIF Door Criteria…….……..... 15
F. SCIF Window Criteria…….……..... 17
G. SCIF Perimeter Penetrations Criteria……...…….……..... 17
H. Alarm Response Time Criteria for SCIFs within the U.S. ……..…….……..... 19
I. Secure Working Areas (SWA) …….. 19
J. Temporary Secure Working Area (TSWA) ……..……...…….. .. 20
Chapter 4. SCIFs Outside the U.S. and NOT Under Chief of Mission (COM) Authority..... 26
A. General…….. 26
B.Establishing Construction Criteria Using Threat Ratings…….……..... 26
C. Personnel…….. 29
D.Construction Security Requirements…….……..... 30
E.Procurement of Construction Materials…….…….. 33
F.Secure Transportation for Construction Material……..….. 34
G.Secure Storage of Construction Material…….....….... 35
H. Technical Security…….……..…….. 36
I. Interim Accreditations……..…….... 36
Chapter 5. SCIFs Outside the U.S. and Under Chief of Mission Authority…….…..... 38
A. Applicability…….… 38
B. General Guidelines…… 38
C. Threat Categories…….…...… 39
D. Construction Requirements…….... 39
E. Personnel…… 41
F. Construction Security Requirements……..... 42
G. Procurement of Construction Materials…….…… 45
H. Secure Transportation for Construction Material……... 46
I. Secure Storage of Construction Material…… 47

J. Technical Security…….. 47
K. Interim Accreditations…… 48
Chapter 6. Temporary, Airborne, and Shipboard SCIFs……. 50
A. Applicability…….. 50
B. Ground-Based T-SCIFs……. 50
C. Permanent and Tactical SCIFS Aboard Aircraft……... 52
D. Permanent and Tactical SCIFs on Surface or Subsurface Vessels…… 54
Chapter 7. Intrusion Detection Systems (IDS) …… 60
A. Specifications and Implementation Requirements……..... 60
B. IDS Modes of Operation…….…...……. 65
C. Operations and Maintenance of IDS……...…… 67
D. Installation and Testing of IDS…….…..... 68
Chapter 8. Access Control Systems (ACS) …… 71
A. SCIF Access Control……..... 71
B. ACS Administration……...…..… 72
C. ACS Physical Protection…….…...…. 72
D. ACS Recordkeeping……...…..… 72
. E. Using Closed Circuit Television (CCTV) to Supplement ACS…….. 73
F. Non-Automated Access Control…….……..... 73
Chapter 9. Acoustic Protection…… 75
A. Overview……. 75
B. Sound Group Ratings…….. 75
C. Acoustic Testing……...… 75
D. Construction Guidance for Acoustic Protection…….…….……... 76
E. Sound Transmission Mitigations…….……..... 76
Chapter 10. Portable Electronic Devices with Recording Capabilities and Embedded Technologies (PEDs/RCET)…….…….…… 79
A. Approved Use of PEDs/RECET in a SCIF…….……..... 79
B. Prohibitions……. 80
C. PED/RCET Risk Levels…….…… 80
D. Risk Mitigation…….….81
Chapter 11. Telecommunications Systems…….. 83
A. Applicability…… 83
B. Unclassified Telephone Systems…….… 83
C. Unclassified Information Systems…….……. 85
D.Using Closed Circuit Television (CCTV) to Monitor the SCIF Entry Point(s) …..….. 85
E.Unclassified Wireless Network Technology…….…….. 85
F.Environmental Infrastructure Systems…….…..... 86
G.Emergency Notification Systems…….…..... 86

H. System Access…… 87
I. Unclassified Cable Control…….. 87
J. Protected Distribution Systems……...…. 88
K. References……..……..……..... 88
Chapter 12. Management and Operations……..… 91
A. Purpose……..… 91
B. SCIF Repository…….……. 91
C. SCIF Management……...…….…... 92
D. SOP…….....…….… 93
E. Changes in Security and Accreditation……...……..…. 94
F. General……..…….…….…… 94
G. Inspections/Reviews…….…… 95
H. Control of Combinations…….. 95
I. De-Accreditation Guidelines……..…….…..…… 96
J. Visitor Access…….…… 96
K. Maintenance…….……..…… 98
L. IDS and ACS Documentation Requirements……...…….……..... 98
M. Emergency Plan……...……... 99
N. SCIF Co-Use and Joint Use….....…….…... 100
O. CUA Form and Instructions...….……...…….…... 101
P. CUA Cancellation...……...……... 102
Chapter 13. Second Party Integree and Second Party Liaison Spaces within SCIFs...……..… 104
Chapter 14. Forms and Plans…….….……113
Fixed Facility Checklist TEMPEST Checklist
Compartmented Area Checklist Shipboard
Checklist Submarine Checklist
Aircraft/UAV Checklist
SCIF Co-Use or Joint-Use Request and MOA
SCIF Co-Use or Joint-Use Request Users Guide
Cancellation of SCIF Co-Use or Joint-Use
Pre-Construction Checklist
Construction Security Plan (CSP)
Inspectable Materials Checklist

This page intentionally left blank.

Chapter 1. Introduction

A. Purpose

This Intelligence Community (IC) Technical Specification sets forth the physical and technical security specifications and best practices for meeting standards of Intelligence Community Standard (ICS) 705-01 (Physical and Technical Standards for Sensitive Compartmented Information Facilities). When the technical specifications herein are applied to new construction and renovations of Sensitive Compartmented Information Facilities (SCIFs), they shall satisfy the standards outlined in ICS 705-01 to enable uniform and reciprocal use across all IC elements and to assure information sharing to the greatest extent possible. This document is the implementing specification for Intelligence Community Directive (ICD) 705 (Sensitive Compartmented Information Facilities), ICS 705-01, and ICS 705-02 (Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities.

The specifications contained herein will facilitate the protection of Sensitive Compartmented Information (SCI) against compromising emanations, inadvertent observation and disclosure by unauthorized persons, and the detection of unauthorized entry.

B. Applicability

IC Elements shall fully implement this standard within 180 days of its signature.

1. SCIFs that have been de-accredited but controlled at the SECRET level (IAW 32 Code of Federal Regulations (CFR) parts 2001 and 2004) for less than one year may be re-accredited. The IC SCIF repository shall indicate that the accreditation was based upon the previous standards.

2. When the technical specifications herein have been applied to new construction, renovations, and operation of Special Access Program Facilities (SAPFs), those facilities shall satisfy the standards outlined in ICD 705 to enable uniform use across all IC elements for accreditation by IC elements as a Sensitive Compartmented Information Facility.

    a) Accreditation of a SAPF as a SCIF will be based upon a review of all required SCIF construction documentation to ensure all ICD 705 requirements were met in the construction, maintenance, and operation of the SAPF.

    b) The Accrediting Official (AO) will conduct a review of all SAPF accreditation documentation for compliance with the technical specifications herein.

        (1) If all required documentation is available and correct, the AO will issue SCIF accreditation.

        (2) If all required documentation is not available and correct, or waivers have been authorized, the AO is not required to issue SCIF accreditation.

c) If the facility is to be maintained as a SAPF and co-utilized as a SCIF, the security posture of the facility will be to the highest requirement of the two.

(1) The AO may issue a more restrictive accreditation based upon the SCI requirements associated with the new SCIF accreditation. For example, 5 minute response versus 15 minutes, or Closed Storage versus Open Storage.

(2) Program indoctrination will be coordinated as part of the co-utilization agreement. Compartmented Areas may be utilized, but no other sub-division of the facility will be permitted. Facilities requiring additional protections are not suitable for co-utilization.

This page intentionally left blank.

Chapter 2. Risk Management

A. Analytical Risk Management Process

1. The Accrediting Official (AO) and the Site Security Manager (SSM) should evaluate each proposed SCIF for threats, vulnerabilities, and assets to determine the most efficient countermeasures required for physical and technical security. In some cases, based upon that risk assessment, it may be determined that it is more practical or efficient to mitigate a standard. In other cases, it may be determined that additional security measures should be employed due to a significant risk factor.

2. Security begins when the initial requirement for a SCIF is known. To ensure the integrity of the construction and final accreditation, security plans should be coordinated with the AO before construction plans are designed, materials ordered, or contracts let.

a) Security standards shall apply to all proposed SCI facilities and shall be coordinated with the AO for guidance and approval. Location of facility construction and or fabrication does not exclude a facility from security standards and or review and approval by the AO. SCI facilities include but are not limited to fixed facilities, mobile platforms, prefabricated structures, containers, modular applications or other new or emerging applications and technologies that may meet performance standards for use in SCI facility construction.

NOTE: Advertised claims by manufactures that their product(s), to include mobile platforms, prefabricated structures, containers and modular structures are built to SCIF standards and can be accredited without modification may not be accurate. AOs are responsible for ensuring security controls spelled out in the ICD/ICS 705 series and this document are implemented to protect the security integrity of the proposed SCIF prior to accreditation.

b) Mitigations are verifiable, non-standard methods that shall be approved by the AO to effectively meet the physical/technical security protection level(s) of the standard. While most standards may be effectively mitigated via non-standard construction, additional security countermeasures and/or procedures, some standards are based upon tested and verified equipment (e.g., a combination lock meeting Federal Specification FF-L 2740) chosen because of special attributes and could not be mitigated with non-tested equipment. The AO's approval is documented to confirm that the mitigation is at least equal to the physical/technical security level of the standard.

c) Exceeding a standard, even when based upon risk, requires that a waiver be processed and approved in accordance with ICD 705.

3. The risk management process includes a critical evaluation of threats, vulnerability, and assets to determine the need and value of countermeasures. The process may include the following:

a) Threat Analysis. Assess the capabilities, intentions, and opportunity of an adversary to exploit or damage assets or information. For SCI Facilities under Chief of Mission (COM) authority or established on a permanent or temporary

basis within or on U.S. diplomatic facilities/compounds, use the Overseas Security Policy Board (OSPB), Security Environment Threat List (SETL) to determine technical threat to a location. When evaluating for TEMPEST, the Certified TEMPEST Technical Authorities (CTTA) shall use the National Security Agency Information Assurance (NSA IA) list as an additional resource for specific technical threat information. *NOTE: These threat documents are classified. Associating the threat level or other threat information with the SCIF location (including country, city, etc.) will normally carry the same classification level identified in the threat document. Ensure that SCIF planning documents and discussions that identify threat with the country or SCIF location are protected accordingly.* It is critical to identify other occupants of common and adjacent buildings. (However, do not attempt to collect information against U.S. persons in violation of Executive Order (EO) 12333.) In areas where there is a diplomatic presence of high and critical technical threat countries, additional countermeasures may be necessary.

b) Vulnerability Analysis. Assess the inherent susceptibility to attack of a procedure, facility, information system, equipment, or policy.

c) Probability Analysis. Assess the probability of an adverse action, incident, or attack occurring.

d) Consequence Analysis. Assess the consequences of such an action (expressed as a measure of loss, such as cost in dollars, resources, programmatic effect/mission impact, etc.).

B. Security in Depth (SID)

1. SID describes the factors that enhance the probability of detection before actual penetration to the SCIF occurs. The existence of a layer or layers of security that offer mitigations for risks may be accepted by the AO. An important factor in determining risk is whether layers of security already exist at the facility. If applied, these layers may, with AO approval, alter construction requirements and extend security alarm response time to the maximum of 15 minutes. Complete documentation of any/all SID measures in place will assist in making risk decisions necessary to render a final standards decision.

2. SID is mandatory for SCIFs located outside the U.S. due to increased threat.

3. The primary means to achieve SID are listed below and are acceptable. SID requires that at least one of the following mitigations is applied:

a) Military installations, embassy compounds, U.S. Government (USG) compounds, or contractor compounds with a dedicated response force of U.S. persons.

b) Controlled buildings with separate building access controls, alarms, elevator controls, stairwell controls, etc., required to gain access to the buildings or elevators. These controls shall be fully coordinated with a formal agreement or managed by the entity that owns the SCIF.

c) Controlled office areas adjacent to or surrounding SCIFs that are protected by alarm equipment installed in accordance with manufacturer's instructions. These controls shall be fully coordinated with a formal agreement or managed by the entity that owns the SCIF.

d) Fenced compounds with access controlled vehicle gate and/or pedestrian gate.

e) The AO may develop additional strategies to mitigate risk and increase probability of detection of unauthorized entry.

C. Compartmented Area (CA)

1. Definition

A CA is an area, room, or a set of rooms within a SCIF that provides controlled separation between control systems, compartments, sub-compartments, or Controlled Access Programs.

2. CA Types

a) Type I CAs are intended for workstation environments that are used to view and process compartmented information. These areas may be comprised of open bays, open spaces, or a set of rooms with multiple cubicles in an accredited SCIF. Within these areas, compartmented information may be securely viewed and/or processed via an approved computer workstation by authorized personnel. Workstations in these environments may include computers with single or multiple monitors. When monitor positioning alone will not adequately protect the material from unauthorized viewing, i.e., shoulder surfing, polarized privacy screens shall be used. Compartmented data shall never be openly displayed on a monitor that faces a primary door or common work area. In addition to processing compartmented information on approved computer workstations, Type I CAs may also include the use of printers, copiers, and scanners if appropriate procedures for control of hard copy material have been established and approved by the AO. No storage or discussion is authorized, logical and/or physical.

b) Type II CAs are areas where discussions of compartmented information may take place. If so equipped and approved, compartmented information may also be viewed and processed. This CA comprises a room, e.g., office or conference room, inside an accredited SCIF where compartmented discussions may be held by authorized personnel. All Type II CAs must meet existing sound transmission class (STC) requirements per ICS 705-1 to ensure that the room or office retains sound within its perimeter. In addition to compartmented discussions, Type II CAs may be used for secure video teleconferencing (SVTC) and related communication conferencing and the use of secure telephones for compartmented discussions. The use of printers, scanners, fax, copiers, and the secure transfer of data to approved removable media require prior approval. No storage is authorized, logical and/or physical.

c) Type III: A restricted discussion area used for viewing, processing, printing, copying, storage and control of accountable compartmented information. This CA is

intended for storing and retaining compartmented information when accountability and strict control of compartmented program information is required. This includes, but is not limited to: notes, briefs, slides, electronic presentations, analytic papers, removable hard drives, field packs, thumb drives, laptops, personal electronic devices (PEDs) or hand-held devices that store compartmented information. In addition to the storage of compartmented material in a GSA-approved container, Type III CAs may be used for processing compartmented information on approved computer workstations; the use of printers, scanners, and copiers; the secure transfer of data to approved removable media; the use of secure facsimile machines; and the use of secure telephone equipment (STE) for compartmented discussions. All personnel residing within or who have unfettered access to a Type III CA must be formally briefed into all compartments that reside within the Type III CA. Visitors are permitted within Type III areas only when all compartmented information (for which the visitor is not briefed) is stored within containers, out of sight, and while the visitor is under constant observation by a fully briefed person.

3. Requirements

   a) The CA shall be approved by the AO with the concurrence of the CA Program Manager or designee. The CA Checklist (Chapter 13) shall be used to request approval.

   b) Any construction or security requirements above those listed herein require prior approval from the element head as described in ICS 705-2.

4. Access Control

   a) Access control to the CA may be accomplished by visual recognition or mechanical/electronic access control devices.

   b) Spin-dial combination locks shall not be installed on CA doors.

   c) Independent alarm systems shall not be installed in a CA.

5. Visual Protection of CA Workstations

If compartmented information will be displayed on a computer terminal or group of terminals in an area where everyone is not accessed to the program, the following measures may be applied to reduce the ability of “shoulder surfing” or inadvertent viewing of compartmented information:

- Position the computer screen away from doorway/cubicle opening.
- Use a polarizing privacy screen.
- Use partitions and/or signs.
- Existing private offices or rooms may be used but may not be a mandatory requirement.

6. Closed Storage

When the storage, processing, and use of compartmented information, product, or deliverables is required, and all information shall be stored while not in use, then all of the following shall apply:

a) Access and visual controls identified above shall be the standard safeguard.

b) Compartmented information shall be physically stored in a General Services Administration (GSA) approved safe.

7. Open Storage

In rare instances when open storage of information is required, the following apply:

a) If the parent SCIF is accredited for open storage, a private office with access control on the door is adequate physical security protection.

b) If the parent SCIF has been built and accredited for closed storage, then the CA perimeter shall be constructed and accredited to open storage standards.

c) The CA AO may approve open or closed storage within the CA. Storage requirements shall be noted in both the CA Fixed Facility Checklist (FFC) and, if appropriate, in a Memorandum of Understanding (MOU).

8. Acoustic and Technical Security

a) All TEMPEST, administrative telephone, and technical surveillance countermeasure (TSCM) requirements for the parent SCIF shall apply to the CA and shall be reciprocally accepted.

b) When compartmented discussions are required, the following apply:

(1) Use existing rooms that have been accredited for SCI discussions.

(2) Use administrative procedures to restrict access to the room during conversations.

This page intentionally left blank.

Chapter 3. Fixed Facility SCIF Construction

Requirements outlined within this chapter apply to all fixed facility SCIFs. The SCIF Pre-Construction Checklist is found in Chapter 13 and may be completed and sent to the Cognizant Security Authority (CSA) and/or AO as part of the concept approval process. All questions about the checklist content and expected information should be directed to the project CSA/AO. Additional information and requirements for facilities located outside the U.S., its possessions or territories, are found in Chapters 4 and 5. Additional information and requirements for temporary SCIFs are described in Chapter 6.

A. Personnel

Roles and responsibilities of key SCIF construction personnel are identified in ICS 705-1 and restated here for reference.

1. AO Responsibilities

   a) Provide security oversight of all aspects of SCIF construction under their security purview.

   b) Review and approve the design concept, Construction Security Plan (CSP), and final design for each construction project prior to the start of SCIF construction.

   c) Depending on the magnitude of the project, determine if the Site Security Manager (SSM) performs duties on a full-time, principal basis, or as an additional duty to on-site personnel.

   d) Accredit SCIFs under their cognizance.

   e) Prepare waiver requests for the IC element head or designee.

   f) Provide the timely input of all required SCIF data to the IC SCIF repository.

   g) Consider SID on USG or USG-sponsored contractor facilities to substitute for standards herein. (SID shall be documented in the CSP and the FFC.)

2. Site Security Managers (SSMs) Responsibilities

   a) Ensure the requirements herein are implemented and advise the AO of compliance or variances.

   b) In consultation with the AO, develop a CSP regarding implementation of the standards herein. (This document shall include actions required to document the project from start to finish.)

   c) Conduct periodic security inspections for the duration of the project to ensure compliance with the CSP.

   d) Document security violations or deviations from the CSP and notify the AO within 3 business days.

   e) Ensure that procedures to control site access are implemented.

3. CTTA Responsibilities

a) Review SCIF construction or renovation plans to determine if TEMPEST countermeasures are required and recommend solutions. To the maximum extent practicable, TEMPEST mitigation requirements shall be incorporated into the SCIF design.

b) Provide the CSA and AO with documented results of review with recommendations.

4. Construction Surveillance Technicians (CSTs) Responsibilities

a) Supplement site access controls, implement screening and inspection procedures, as well as monitor construction and personnel, when required by the AO.

b) In low and medium technical threat countries, begin surveillance of non-cleared workers at the start of SCIF construction or the installation of major utilities, whichever comes first.

c) In high and critical technical threat countries, begin surveillance of non-cleared workers at the start of: construction of public access or administrative areas adjacent to the SCIF; SCIF construction; or the installation of major utilities, whichever comes first.

B. Construction Security

1. Prior to awarding a construction contract, a CSP for each project shall be developed by the SSM and approved by the AO.

2. Construction plans and all related documents shall be handled and protected in accordance with the CSP.

3. For SCIF renovation projects, barriers shall be installed to segregate construction workers from operational activities and provide protection against unauthorized access and visual observation. Specific guidance shall be contained in the CSP.

4. Periodic security inspections shall be conducted by the SSM or designee for the duration of the project to ensure compliance with construction design and security standards.

5. Construction and design of SCIFs should be performed by U.S. companies using U.S. citizens to reduce risk, but may be performed by U.S. companies using U.S. persons (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)). The AO shall ensure mitigations are implemented when using non-U.S. citizens. These mitigations shall be documented in the CSP.

6. All site control measures used shall be documented in the CSP. Among the control measures that may be considered are the following:

- Identity verification.
- Random searches at site entry and exit points.

- Signs at all entry points listing prohibited and restricted items (e.g., cameras, firearms, explosives, drugs, etc.).
- Physical security barriers to deny unauthorized access.
- Vehicle inspections.

C. Perimeter Wall Construction Criteria

1. General

a) SCIF perimeters include all walls that outline the SCIF confines, floors, ceilings, doors, windows and penetrations by ductwork, pipes, and conduit. This section describes recommended methods to meet the standards described within ICS 705-1 for SCIF perimeters.

b) Perimeter wall construction specifications vary by the type of SCIF, location, use of SID, and discussion requirements.

c) Closed storage areas that do not require discussion areas do not have any forced entry or acoustic requirements.

d) Open storage facilities without SID require additional protection against forced and surreptitious entry.

e) When an existing wall is constructed with substantial material (e.g., brick, concrete, cinderblock, etc.) equal to meet the perimeter wall construction standards, the existing wall may be utilized to satisfy the specification.

2. Closed Storage, Secure Working Area (SWA), Continuous Operation, or Open Storage with SID - Use Wall A - Suggested Standard Acoustic Wall (see construction drawing for details).

a) Three layers inch-thick gypsum wallboard (GWB), one layer on the uncontrolled side of the SCIF and two on the controlled side of the SCIF, to provide adequate rigidity and acoustic protection (Sound Class 3).

b) allboard shall be attached to 3 inch-wide 16 gauge metal studs or wooden 2 x 4 studs placed no less than 16" on center (o.c.).

c) 16 gauge continuous track (top & bottom) w/ anchors at 32" o.c. maximum) – bed in continuous bead of acoustical sealant.

d) The interior two layers of wallboard shall be mounted so that the seams do not align (i.e., stagger joints).

e) Acoustic fill 3 ½ " (89mm) sound attenuation material, fastened to prevent sliding down and leaving void at the top.

f) The top and bottom of each wall shall be sealed with an acoustic sealant where it meets the slab.

g) Fire safe non-shrink grout, or acoustic sealant in all voids above/below track both sides of partition.

h) Entire wall assembly shall be finished and painted from true floor to true ceiling.

3. Open Storage without SID -- Use Wall B - Suggested Wall for Expanded Metal or Wall C - Suggested Wall for Plywood.

a) hree layers of inch-thick GWB, one layer on the uncontrolled side of the SCIF and two on the controlled side of the SCIF to provide adequate rigidity and acoustic protection (Sound Class 3).

b) allboard shall be attached to 3 inch-wide 16 gauge metal studs or wooden 2 x 4 studs placed no less than 16" o.c.

c) 16 gauge continuous track (top & bottom) w/ anchors at 32" on center (o.c.) maximum) – bed in continuous bead of acoustical sealant.

d) Wall B - Suggested Wall for Expanded Metal (see drawing for Wall B-Suggested Construction for Expanded Metal).

(1) Three-quarter inch mesh, # 9 (10 gauge) expanded metal shall be affixed to the interior side of all SCIF perimeter wall studs.

(2) Expanded metal shall be spot-welded to the studs every six inches along the length of each vertical stud and at the ceiling and floor.

(3) Hardened screws with one inch washers or hardened clips may be used in lieu of welding to fasten metal to the studs. Screws shall be applied every six inches along the length of each vertical stud and at the ceiling and floor.

(4) Fastening method shall be noted in the FFC.

(5) Entire wall assembly shall be finished and painted from true floor to true ceiling.

e) Wall C - Suggested Wall for Plywood (see drawing for Wall C-Suggested Construction for Plywood).

(1) hree layers of inch-thick GWB, two layers on the uncontrolled side and one layer GWB over minimum ½ " plywood on the controlled side of the SCIF.

NOTE: CTTA recommended countermeasures (foil backed GWB or layer of approved Ultra Radiant R-Foil) shall be installed in accordance with (IAW) best practices for architectural Radio Frequency (RF) shielding. Foil shall be located between the layer of plywood and GWB.

(2) 1/2" Plywood affixed 8' vertical by 4' horizontal to 16 gauge studs using glue and #10 steel tapping screws at 12 o.c.

(3) GWB shall be mounted to plywood with screws avoiding contact with studs to mitigate any possible acoustic flanking path.

(4) 16 gauge continuous track (top & bottom) w/ anchors at 32" o.c. maximum) – bed in continuous bead of acoustical sealant.

(5) Fire safe non-shrink grout, or acoustic sealant in all voids above/below track both sides of partition.

(6) Entire wall assembly shall be finished and painted from true floor to true ceiling.

4. Radio Frequency (RF) Protection for Perimeter Walls

a) RF protection shall be installed at the direction of the CTTA when a SCIF utilizes electronic processing and does not provide adequate RF attenuation at the inspectable space boundary. It is recommended for all applications where RF interference from the outside of the SCIF is a concern inside the SCIF.

b) Installation of RF protection should be done using either the drawings or *Best Practices Guidelines for Architectural Radio Frequency Shielding,* prepared by the Technical Requirements Steering Committee under the Center for Security Evaluation. This document is available through the Center for Security Evaluation, Office of the Director of National Intelligence (NCSC/CSE).

5. Vault Construction Criteria

GSA-approved modular vaults meeting Federal Specification AA-V-2737 or one of the following construction methods may be used:

a) Reinforced Concrete Construction

(1) Walls, floor, and ceiling will be a minimum thickness of eight inches of reinforced concrete.

(2) The concrete mixture will have a comprehensive strength rating of at least 2,500 pounds per square inch (psi).

(3) Reinforcing will be accomplished with steel reinforcing rods, a minimum of inches in diameter positioned centralized in the concrete pour and spaced horizontally and vertically six inches on center; rods will be tied or welded at the intersections.

(4) The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

b) Steel-Lined Construction Where Unique Structural Circumstances Do Not Permit Construction of a Concrete Vault

(1) Construction will use ¼ inch-thick steel alloy-type plates having characteristics of high-yield and high-tensile strength.

(2) The steel plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates.

(3) If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling.

(4) If floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor

and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

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

D. Floor and Ceiling Construction Criteria

1. Floors and ceilings shall be constructed to meet the same standards for force protection and acoustic protection as walls.

2. All floor and ceiling penetrations shall be kept to a minimum.

E. SCIF Door Criteria

1. Door type definitions:
   a) Primary door: A SCIF perimeter door recognized as the main entrance.
   b) Secondary door: A SCIF perimeter door employed as both an entry and egress door that is not the Primary door.
   c) Emergency egress-only door: A SCIF perimeter door employed as an emergency egress door with no entry capability.

2. Primary door criteria:
   a) There shall be only one Primary door to a SCIF.
   b) The Primary door shall be equipped with the following:
      (1) A GSA-approved pedestrian door deadbolt meeting the most current version of Federal Specification FF-L-2890. Previously AO-approved FFL-2740 integrated locking hardware may be used. Additional standalone and flush-mounted dead bolts are prohibited.
      (2) A combination lock meeting the most current version of Federal Specification FFL- 2740. Previously AO-approved combination lock or deadbolt lock type may be used.
      (3) An approved access control device (see Chapter 8). May be equipped with a by-pass keyway for use in the event of an access control system failure.
      (4) Include requirements in E.5 below.

3. **Secondary** door criteria:
   a) Secondary doors may be established with AO approval and as required by building code, safety and accessibility requirements,
      (1) Secondary doors shall:
         (a) Be equipped with a GSA-approved pedestrian door egress device with deadbolt meeting the most current version of Federal Specification FF-L-2890 for secondary door use. An AO-approved

alternate device with similar functionality may be authorized. Additional standalone and flush-mounted deadbolts are prohibited.

(b) Have approved access control hardware (see Chapter 8). The access control system must be deactivated when the SCIF is not occupied, or as determined by the AO.

(c) Include requirements in E.5 below.

4. Emergency Egress-only doors shall:
   a) Be installed as required by building code, safety and accessibility requirements.
   b) Be equipped with GSA-approved pedestrian door emergency egress device with deadbolt configuration meeting the most current version of Federal Specification FF-L-2890 for exit only door use. An AO-approved alternate device with similar functionality and no exterior hardware may be authorized. Additional standalone and flush-mounted deadbolts are prohibited.
   c) Be alarmed 24/7 and have a local audible annunciator that must be activated if the door is opened.
   d) Include requirements in E.5 below.

5. Criteria for **all** SCIF perimeter doors:

   a) All SCIF perimeter doors shall comply with applicable building code, safety, and accessibility requirements as determined by the Authority Having Jurisdiction.

   b) Ensure SCIF Standard Operating Procedures (SOP) includes procedures to ensure all doors are secured at end of day.

   c) All SCIF perimeter pedestrian doors shall be equipped with an automatic, non-hold door-closer which shall be installed internal to the SCIF.

   d) Door hinge pins that are accessible from outside of the SCIF shall be modified to prevent removal of the door, e.g., welded, set screws, dog bolts, etc.

   e) SCIF perimeter doors and frame assemblies shall meet acoustic requirements as described in Chapter 9 unless declared a non-discussion area.

   f) All SCIF perimeter doors shall be alarmed in accordance with Chapter 7.

   g) SCIF Perimeter doors shall meet TEMPEST requirements per CTTA guidance.

   h) When practical and permissible, SCIF entry doors should incorporate a vestibule to preclude visual observation and enhance door acoustic protection.

6. SCIF door fabrication and unique criteria:
   a) Wooden SCIF doors shall be 1 ¾ inch-thick solid wood core (i.e. wood stave, structural composite lumber).
   b) Steel doors shall meet following specifications:
      (1) 1 ¾ inch-thick face steel equal to minimum 18-gauge steel.
      (2) Hinges reinforced to 7-gauge steel and preferably a lift hinge.
      (3) Door closure installation reinforced to 12-gauge steel.

(4) Lock area predrilled and/or reinforced to 10-gauge steel.

c) Vault doors shall not be used to control day access to a facility. To mitigate both security and safety concerns, a vestibule with an access control device may be constructed for the purpose of day access to the vault door.

d) Roll-up Doors shall be minimum 18-gauge steel and shall be secured inside the SCIF using dead-bolts on both the right and left side of the door and alarmed in accordance with Chapter 7.

e) SCIF perimeter Double Door Specifications:

(1) The fixed leaf shall be secured at the top and bottom with deadbolts.

(2) An astragal shall be attached to one door.

(3) Each leaf of the door shall have an independent security alarm contact.

f) Adjacent SCIF adjoining doors:

(1) Doors that join adjacent SCIFs, not required for emergency egress, shall:

(a) Be dead bolted on both sides.

(b) Be alarmed on both sides according to chapter 7.

(c) Meet acoustic requirements as required.

(d) Be covered by AO SOP.

g) Other door types shall be addressed on an individual basis as approved by the AO.

F. SCIF Window Criteria

1. Every effort should be made to minimize or eliminate windows in the SCIF, especially on the ground floor.

2. Windows shall be non-opening.

3. Windows shall be protected by security alarms in accordance with Chapter 7 when they are within 18 feet of the ground or an accessible platform.

4. Windows shall provide visual and acoustic protection.

5. Windows shall be treated to provide RF protection when recommended by the CTTA.

6. All 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), shall be protected against forced entry and meet the standard for the perimeter.

G. SCIF Perimeter Penetrations Criteria

1. All penetrations of perimeter walls shall be kept to a minimum.

2. Metallic penetrations may require TEMPEST countermeasures, to include dielectric breaks or grounding, when recommended by the CTTA.

3. Utilities servicing areas other than the SCIF shall not transit the SCIF unless mitigated with AO approval. This restriction does not apply to secure communication

lines required to transit a SCIF to service an adjacent SCIF through a common perimeter surface.

4. Electrical Utilities should enter the SCIF at a single point.

5. All utility (power and signal) distribution on the interior of a perimeter wall treated for acoustics or RF shall be surface mounted, contained in a raceway, or an additional wall shall be constructed using furring strips as stand-off from the existing wall assembly. If the construction of an additional wall is used gypsum board may be inch-thick and need only go to the false ceiling.

6. Installation of additional conduit penetration for future utility expansion is permissible provided the expansion conduit is filled with acoustic fill and capped (end of pipe cover).

7. Vents and Ducts

a) All vents and ducts shall be protected to meet the acoustic requirements of the SCIF. (See Figure 4, Typical Air (Z) Duct Penetration, for example.)

b) Walls surrounding duct penetrations shall be finished to eliminate any opening between the duct and the wall.

c) All vents or duct openings that penetrate the perimeter walls of a SCIF and exceed 96 square inches shall be protected with permanently affixed bars or grills.

(1) If one dimension of the penetration measures less than six inches, bars or grills are not required.

(2) When metal sound baffles or wave forms are permanently installed and set no farther apart than six inches in one dimension, then bars or grills are not required.

(3) If bars are used, they shall be a minimum of ½ inch diameter steel, welded vertically and horizontally six inches on center; a deviation of ½ inch in vertical and/or horizontal spacing is permissible.

(4) If grilles are used they shall be of:

(a) ¾ inch-mesh, #9 (10 gauge), case-hardened, expanded metal; or

(b) expanded metal diamond mesh, 1-1/2” #10 (1-3/8” by 3” openings, 0.093” thickness, with at least 80% open design) tamperproof; or

(c) welded wire fabric (WWF) 4x4 W2.9xW2.9 (6 gauge smooth steel wire welded vertically and horizontally four inches o.c.).

(5) If bars, grilles, or metal baffles/wave forms are required, an access port shall be installed inside the secure perimeter of the SCIF to allow visual inspection of the bars, grilles, or metal baffles/wave forms. 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. This shall be noted in the FFC.

H. Alarm Response Time Criteria for SCIFs within the U.S.

Response times for Intrusion Detection Systems (IDS) shall meet 32 CFR Parts 2001 and 2004.

a) Closed Storage response time of 15 minutes.

b) Open Storage response time within 15 minutes of the alarm annunciation if the area is covered by SID or a five minute alarm response time if it is not.

I. Secure Working Areas (SWA)

SWAs are accredited facilities used for discussing, handling, and/or processing SCI, but where SCI will not be stored.

1. The SWA shall be controlled at all times by SCI-indoctrinated individuals or secured with a GSA-approved combination lock.

2. The SCIF shall be alarmed in accordance with Chapter 7 with an initial alarm response time of 15 minutes.

3. Access control shall be in accordance with Chapter 8.

4. Perimeter construction shall comply with section 3.C. above.

5. All SCI used in an SWA shall be removed and stored in GSA-approved security containers within a SCIF, a vault, or be destroyed when the SWA is unoccupied.

J. Temporary Secure Working Area (TSWA)

TSWAs are 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. Extension requests require a plan to accredit as a SCIF or SWA. Storage of SCI is not permitted within a TSWA.

1. When a TSWA is in use at the SCI level, access shall be limited to SCI- indoctrinated persons.

2. The AO may require an alarm system.

3. No special construction is required.

4. When the TSWA is approved for SCI discussions, sound attenuation specifications of Chapter 9 shall be met.

5. The AO may require a TSCM evaluation if the facility has not been continuously controlled at the SECRET level.

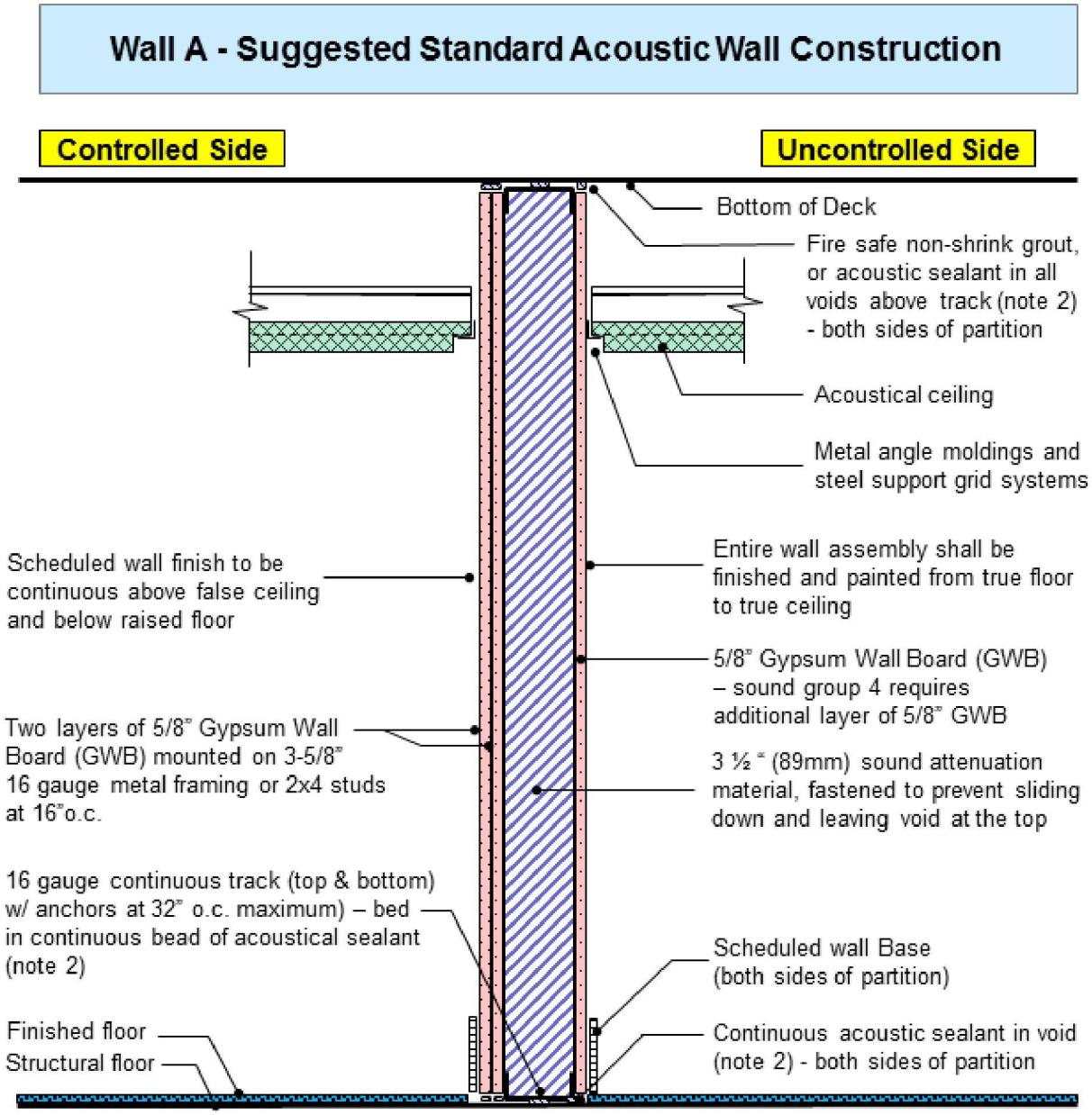
6. When the TSWA is not in use at the SCI level, the following shall apply:

   a) The TSWA shall be secured with a high-security, AO-approved key or combination lock.

   b) Access shall be limited to personnel possessing a minimum U.S. SECRET clearance.

Figure 1

Wall A – Suggested Standard Acoustic Wall Construction



Notes:

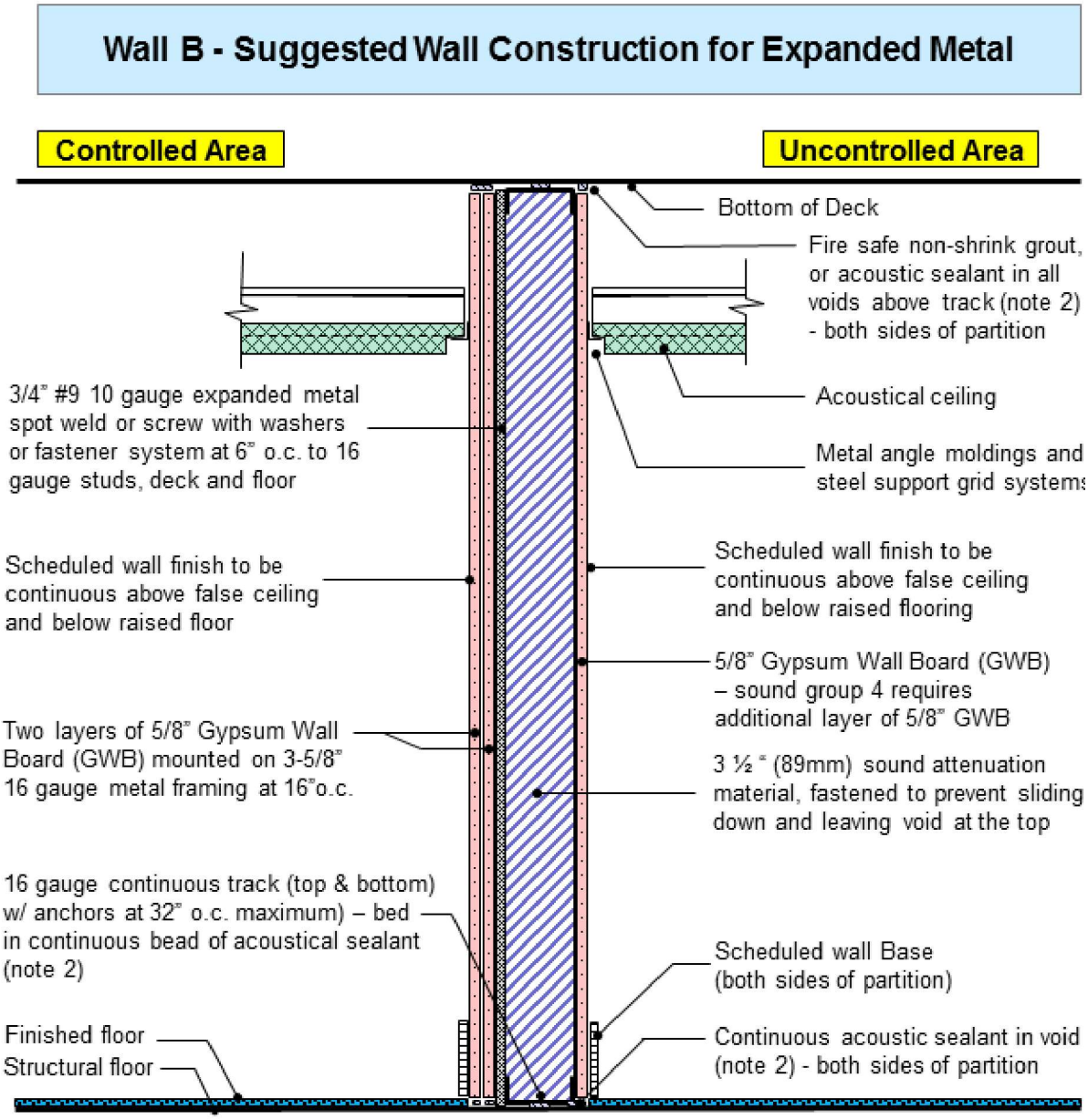
1 CTTA recommended countermeasures (foil backed GWB or layer of approved Ultra Radiant R-Foil) shall be installed IAW best practices for architectural Radio Frequency (RF) shielding. Foil shall be located between the two layers of GWB.

2 Partition shall be sealed continuously with acoustical sealant whenever it abuts another element (e.g., wall, column, mullion, etc.)

3 Any electrical or communications outlets required on the perimeter wall shall be surface mounted.

Figure 2

Wall B - Suggested Construction for Expanded Metal



Notes:

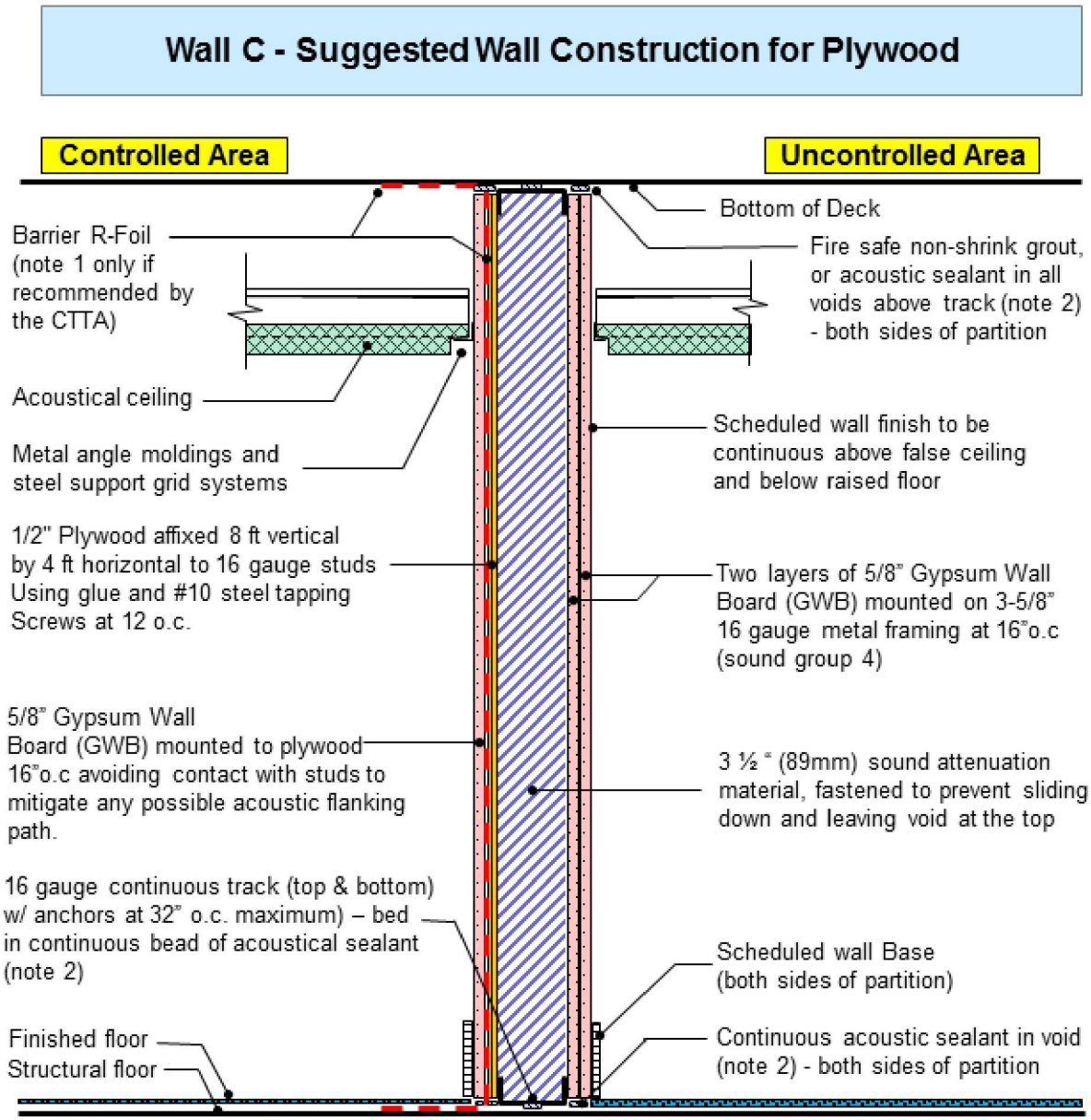
1 CTTA recommended countermeasures (foil backed GWB or layer of approved Ultra Radiant R-Foil) shall be installed IAW best practices for architectural Radio Frequency (RF) shielding. Foil shall be located between the two layers of GWB.

2 Partition shall be sealed continuously with acoustical sealant whenever it abuts another element (e.g., wall, column, mullion, etc.)

3 Any electrical or communications outlets required on the perimeter wall shall be surface mounted.

Figure 3

Wall C – Suggested Construction for Plywood



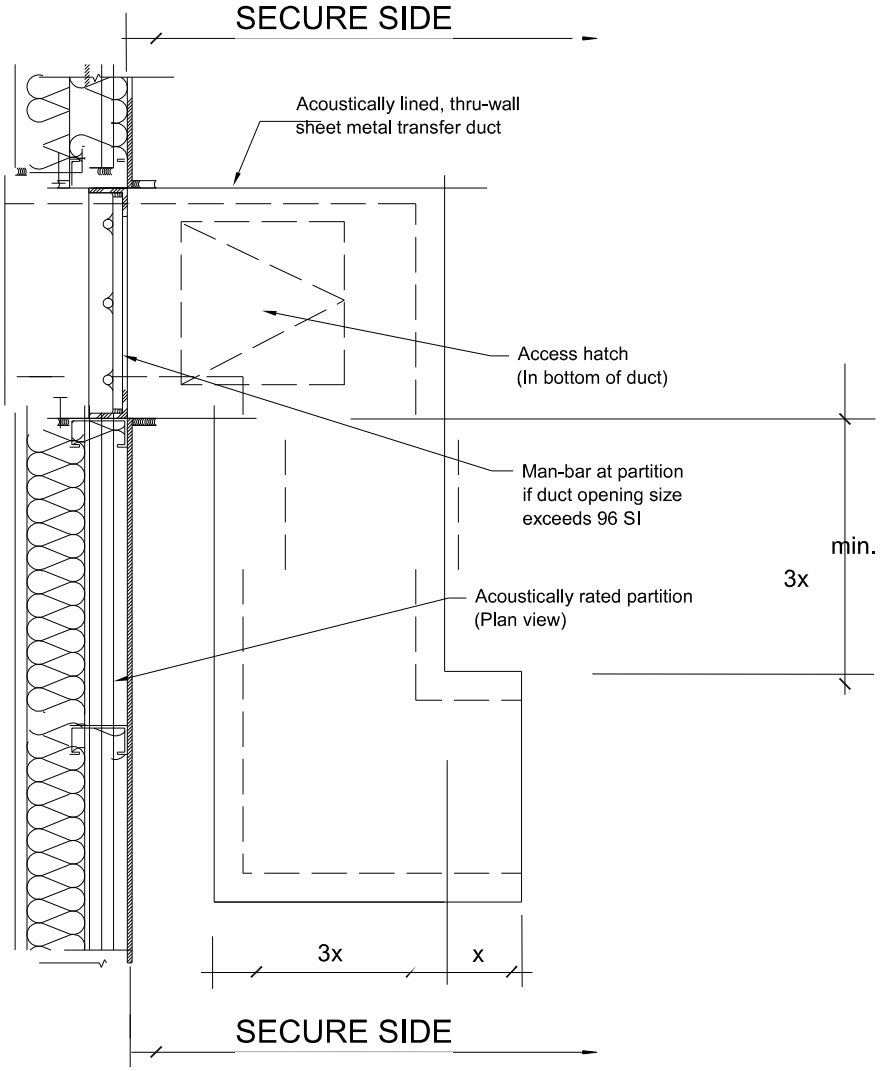
Notes:

1 CTTA recommended countermeasures (foil backed GWB or layer of approved Ultra Radiant R-Foil) shall be installed IAW best practices for architectural Radio Frequency (RF) shielding. Foil shall be located between the layer of plywood and GWB.

2 Partition shall be sealed continuously with acoustical sealant whenever it abuts another element (e.g., wall, column, mullion, etc.).

3 Any electrical or communications outlets required on the perimeter wall shall be surface mounted.

Figure 4
Typical Perimeter Air (Z) Duct Penetration



Rev. 04-05

This page intentionally left blank.

Chapter 4. SCIFs Outside the U.S. and NOT Under Chief of Mission (COM) Authority

A. General

1. Requirements outlined here apply only to SCIFs located outside of the U.S., its territories and possessions that are not under COM authority.

2. The application and effective use of SID may allow AOs to deviate from this guidance at Category II and III facilities.

B. Establishing Construction Criteria Using Threat Ratings

1. The Department of State's (DoS) Security Environment Threat List (SETL) shall be used in the selection of appropriate construction criteria based on technical threat rating.

2. If the SETL does not have threat information for the city of construction, the SETL threat rating for the closest city within a given country shall apply. When only the capital is noted, it will represent the threat for all SCIF construction within that country.

3. Based on technical threat ratings, building construction has been divided into the following three categories for construction purposes:

- Category I - Critical or High Technical Threat, High Vulnerability Buildings
- Category II - High Technical Threat, Low Vulnerability Buildings
- Category III - Low and Medium Technical Threat

4. Facilities in Category I Areas

a) Open Storage Facilities

(1) Open storage is to be avoided in Category I areas. The head of the IC element shall certify mission essential need and approve on case-by-case basis. When approved, open storage should only be allowed when the host facility is manned 24-hours-per-day by a cleared U.S. presence or the SCIF is continuously occupied by U.S. SCI-indoctrinated personnel.

(2) SCI shall be contained within approved vaults or Class M or greater modular vaults.

(3) The SCIF shall be alarmed in accordance with Chapter 7.

(4) Access control shall be in accordance with Chapter 8.

(5) An alert system and/or duress alarm is recommended.

(6) Initial alarm response time shall be five minutes.

b) Closed Storage Facilities

(1) The SCIF perimeter shall provide five minutes of forced-entry protection. (Refer to Wall B or Wall C construction methods.)

(2) The SCIF shall be alarmed in accordance with Chapter 7.

(3) Access control system shall be in accordance with Chapter 8.

(4) SCI shall be stored in GSA-approved containers or in an area that meets vault construction standards.

(5) Initial alarm response time shall be within 15 minutes.

c) Continuous Operation Facilities

(1) An alert system and duress alarm is required.

(2) The capability shall exist for storage of all SCI in GSA-approved security containers or vault.

(3) The emergency plan shall be tested semi-annually.

(4) Perimeter walls shall comply with enhanced wall construction methods in accordance Wall B or C standards.

(5) The SCIF shall be alarmed in accordance with Chapter 7.

(6) Access control shall be in accordance with Chapter 8.

(7) Initial response time shall be five minutes.

d) SWAs

Construction and use of SWAs is not authorized for facilities in Category I areas because of the significant risk to SCI.

e) TSWAs

Construction and use of TSWAs is not authorized for facilities in Category I areas because of the significant risk to SCI.

5. Facilities in Category II and III Areas

a) Open Storage Facilities

(1) Open storage is to be avoided in Category II areas. The head of the IC element shall certify mission essential need and approve on case-by-case basis. When approved, open storage should only be allowed when the host facility is manned 24-hours-per-day by a cleared U.S. presence or the SCIF is continuously occupied by U.S. SCI-indoctrinated personnel.

(2) In Category III areas, open storage should only be allowed when the host facility is manned 24-hours-per-day by a cleared U.S. presence or the SCIF is continuously occupied by U.S. SCI-indoctrinated personnel.

(3) The SCIF perimeter shall provide five minutes of forced-entry protection. (Refer to Wall B or Wall C construction methods.)

(4) The SCIF shall be alarmed in accordance with Chapter 7.

(5) Access control shall be in accordance with Chapter 8.

(6) An alert system and/or duress alarm is recommended.

(7) Initial alarm response time shall be five minutes.

b) Closed Storage Facilities

(1) The SCIF perimeter shall provide five minutes of forced-entry protection. (Refer to Wall B or Wall C construction methods.)

(2) The SCIF must be alarmed in accordance with Chapter 7.

(3) Access control system shall be in accordance with Chapter 8.

(4) SCI shall be stored in GSA-approved containers.

(5) Initial alarm response time shall be within 15 minutes.

c) Continuous Operation Facilities

(1) Wall A - Standard wall construction shall be utilized.

(2) The SCIF shall be alarmed in accordance with Chapter 7.

(3) Access control shall be in accordance with Chapter 8.

(4) Initial response time shall be five minutes.

(5) An alert system and/or duress alarm is recommended.

(6) The capability shall exist for storage of all SCI in GSA-approved security containers.

(7) The emergency plan shall be tested semi-annually.

d) SWAs

(1) Perimeter walls shall comply with standard Wall A construction.

(2) The SCIF shall be alarmed in accordance with Chapter 7.

(3) Access control shall be in accordance with Chapter 8.

(4) Initial alarm response time shall be within 15 minutes.

(5) The SWA shall be controlled at all times by SCI-indoctrinated individuals or secured with a GSA-approved combination lock.

(6) An alert system and/or duress alarm is recommended.

(7) All SCI used in an SWA shall be removed and stored in GSA-approved security containers within a SCIF or be destroyed.

(8) The emergency plan shall be tested semi-annually.

e) TSWAs

(1) No special construction is required.

(2) The AO may require an alarm system.

(3) When the TSWA is approved for SCI discussions, sound attenuation specifications of Chapter 9 shall be met.

(4) When a TSWA is in use at the SCI level, access shall be limited to SCI-indoctrinated persons.

(5) The AO may require a TSCM evaluation if the facility has not been continuously controlled at the SECRET level.

(6) When a TSWA is **not** in use at the SCI level, the following shall apply:

(a) The TSWA shall be secured with a high security, AO-approved key or combination lock.

(b) Access shall be limited to personnel possessing a U.S. SECRET clearance.

C. Personnel

1. SSM Responsibilities

a) Ensures the security integrity of the construction site (hereafter referred to as the "site").

b) Develops and implements a CSP.

c) Ensures that the SSM shall have 24-hour unrestricted access to the site (or alternatives shall be stated in CSP).

d) Conducts periodic security inspections for the duration of the project to ensure compliance with the CSP.

e) Documents security violations or deviations from the CSP and notifies the AO.

f) Maintains a list of all workers used on the project; this list shall become part of the facility accreditation files.

g) Implements procedures to deny unauthorized site access.

h) Works with the construction firm(s) to ensure security of the construction site and compliance with the requirements set forth in this document.

i) Notifies the AO if any construction requirements cannot be met.

2. CST Requirements and Responsibilities

a) Possesses U. S. TOP SECRET clearances.

b) Is specially trained in surveillance and the construction trade to deter technical penetrations and thwart implanted technical collection devices.

c) Supplements site access controls, implements screening and inspection procedures, and, when required by the CSP, monitors construction and personnel.

d) Is not required when U.S. TOP SECRET-cleared contractors are used

e) In Category III countries, must do the following:

(1) Shall begin surveillance of non-cleared workers at the start of SCIF construction or the installation of major utilities, whichever comes first.

(2) Upon completion of all work, shall clear and secure the areas for which they are responsible prior to turning control over to the cleared American guards (CAGs).

f) In Category I and II countries, must do the following:

(1) Shall begin surveillance of non-cleared workers at the start of construction of public access or administrative areas adjacent to the SCIF, SCIF construction, or the installation of major utilities, whichever comes first.

(2) Upon completion of all work, shall clear and secure the areas for which the CST is responsible prior to turning over control to the CAGs.

g) On U.S. military installations, when the AO considers the risk acceptable, alternative countermeasures may be substituted for the use of a CST as prescribed in the CSP.

3. CAG Requirements and Responsibilities

a) Possesses a U.S. SECRET clearance (TOP SECRET required under COM authority)

b) Performs access-control functions at all vehicle and pedestrian entrances to the site except as otherwise noted in the CSP.

(1) Screens all non-cleared workers, vehicles, and equipment entering or exiting the site.

(2) Denies introduction of prohibited materials, such as explosives, weapons, electronic devices, or other items as specified by the AO or designee.

(3) Conducts random inspections of site areas to ensure no prohibited materials have been brought on to the site. (All suspicious materials or incidents shall be brought to the attention of the SSM or CST.)

D. Construction Security Requirements

1. Prior to awarding a construction contract, a CSP for each project shall be developed by the SSM and approved by the AO.

2. Construction plans and all related documents shall be handled and protected in accordance with the CSP.

3. For SCIF renovation projects, barriers shall be installed to segregate construction workers from operational activities. These barriers will provide protection against unauthorized access and visual observation. Specific guidance shall be contained in the CSP.

4. When expanding existing SCIF space into areas not controlled at the SECRET level, maximum demolition of the new SCIF area is required.

5. For areas controlled at the SECRET level, or when performing renovations inside existing SCIF space, maximum demolition is not required.

6. All requirements for demolition shall be documented in the CSP.

7. Citizenship and Clearance Requirements for SCIF Construction Personnel

a) Use of workers from countries identified in the SETL as "critical technical threat level" or listed on the DoS Prohibited Countries Matrix is prohibited.

b) General construction of SCIFs shall be performed using U.S. citizens and U.S. firms.

c) SCIF finish work (work that includes closing up wall structures; installing, floating, taping and sealing wallboards; installing trim, chair rail, molding, and floorboards; painting; etc.) in Category III countries shall be accomplished by SECRET-cleared, U.S. personnel.

d) SCIF finish work (work that includes closing up wall structures; installing, floating, taping and sealing wallboards; installing trim, chair rail, molding, and floorboards; painting; etc.) in Category I and II countries shall be accomplished by TOP SECRET-cleared, U.S. personnel.

e) On military facilities, the AO may authorize foreign national citizens or firms to perform general construction of SCIFs. In this situation, the SSM shall prescribe, with AO approval, mitigating strategies to counter security and counterintelligence threats.

f) All non-cleared construction personnel shall provide the SSM with biographical data (full name, current address, Social Security Number (SSN), date and place of birth (DPOB), proof of citizenship, etc.), and fingerprint cards as allowed by local laws prior to the start of construction/renovation.

(1) Two forms of I-9 identification are required to verify U.S. persons.

(2) Whenever host nation agreements or Status of Forces Agreements make this information not available, it shall be addressed in the CSP.

g) When non-U.S. citizens are authorized by the AO:

(1) The SSM shall conduct checks of criminal and subversive files, local, national, and host country agency files, through liaison channels and consistent with host country laws.

(2) Checks shall be conducted of CIA indices through the country's Director of National Intelligence (DNI) representative and appropriate in-theater U.S. military authorities.

h) Access to sites shall be denied or withdrawn if adverse security, Counterintelligence (CI), or criminal activity is revealed. The SSM shall notify the AO when access to the site is denied or withdrawn.

i) For new facilities, the following apply:

(1) Non-cleared workers, monitored by CSTs, may perform the installation of major utilities and feeder lines.

(2) Installation shall be observed at perimeter entry points and when any trenches are being filled.

(3) The number of CSTs shall be determined by the size of the project (square footage and project scope) as outlined in the CSP.

j) For existing facilities, the following apply:

(1) Non-cleared workers, monitored by CSTs or cleared escorts, may perform maximum demolition and debris removal.

(2) TOP SECRET-cleared workers shall be used to renovate or construct SCIF space.

(3) SECRET-cleared individuals may perform the work when escorted by TOP SECRET-cleared personnel.

(4) SCI-indoctrinated escorts are not required when the existing SCIF has been sanitized or a barrier has been constructed to separate the operational areas from the areas identified for construction.

k) Prior to initial access to the site, all construction personnel shall receive a security briefing by the SSM or designee on the security procedures to be followed.

l) If a construction worker leaves the project under unusual circumstances, the SSM shall document the occurrence and notify the AO. The AO shall review for CI concerns.

m) The SSM may require cleared escorts or CSTs for non-cleared workers performing work exterior to the SCIF that may affect SCIF security.

n) The ratio of escort personnel to construction personnel shall be determined by the SSM on a case-by-case basis and documented in the CSP. Prior to assuming escort duties, all escorts shall receive a briefing regarding their responsibilities.

8. Access Control of Construction Sites

a) Access control to the construction site and the use of badges are required.

b) Guards are required for SCIF construction outside the U.S.

c) All site control measures used shall be documented in the CSP. The following are site control measures that should be considered:

- Identity verification.
- Random searches at site entry and exit points.
- Signs, in English and other appropriate languages, at all entry points listing prohibited and restricted items (e.g., cameras, firearms, explosives, drugs, etc.).
- Physical security barriers to deny unauthorized access.
- Vehicle inspections.

d) Guards

(1) Local guards, supervised by CAGs and using procedures established by the AO and documented in the CSP, may search all non-cleared personnel, bags, toolboxes, packages, etc., each time they enter or exit the site.

(2) In Category I countries, CAGs shall be assigned to protect the site and surrounding area as defined in the CSP.

(3) For existing SCIFs, TOP SECRET/SCI-indoctrinated guards are not required to control access to the site or secure storage area (SSA) provided that TOP SECRET/SCI-indoctrinated personnel are present on a 24-hour basis and prescribed post security resources are in place.

(4) Use of non-cleared U.S. guards or non-U.S. guards to control access to the site or SSA requires the prior approval of the AO. A SECRET-cleared, U.S. citizen must supervise any non-cleared or non-U.S. guards. Non-cleared or non-U.S. guards shall not have unescorted access to the site.

E. Procurement of Construction Materials

1. General Standards. These standards apply to construction materials (hereafter referred to as "materials") used in SCIF construction outside the U.S. These standards do not apply to installations on a roof contiguous to the SCIF provided there is no SCIF penetration.

a) Procurements shall be in accordance with Federal Acquisition Regulations.

b) In exceptional circumstances, SSMs may deviate from procurement standards with a waiver; such deviation shall be noted in the CSP.

c) For building construction projects in Category III countries, cleared U.S. citizens may randomly select up to 35% of building materials from non-specific general construction materials for SCIF construction. Random selection may exceed 35% only if materials can be individually inspected.

d) For building construction projects in Category I and II countries, cleared U.S. citizens may randomly select up to 25% of building materials from non-specific general construction materials for SCIF construction. Random selection may exceed 25% only if materials can be individually inspected.

e) Procurement of materials from host or third party countries identified in the SETL as critical for technical intelligence or listed in the DoS Prohibited Countries Matrix is prohibited.

f) All such materials must be selected immediately upon receipt of the shipment and transported to secure storage.

2. Inspectable (e.g., See Chapter 13 Inspectable Materials Checklist) Materials

a) Inspectable materials may be procured from U.S. suppliers without security restrictions.

b) The purchase of inspectable materials from host or third party countries requires advanced approval from the AO.

c) Procurement of materials from host or third party countries identified in the SETL as critical for technical intelligence or listed in the DoS Prohibited Countries Matrix is prohibited.

d) All inspectable materials procured in host and third party countries, or shipped to site in unsecured manner, shall be inspected using an AO-approved method as outlined in the CSP and then moved to an SSA.

e) Random selection of all inspectable material selected from stock stored outside of the SSA shall be inspected using AO-approved methods outlined in the CSP prior to use in SCIF construction.

3. Non-Inspectable Materials

a) Non-inspectable materials may be procured from U.S. suppliers or other AO-approved channels with subsequent secure transportation to the SSA at the construction site.

b) Non-inspectable materials may be procured in a host or third party country if randomly selected by U.S. citizens with a security clearance level approved by the AO.

c) Materials shall be randomly chosen from available suppliers (typically three or more) without advance notice to, or referral from, the selected supplier and without reference of the intended use of material in a SCIF.

d) Selections shall be made from available shelf stock and transported securely to an SSA.

e) Procurement officials should be circumspect about continually purchasing non-inspectable materials from the same local suppliers, and thereby establishing a pattern that could be reasonably discernible by hostile intelligence services, foreign national staff, and suppliers.

F. Secure Transportation for Construction Material

1. Inspectable Materials

a) Secure transportation of inspectable materials is not required, but materials shall be inspected using procedures approved by the AO prior to use.

b) Once inspected, all inspectable materials shall be stored in a SSA prior to use.

c) If securely procured, securely shipped, and stored in a secure environment, inspectable materials may be utilized within the SCIF without inspection.

2. Non-Inspectable Materials

a) Non-inspectable materials include inspectable materials when the site does not possess the capability to inspect them by AO-approved means.

b) Non-inspectable materials shall be securely procured and shipped to site by secure transportation from the U.S., a secure logistics facility, or low threat third party country using one of the following secure methods:

(1) Securely packaged or containerized and under the 24-hour control of an approved courier or escort office. (Escorted shipments shall be considered compromised if physical custody or direct visual observation is lost by the escort officer during transit. Non-inspectable materials that are confirmed or suspected of compromise shall not be used in a SCIF.)

(2) Securely shipped using approved transit security technical safeguards capable of detecting evidence of tampering or compromise. (An unescorted container protected by technical means ("trapped") is considered compromised if evidence of tampering of the protective technology is discovered, or if an unacceptable deviation from the approved transit security plan occurs. Non-inspectable materials that are confirmed or suspected of compromise shall not be used in a SCIF.).

(3) Non-inspectable materials shall be shipped using the following surface and air carriers in order of preference:

- U.S. Military
- U.S. Flag Carriers
- Foreign Flag Carriers

G. Secure Storage of Construction Material

1. A SSA shall be established and maintained for the secure storage of all SCIF construction material and equipment. An SSA is characterized by true floor to true ceiling, slab-to-slab construction of some substantial material, and a solid wood-core or steel-clad door equipped with an AO-approved security lock.

2. All inspected and securely shipped materials shall be placed in the SSA upon arrival and stored there until required for installation.

3. Alternative SSAs may include the following:

a) A shipping container located within a secure perimeter that is locked, alarmed, and monitored.

b) A room or outside location enclosed by a secure perimeter that is under direct observation by a SECRET-cleared U.S. citizen.

4. The SSA shall be under the control of CAGs or other U.S. personnel holding at least U.S. SECRET clearances.

5. Supplemental security requirements for SSAs shall be set forth in the CSP and may vary depending on the location and/or threat to the construction site.

H. Technical Security

1. TEMPEST countermeasures shall be pre-engineered into the construction of the SCIF.

2. In Category I countries, a TSCM inspection shall be required for new SCIF construction or for significant renovations (50% or more of SCIF replacement cost).

3. In Category II and III countries, a TSCM inspection may be required by the AO for new SCIF construction or significant renovations (50% or more of SCIF replacement cost).

4. A TSCM inspection shall be required if uncontrolled space is converted (maximum demolition) to new SCIF space.

5. When a TSCM inspection is not conducted, a mitigation strategy based on a physical security inspection that identifies preventative and corrective countermeasures shall be developed to address any technical security concerns.

I. Interim Accreditations

1. Upon completion of a successful inspection, the respective agency's AO may issue an Interim Accreditation pending receipt of required documentation.

2. If documentation is complete, AOs may issue an Interim Accreditation pending the final inspection.

This page intentionally left blank.

Chapter 5. SCIFs Outside the U.S. and Under Chief of Mission Authority

A. Applicability

1. This portion applies to the construction of SCIFs located overseas and that are on any compound that falls under the DoS COM authority or created to support any Tenant Agency that falls under COM authority.

2. The creation of new SCIF space at facilities that fall under COM authority is governed by both ICDs and Overseas Security Policy Board (OSPB) standards published as 12 Foreign Affairs Handbook-6 (12 FAH-6). If there is a conflict between the standards, the more stringent shall apply.

3. For SCIFs constructed in new facilities (new compound or new office building under COM authority), the proponent activity shall coordinate specific requirements for the proposed SCIF with the DoS/Overseas Buildings Operations (OBO).

4. For SCIFs constructed in existing facilities under COM authority, the project proponent activity must coordinate SCIF requirements with DoS/Bureau of Diplomatic Security (DS), the affected Embassy or Consulate (through the Regional Security Officer (RSO) and General Services Officer (GSO)), and DoS/OBO.

5. Upon an upgrade in the SETL Technical Threat rating for a facility under COM authority, the tenant agency in concert with the RSO, shall conduct a survey for OSPB compliance to the new technical threat requirements, and document any compliance issues accordingly. Upgrade requirements shall be coordinated through the RSO, GSO, and DoS/OBO and DS.

6. Temporary SCIFs may only be authorized by exception for facilities under COM authority. The AO of the tenant agency shall notify both the RSO and the DoS AO of the requirement and the expected duration of these facilities. Prior to accreditation, the tenant agency AO must coordinate with the DoS AO.

B. General Guidelines

1. SCIFs located under COM authority outside the U.S. are located within the CAA.

2. Prior to initiating any SCIF implementation process for upgrade or new construction in an existing office building, the tenant agency CSA shall do the following:

   a) Obtain concurrence from the Post‘s Counterintelligence Working Group (CIWG).

   b) Obtain written approval from the COM.

   c) Notify the DoS AO of CWIG and COM approvals.

   d) Coordinate OSPB preliminary survey with the post RSO/Engineering Services Office (ESO) if space is not core CAA.

3. A Preliminary Survey shall be developed by the RSO/ESO and submitted to DoS/DS for review and approval prior to awarding a construction contract. A CSP shall then be developed by the tenant and forwarded to DoS/OBO for processing.

4. All SCIF design, construction, or renovation shall be in compliance with OSPB standards for facilities under COM authority.

5. Any waivers that are granted for a SCIF by a waiver authority that would result in non-compliance with OSPB standards shall require an exception to OSPB standards from DoS/DS.

6. Written approval of the request for an exception to OSPB standards must be received prior to the commencement of any construction projects.

7. Upon completion of construction, the tenant agency AO will accredit the SCIF for SCI operations.

C. Threat Categories

1. The DoS SETL shall be used in the selection of appropriate construction criteria. Based on technical threat ratings, building construction has been divided into three categories for construction purposes:

- Category I - Critical or High Technical Threat, High Vulnerability Buildings
- Category II - High Technical Threat, Low Vulnerability Buildings
- Category III - Low and Medium Technical Threat

2. High and Low Vulnerability Buildings will be determined in accordance with the definitions in the OSPB standards.

3. SCIF design and construction shall comply with the building codes utilized by DoS/OBO.

4. SCIF construction projects are subject to the DoS Construction Security Certification requirements stipulated in Section 160 (a), Public Law 100-204, as amended. Construction activities may not commence until the required certification has been obtained from DoS.

5. SCIF construction projects are subject to permit requirements established by DoS/OBO.

6. Open storage in Category I and II areas is to be avoided. The CSA shall certify mission-essential need and approve on a case-by-case basis.

7. Open storage shall only be allowed for Category III posts when the host facility is manned 24-hours per day by a cleared U.S. presence (i.e., Marine Security Guard).

8. Open storage of SCI material is not authorized in lock-and-leave facilities (i.e., no Marine Security Guard).

D. Construction Requirements

1. Perimeter Wall Construction (all facilities regardless of type or location).

a) Perimeter walls shall comply with enhanced wall construction (See drawings for Walls B and C.)

b) Perimeter shall meet acoustic protection standards unless designated as a non-discussion area.

2. All SCIFs must be alarmed in accordance with Chapter 7.

3. Initial alarm response times shall be within 15 minutes for closed storage and five minutes for open storage.

4. Access control systems shall be in accordance with Chapter 8.

5. SCI shall be stored in GSA-approved containers.

6. An alert system and/or duress alarm is recommended.

7. Continuous Operation Facilities

a) An alert system and/or duress alarm is recommended.

b) The capability shall exist for storage of all SCI in GSA-approved security containers.

c) The emergency plan shall be tested semi-annually.

d) The SCIF shall be alarmed in accordance with Chapter 7.

e) Access control shall be in accordance with Chapter 8.

f) Initial response time shall be five minutes.

8. TSWAs

a) When a TSWA is in use at the SCI level, the following apply:

(1) Unescorted access shall be limited to SCI-indoctrinated persons.

(2) The AO may require an alarm system.

(3) No special construction is required.

(4) When the TSWA is approved for SCI discussions the following apply:

(a) Sound attenuation specifications of Chapter 9 shall be met.

(b) The AO may require a TSCM evaluation if the facility has not been continuously controlled at the SECRET level.

b) When the TSWA is **not** in use at the SCI level, the following shall apply:

(1) The TSWA shall be secured with a DoS/DS-approved key or combination lock.

(2) Unescorted access shall be limited to personnel possessing a U.S. SECRET clearance.

9. SWA

a) Initial alarm response times shall be within 15 minutes.

b) The SWA shall be controlled at all times by SCI-indoctrinated individuals or secured with a GSA-approved combination lock.

c) The SWA shall be alarmed in accordance with Chapter 7.

d) Access control shall be in accordance with Chapter 8.

e) Perimeter walls shall comply with standard Wall A.

f) An alert system and/or duress alarm is recommended.

g) All SCI used in a SWA shall be removed and stored in GSA-approved security containers within a SCIF or be destroyed.

h) There shall be an emergency plan that is tested semi-annually.

E. Personnel

1. SSM Requirements and Responsibilities

   a) Possesses a U.S. TOP SECRET clearance.

   b) Ensures the security integrity of the construction site.

   c) Develops and implements a CSP.

   d) Shall have 24-hour unrestricted access to the site (or alternatives shall be stated in CSP).

   e) Conducts periodic security inspections for the duration of the project to ensure compliance with the CSP.

   f) Documents security violations or deviations from the CSP and notifies the RSO and the tenant AO.

   g) Maintains a list of all workers utilized on the project; this list shall become part of the facility accreditation files.

   h) Implements procedures to deny unauthorized site access.

   i) Works with the construction firm(s) to ensure security of the construction site and compliance with the requirements set forth in this document.

   j) Notifies the RSO and tenant AO if any construction requirement cannot be met.

2. CST Requirements and Responsibilities

   a) Possesses a TOP SECRET clearance.

   b) Is specially trained in surveillance and the construction trade to deter technical penetrations and to detect implanted technical collection devices.

   c) Supplements site access controls, implements screening and inspection procedures, and when required by the CSP, monitors construction and personnel.

   d) Is not required when contractors who are U.S. citizens with U.S. TOP SECRET clearances are used.

e) In Category III countries the following shall apply:

(1) The CST shall begin surveillance of non-cleared workers at the start of SCIF construction.

(2) Upon completion of all work, the CST shall clear and secure the areas for which they are responsible prior to turning control over to the CAGs.

f) In Category I and II countries the following shall apply:

(1) The CST shall begin surveillance of non-cleared workers at the start of construction of public access or administrative areas adjacent to the SCIF, or SCIF construction, whichever comes first.

(2) Upon completion of all work, the CST shall clear and secure the areas for which the CST is responsible prior to turning over control to the CAGs.

3. CAG Requirements and Responsibilities

a) Possesses a U.S. TOP SECRET clearance.

b) Performs access control functions at all vehicle and pedestrian entrances to the site except as otherwise noted in the CSP.

(1) Screens all non-cleared workers, vehicles, and equipment entering or exiting the site.

(2) Uses walk-through and/or hand-held metal detectors or other means approved by the RSO or designee to deny introduction of prohibited materials such as explosives, weapons, electronic devices, or other items as specified by the RSO or designee.

(3) Conducts random inspections of site areas to ensure no prohibited materials have been brought on to the site. All suspicious materials or incidents shall be brought to the attention of the SSM.

c) In Category III countries, CAGs shall be assigned to protect the site and surrounding area at the start of construction of the SCIF or commencement of operations of the SSA.

d) In Category I and II countries, CAGs shall be assigned to protect the site and surrounding area at the start of construction of the SCIF, areas adjacent to the SCIF, or commencement of operations of the SSA.

e) For existing SCIFs, TOP SECRET/SCI-indoctrinated U.S. citizen guards are not required to control access to the site or SSA provided the following apply:

(1) TOP SECRET/SCI-indoctrinated U.S. citizens are present on a 24-hour basis in the SCIF or the SCIF can be properly secured and alarmed.

(2) Prescribed post security resources are in place to monitor the SSA.

F. Construction Security Requirements

1. Prior to awarding a construction contract, a CSP for each project shall be developed by the SSM and approved by DoS/DS and DoS/OBO and the tenant AO.

2. Construction plans and all related documents shall be handled and protected in accordance with the CSP.

3. For SCIF renovation projects, barriers shall be installed to segregate construction workers from operational activities. These barriers will provide protection against unauthorized access and visual observation. Specific guidance shall be contained in the CSP.

4. When expanding existing SCIF space into areas not controlled at the SECRET level, maximum demolition of the new SCIF area is required.

5. For areas controlled at the SECRET level that meet OSPB pre-conditions, or when performing renovations inside existing SCIF space, maximum demolition is not required.

6. All requirements for demolition shall be documented in the CSP.

7. Periodic security inspections shall be conducted by the SSM or designee for the duration of the project to ensure compliance with construction design and security standards.

8. Citizenship and Clearance Requirements for SCIF Construction Personnel

a) Use of workers from countries identified as critical for Technical or Human Intelligence threat, or listed on the DoS Prohibited Countries Matrix, is prohibited.

b) General construction and finish work is defined by OSPB standards.

c) General construction of SCIFs shall be performed using U.S. citizens and U.S. firms. Use of foreign national citizens or firms to perform general construction of SCIFs may be authorized in accordance with OSPB standards. In this situation, the CSP shall prescribe mitigating strategies to counter security and counterintelligence threats.

d) SCIF finish work shall be accomplished by appropriately cleared personnel as directed by OSPB standards for CAA construction.

e) All non-cleared construction personnel shall provide the SSM with biographical data (full name, current address, SSN, DPOB, proof of citizenship, etc.), and fingerprint cards as allowed by local laws prior to the start of construction/renovation.

f) Two forms of I-9 identification are required to verify U.S. persons.

g) Whenever host nation agreements make this information not available, it shall be addressed in the CSP.

h) When non-U.S. citizens are authorized, the following shall apply:

(1) The SSM shall conduct, through liaison channels, checks of criminal and subversive files, local and national; and host country agencies, consistent with host country laws.

(2) Checks shall also be conducted of CIA indices through the country's DNI representative and appropriate in-theater U.S. military authorities.

(3) Access to sites shall be denied or withdrawn if adverse security, CI, or criminal activity is revealed. The SSM shall notify the AO and RSO when access to the site is denied or withdrawn.

(4) For existing facilities, the following apply:

(a) Non-cleared workers monitored by CSTs may perform maximum demolition for conversion of non-CAA to SCIF. Debris removal by non-cleared workers must be monitored at a minimum by cleared U. S. citizen escorts.

(b) TOP SECRET-cleared U.S. citizens must perform maximum demolition within, or penetrating the perimeter of, an existing SCIF.

(c)TOP SECRET-cleared U.S. citizens shall be used to renovate SCIF space.

(d) SECRET-cleared individuals may perform the work when escorted by TOP SECRET-cleared U.S. citizens.

(e) SCI-indoctrinated escorts are not required when the existing SCIF has been sanitized or a barrier has been constructed to separate the operational areas from the areas identified for construction.

i) Prior to initial access to the site, all construction personnel shall receive a security briefing by the SSM or designee on the security procedures to be followed.

j) If a construction worker leaves the project under unusual circumstances, the SSM shall document the occurrence and notify the RSO and tenant AO. The RSO shall review for CI concerns.

k) The SSM may require cleared escorts or CSTs for non-cleared workers performing work exterior to the SCIF that may affect SCIF security.

l) The ratio of escort personnel to construction personnel shall be determined by the SSM on a case-by-case basis and documented in the CSP. Prior to assuming escort duties, all escorts shall receive a briefing regarding their responsibilities.

9. Access Control of Construction Sites

a) Access control to the construction site and the use of badges are required.

b) Guards are required for SCIF construction outside the U.S.

c) All site control measures used shall be documented in the CSP.

d) The following site control measures should be considered:

(1) Identity verification.

(2) Random searches at site entry and exit points.

(3) Signs, in English and other appropriate languages, at all entry points listing prohibited and restricted items (e.g., cameras, firearms, explosives, drugs, etc.).

(4) Physical security barriers to deny unauthorized access.

(5) Vehicle inspections.

10. Local Guards

a) Local guards, supervised by CAGs and using procedures established by the RSO and documented in the CSP, may search all non-cleared personnel, bags, toolboxes, packages, etc., each time they enter or exit the site.

b) Use of non-cleared U.S. guards or non-U.S. guards to control access to the site or secure storage area (SSA) requires the prior approval of the RSO. A SECRET-cleared U.S. citizen must supervise non-cleared or non-U.S. guards. Non-cleared or non-U.S. guards shall not have unescorted access to the site.

G. Procurement of Construction Materials

1. General Standards

a) These standards apply to construction materials used in SCIF construction under COM authority. These standards do not apply to installations on a roof contiguous to the SCIF provided there is no SCIF penetration.

b) Procurements shall be in accordance with Federal Acquisition Regulations.

c) In exceptional circumstances, SSMs may deviate from procurement standards with a waiver; such deviation shall be noted in the CSP.

d) For building construction projects in Category III countries, cleared U.S. citizens may randomly select up to 35% of building materials from non-specific general construction materials for SCIF construction. Random selection may exceed 35% only if materials can be individually inspected.

e) For building construction projects in Category I and II countries, cleared U.S. citizens may randomly select up to 25% of building materials from non-specific general construction materials for SCIF construction. Random selection may exceed 25% only if materials can be individually inspected.

f) All such materials must be selected immediately upon receipt of the shipment and transported to secure storage.

g) Procurement of materials from host or third party countries identified in the SETL as critical for technical intelligence, or listed on the DoS Prohibited Countries Matrix, is prohibited.

2. Inspectable Materials Specifically Destined for SCIF Construction

a) Inspectable materials specifically destined for SCIF construction may be procured from U.S. third-country or local suppliers without security restrictions.

b) All inspectable materials specifically destined for SCIF construction procured in host and third party countries or shipped to site in an unsecured manner from the U.S. shall be inspected using a DoS/DS-approved method and then moved to an SSA.

c) All inspectable material selected from stock stored outside of the SSA shall be inspected using DoS/DS-approved methods prior to use in SCIF construction.

3. Non-Inspectable Materials Specifically Destined for SCIF Construction

a) Non-inspectable materials specifically destined for SCIF construction shall be procured from U.S. suppliers with subsequent secure transportation to the SSA at the construction site.

b) On an exceptional basis, non-inspectable materials may be procured in a host or third party country if randomly selected by cleared U.S. citizens.

(1) Materials shall be randomly chosen from available suppliers (typically three or more) without advance notice to, or referral from, the selected supplier and with no reference of the intended use of material in a SCIF.

(2) Such selections shall be made from available shelf stock, brought immediately under personal control of a cleared U.S. citizen, and transported securely to an SSA.

(3) Procurement officials should be circumspect about continually purchasing non-inspectable materials from the same local suppliers and establishing a pattern that could be reasonably discernible by hostile intelligence services, foreign national staff, and suppliers.

H. Secure Transportation for Construction Material

1. Inspectable Materials Specifically Destined for SCIF Construction

a) Inspectable materials do not require secure transportation but shall be inspected using procedures approved by the DoS/DS prior to use in the SCIF.

b) Once inspected, all inspectable items shall be stored in an SSA.

c) Materials may be utilized within the SCIF without inspection if securely procured, securely shipped, and stored in a secure environment.

2. Non-inspectable Materials Specifically Destined for SCIF Construction

a) Non-inspectable material includes inspectable materials when the site does not possess the capability to inspect by Do/DS-approved means.

b) Non-inspectable materials shall be securely procured and shipped to site by secure transportation from the U.S., a secure logistics facility, or low threat third party country using one of the following secure methods:

(1) Securely packaged or containerized and under the 24-hour control of an approved courier or escort officer. (Escorted shipments shall be considered compromised if physical custody or direct visual observation is lost by the escort officer during transit. Non-inspectable materials that are confirmed compromised or suspected of compromise shall not be used in a SCIF.)

(2) Securely shipped using approved transit security technical safeguards capable of detecting evidence of tampering or compromise. (An unescorted container protected by technical means ("trapped") is considered compromised if evidence of tampering of the protective technology is discovered, or if an unacceptable deviation from the approved transit security plan occurs. Non-inspectable

materials that are confirmed compromised or suspected of compromise shall not be used in a SCIF.)

(3) Non-inspectable materials shall be shipped using the following surface and air carriers in order of preference:

(a) U.S. Military
(b) U.S. Flag Carriers
(c) Foreign Flag Carriers

I. Secure Storage of Construction Material

1. Upon arrival, all inspected and securely shipped materials shall be placed in the SSA until required for installation.

2. An SSA shall be established and maintained for the secure storage of all SCIF construction material and equipment. It is characterized by true floor to true ceiling, slab-to-slab construction of some substantial material and a solid wood-core or steel-clad door equipped with a DoS/DS-approved security lock.

3. Alternative SSA's may include a shipping container located within a secure perimeter that is locked, alarmed, and monitored, or a room or outside location enclosed by a secure perimeter that is under direct observation by a SECRET-cleared U.S. citizen.

4. The SSA shall be under the control of CAGs or other U.S. citizens holding at least U.S. SECRET clearances.

5. Supplemental security requirements for SSAs shall be set forth in the CSP and may vary depending on the location and/or threat to the construction site.

J. Technical Security

1. TEMPEST countermeasures shall be pre-engineered into the building.

2. A TSCM inspection shall be required in Category I countries for new SCIF construction or significant renovations (50% or more of SCIF replacement cost).

3. A TSCM inspection may be required by the AO in Category II or III countries for new SCIF construction or significant renovations (50% or more of SCIF replacement cost).

4. A TSCM inspection, conducted at the completion of construction, shall be required if uncontrolled space is converted (maximum demolition) to new SCIF space.

5. When a TSCM inspection is not conducted, a mitigation strategy based on a physical security inspection that identifies preventative and corrective countermeasures shall be developed to address any technical security concerns.

K. Interim Accreditations

1. Upon completion of a successful inspection, the respective agency's AO may issue an Interim Accreditation pending receipt of required documentation.

2. If documentation is complete, AOs may issue an Interim Accreditation pending the final inspection.

This page intentionally left blank.

Chapter 6. Temporary, Airborne, and Shipboard SCIFs

A. Applicability

1. General Information

a) This chapter covers all SCIFs designed to be temporary or such as those at sites for contingency operations, emergency operations, and tactical military operations. This chapter does not apply to temporary SCIFs established or operated within or on U.S. diplomatic facilities/compounds; see Chapter 5 for applicable guidance.

b) These standards apply to the following:

(1) All ground-based temporary SCIFs (T-SCIFs), including those on mobile platforms (e.g., trucks and trailers).

(2) SCIFs aboard aircraft.

(3) SCIFs aboard surface and sub-surface vessels.

c) When employing T-SCIFs, a risk management approach shall be used that balances the operational mission and the protection of SCI.

2. Accreditation

a) Accreditation for the use of T-SCIFs shall not exceed one year without mission justification and approval by the AO.

b) When the T-SCIF owner determines that a T-SCIF is no longer required, the withdrawal of accreditation shall be initiated by the SSO/Contractor Special Security Officer (CSSO).

(1) Upon notification, the AO will issue appropriate SCI withdrawal correspondence.

(2) The AO or appointed representative will conduct a close-out inspection of the facility to ensure that all SCI material has been removed.

B. Ground-Based T-SCIFs

1. T-SCIF Structures and Activation

a) Ground-based T-SCIFs may be established in hardened structures (e.g., buildings, bunkers) or semi-permanent structures (e.g., truck-mounted or towed military shelters, prefabricated buildings, tents).

b) Permanent-type hardened structures shall be used to the greatest extent possible for T-SCIFs.

c) Prior to T-SCIF activation, the AO may require submission of a standard fixed facility checklist or a T-SCIF checklist produced before or after a deployment.

2. SCI Storage and Destruction

a) Under field or combat conditions, open storage of SCI media and materials requires a continuous presence by SCI-indoctrinated personnel.

b) Under field or combat conditions every effort shall be made to obtain from any available host command necessary support for the storage and protection of SCI (e.g., security containers, generators, guards, weapons, etc.).

c) The quantity of SCI material within a T-SCIF shall be limited, to the extent possible, to an amount consistent with operational needs.

d) All SCI shall be stored in GSA-approved security containers.

e) The AO may approve exceptions to the storage of SCI material in GSA-approved storage containers for a specified period of time.

f) When no longer needed, SCI material shall be destroyed by means approved by the AO.

3. Security Requirements

a) T-SCIF security features shall provide acoustical, visual, and surreptitious entry protection.

b) A TSCM inspection shall be requested for any structure proposed for T-SCIF use if the space was previously occupied by a non-U.S. element. It is the AO's responsibility to evaluate operating the SCIF prior to TSCM inspection and formally assume all risk associated with early operation.

c) When possible, T-SCIFs shall be established within the perimeters of U.S.-controlled areas or compounds.

d) If a U.S.-controlled area or compound is not available, the T-SCIF shall be located within an area that affords the greatest degree of protection against surreptitious or forced entry.

e) When a T-SCIF is in operation, the perimeter of its immediate area shall be observed and protected by U.S. guards with U.S. SECRET clearances. Guards shall be equipped with emergency communication devices and, if necessary, with weapons.

f) During non-operational hours, the T-SCIF shall be provided security protection in accordance with AO guidelines.

g) The T-SCIF shall have only one entrance which shall be controlled during hours of operation by an SCI-indoctrinated person using an access roster.

h) Unclassified telecommunications equipment shall meet the requirements outlined in Chapter 10 to the greatest extent practical.

i) Telephones obtained in a foreign country shall not be used within a T-SCIF.

j) Cables and wires penetrating the T-SCIF perimeter shall be protected. The AO may require inspections and routing of cables and wiring through protective distribution systems or may require other countermeasures.

k) AO-approved emergency destruction and evacuation plans shall be developed and rehearsed periodically by all personnel assigned to the T-SCIF; the results of the rehearsal drills shall be documented.

l) When in transit, ground-based and mobile (e.g., truck-mounted, towed military shelters) T-SCIFs containing unsecured and non-encrypted SCI shall be accompanied by a U.S. TOP SECRET-cleared individual with SCI access approval(s).

m) During movement, T-SCIF structures shall be secured with GSA-approved locking devices and equipped with tamper-evident seals.

n) When in transit, hardened T-SCIFs having no open storage of SCI may be monitored by a U.S SECRET-cleared individual.

o) Hardened T-SCIFs shall be designed with TEMPEST countermeasures as identified by the CTTA. The AO, in collaboration with the CTTA, shall provide red/black separation and "protected distribution" guidance for field installation in accordance with CNSSAM TEMPEST 1/13 and CNSSI 7003.

p) When a T-SCIF is no longer required, the responsible SCI security official shall conduct a thorough facility inspection to ensure all SCI material has been removed.

C. Permanent and Tactical SCIFs Aboard Aircraft

1. The Aircraft Facility Checklist (see Forms & Plans) will be used for permanent SCIFs aboard aircraft.

2. The AO may determine that an Aircraft Facility Checklist may not be required for tactical SCIFs aboard aircraft if the following information is provided:

a) Name of aircraft (tail number)/airborne T-SCIF.

b) Major command/organization.

c) ID number of parent SCIF, if applicable.

d) Location T-SCIF deployed from and date of deployment.

e) Location T-SCIF deployed to and date of deployment.

f) SCI compartment(s) involved in T-SCIF operations.

g) Time period for T-SCIF operations.

h) Name of exercise or operation.

i) Points of contact (responsible officers).

j) Type of aircraft and area to be accredited as a T-SCIF.

k) Description of security measures for entire period of T-SCIF use (standard operating procedures).

l) Additional comments to add clarification.

3. Security Requirements for Aircraft when Operating in Support of Missions Involving SCI Material

a) SCIF location shall be identified by aircraft tail number.

b) Access to the aircraft interior shall be controlled at all times by SCI-indoctrinated personnel.

c) There are no unique physical security construction standards for SCIFs aboard aircraft.

d) Accreditation, such as that from the Defense Courier Service, is not required for aircraft used solely to transport SCI material between airfields.

e) When all personnel on an aircraft are not briefed on every SCI compartment aboard, procedural methods or physical barriers shall be employed to isolate compartments of the SCI.

f) When an aircraft T-SCIF is no longer required, the responsible SCI security official shall conduct an inspection of the aircraft to ensure all SCI material has been removed.

4. SCI Storage and Destruction

a) SCI materials shall be encrypted or secured in an AO-approved security container.

b) When no longer needed, SCI materials shall be destroyed by means approved by the AO.

c) Following an unscheduled landing in U.S.-controlled or non-hostile territory, the senior SCI-indoctrinated person shall retain control of the SCI material until approved storage arrangements can be effected through a local Special Security Officer or SCI-indoctrinated official.

d) Prior to an unscheduled landing in unfriendly or hostile territory, every reasonable effort shall be made to destroy unencrypted SCI material and communications security equipment in accordance with the emergency destruction plan.

e) If the aircraft is stationary, in the absence of SCI-indoctrinated personnel, all SCI information shall be encrypted or removed and stored in an alternative accredited SCIF or location approved by the AO.

f) Emergency destruction plans for SCI material shall be developed, approved by the AO, and rehearsed periodically by all personnel assigned to the aircraft; rehearsal results shall be documented.

5. Additional Security Requirements for Stationary Aircraft

a) The aircraft shall be parked within a controlled area that affords the greatest protection against surreptitious or forced entry.

b) In the absence of SCI-indoctrinated personnel, all SCI information shall be encrypted or removed and stored in an alternative accredited SCIF or location approved by the AO.

c) If the aircraft cannot be positioned within a U.S.-controlled area, the SCI is not encrypted, and removal of the SCI is not possible, then the following measures must be taken:

(1) SCI-indoctrinated personnel shall remain with the aircraft.

(2) A guard force that can control the perimeter of the aircraft shall be deployed, unless infeasible. The guards shall possess U.S. SECRET clearances and be armed and equipped with emergency communication devices.

d) If the aircraft is located within a U.S.-controlled area, the SCI is not encrypted, and removal of SCI is not possible then, the following measures shall be taken:

(1) The AO may mitigate the requirement for SCI-indoctrinated personnel provided the aircraft is equipped with, or stored within a structure equipped with, an intrusion detection system approved by the AO.

(2) All aircraft hatches and doors shall be secured with AO-approved locks and tamper-evident seals.

(3) A guard force must be available to respond to an alarm within five minutes.

(4) Guards shall possess U.S. SECRET clearances and be armed and equipped with emergency communication devices.

(5) If a cleared U.S. guard force is not available, the AO may approve other mitigation measures.

D. Permanent and Tactical SCIFs on Surface or Subsurface Vessels

1. Permanent shipboard SCIFs shall consist of any area aboard a vessel where SCI is processed, stored, or discussed.

2. The Shipboard Checklist (see Forms & Plans) will be used for permanent SCIFs. The AO may determine that this checklist may not be required providing the below information is available:

a) Name of vessel/hull number.

b) Major command/organization.

c) ID number of parent SCIF, if applicable.

d) Location SCIF deployed from and date of deployment.

e) Location SCIF deployed to and date of deployment.

f) SCI compartment(s) and sub-compartments involved in SCIF operations.

g) Name of exercise or operation.

h) Points of contact (responsible officers).

i) Description of security measures for entire period of SCIF use (standard operating procedures).

j) Additional comments to add clarification.

3. Security Requirements for Permanent SCIFs

a) The perimeter (walls, floors, and ceiling) shall be fabricated of structural bulkheads comprised of standard shipboard/submarine construction materials.

b) Elements of the perimeter shall be fully braced and welded or bonded in place.

c) Doors shall conform to the following requirements:

(1) Perimeter doors and emergency exit(s) shall be constructed of standard shipboard materials and shall be mounted in a frame, braced and welded or bonded in place in a manner commensurate with the structural characteristics of the bulkhead, deck, or overhead.

(2) The primary entry door shall be equipped with a GSA-approved combination lock and an access control device.

(3) If the door is in a bulkhead that is part of an airtight perimeter, the airtight integrity may be maintained by co-locating the door with the metal joiner door, or by adding a vestibule.

(4) Metal joiner doors shall be equipped with a combination lock that meets specification FF-L-2740A and with an access control device approved by the AO.

(5) Doors shall be constructed in a manner that will preclude unauthorized removal of hinge pins and anchor bolts, and obstruct access to lock-in bolts between the door and frame.

(6) Doorways or similar openings that allow visual access to the SCIF shall be screened or curtained.

d) No damage control fittings or cables shall be located within, or pass through, the SCIF. This does not apply to smoke dampers or other life-safety devices that are operated by personnel within the space during working hours.

e) Removable hatches and deck plates less than 10 square feet that are secured by exposed nuts and bolts (external to the SCIF) shall be secured with a high security padlock (unless their weight makes this unreasonable). Padlock keys shall be stored in a security container located within the SCIF.

f) Vents, ducts, and similar openings with a cross-sectional measurement greater than 96 inches shall be protected by a fixed barrier or security grill. (This requirement is not applicable to through-ducts that do not open into the SCIF.)

(1) Grills shall be fabricated of steel or aluminum grating or bars with a thickness equal to the perimeter barrier.

(2) If a grating is used, bridge center-to-center measurements will not exceed 1.5 inches by 4 inches.

(3) Bars shall be mounted in a grid pattern, six-inches on center.

(4) The grating or bars shall be welded into place.

g) Construction of the SCIF perimeter shall afford adequate sound attenuation. Air handling units and ducts may require baffles if SCIF discussions can be overhead in adjacent areas.

h) The SCIF shall be equipped with an AO-approved intrusion detection system (IDS) or other countermeasures if SCI-indoctrinated personnel cannot continuously occupy the area.

i) Passing scuttles and windows should not be installed between the SCIF and any other space on the ship. If installed, they shall be secured on the inside of the SCIF.

j) All SCI cryptographic and processing equipment shall be located within the SCIF.

k) Unclassified telecommunications shall meet the requirements outlined in Chapter 11, to the greatest extent practical.

l) Sound-powered telephones will not be permitted in the SCIF without additional mitigations determined by the AO. If a deviation is granted, sound-powered telephones located within the SCIF and connecting to locations outside the SCIF shall comply with the following:

(1) Telephone cables shall not break out to jack-boxes, switchboards, or telephone sets other than at designated stations. Cables shall not be shared with any circuit other than call or signal systems associated with the SCIF circuit.

(2) Telephone cables shall be equipped with a selector switch located at the controlling station and shall be capable of disconnecting all stations, selecting any one station, and disconnecting the remaining stations.

(3) Sound-powered telephones not equipped with a selector switch shall have a positive disconnect device attached to the telephone circuit.

(4) Within any SCIF, sound-powered telephones not used for passing SCI information shall have a warning sign prominently affixed indicating the restriction.

(5) A call or signal system shall be provided. Call signal station, type ID/D, shall provide an in-line disconnect to prevent a loudspeaker from functioning as a microphone.

m) The approval of the AO is required for unencrypted, internal, communication-announcing systems that pass through the SCIF perimeter.

n) Intercommunications-type announcing systems installed within an SCIF shall meet the following standards:

(1) The system shall operate only in the push-to-talk mode.

(2) Receive elements shall be equipped with a local buffer amplifier to prevent loudspeakers or earphones from functioning as microphones.

(3) Except as specified, radio transmission capability for plain radio-telephone (excluding secure voice) will not be connected.

(4) Cable conductors assigned to the transmission of plain language radio-telephone will be connected to ground at each end of the cable.

(5) A warning sign will be posted that indicates the system may not be used to pass SCI.

(6) Unencrypted internal communication systems that pass through the SCIF perimeter shall be in grounded ferrous conduit.

o) Commercial intercommunication equipment shall not be installed within a SCIF without prior AO approval.

p) Loudspeakers used on general announcing systems shall be equipped with a one-way buffer amplifier to protect against microphonic responses.

q) Pneumatic tube systems shall not be installed within the SCIF. The following safeguards apply to existing systems on older ships:

(1) Covers shall be locked at both ends with an AO-approved lock. Keys shall be stored within an approved security container within the SCIF.

(2) The system shall have the capability to maintain the pressure or vacuum and the capability to lock in the secure position at the initiating end.

(3) There shall be a direct voice communications link between both ends to confirm the transportation and receipt of passing cartridges.

(4) Cartridges passing SCI material shall have a distinctive color.

(5) Pneumatic tubes shall be visually inspectable along their entire length.

(6) The CTTA shall conduct a TEMPEST countermeasures inspection and shall recommend safeguards to limit compromising emanations. TEMPEST safeguards should be pre-engineered into platforms to the greatest extent possible.

4. General Requirements for T-SCIFs

a) SCIFs on sub-surface vessels shall be accredited as T-SCIFs.

b) T-SCIFs aboard a vessel include portable platforms or containers temporarily placed within ship space such as embarked Portable Shipboard Collection Vans.

c) T-SCIFs shall be occupied by an SCI-indoctrinated person at all times unless the facility is protected by a GSA-approved lock, an approved intrusion detection system, and a response capability or other countermeasures approved by the AO.

5. Security Requirements for T-SCIFs

a) Overall T-SCIF construction standards shall be the same as those used for permanent shipboard SCIFs.

b) Vents, ducts, and similar openings shall be constructed to the same standards as those used for a shipboard SCIF.

c) SCI materials shall be destroyed by means approved by the AO when no longer needed.

d) AO-approved emergency destruction plans shall be rehearsed periodically by all personnel assigned to the T-SCIF and the rehearsals documented.

e) Unclassified telecommunications shall meet the requirements for a shipboard SCIF, to the greatest extent practical.

f) When the T-SCIF is no longer required, the responsible SCI security official shall conduct a closing inspection of the T-SCIF to ensure all SCI material has been removed.

g) The CTTA shall conduct a TEMPEST countermeasures inspection and shall recommend safeguards to limit compromising emanations. TEMPEST safeguards should be pre-engineered into platforms to the greatest extent possible.

6. Additional Security Standards for Mobile Platforms or Containers

a) Construction of the perimeter must be of sufficient strength to reveal evidence of physical penetration (except for required antenna cables and power lines).

b) Doors must fit securely and be equipped with a locking device that can be locked from the inside and outside.

7. SCI Storage and Destruction

a) SCI material shall be stored in a GSA-approved security container that is welded or otherwise permanently secured to the structural deck.

b) When no longer needed, SCI materials shall be destroyed by means approved by the AO.

c) AO-approved emergency destruction and evacuation plans shall be developed and rehearsed periodically by all personnel assigned to the SCIF and the rehearsals shall be documented.

This page intentionally left blank.

Chapter 7. Intrusion Detection Systems (IDS)

A. Specifications and Implementation Requirements

1. General SCIF IDS Requirements

   a) SCIFs shall be protected by IDS when not occupied.

   b) 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. However, these adjacent areas do not need IDS protection if the AO determines that a facility's security programs consist of layered and complementary controls sufficient to deter and detect unauthorized entry and movement.

   c) Doors without access control systems and that are not under constant visual observation shall be continuously monitored by the IDS.

   d) If any component of the IDS is disrupted to the extent the system no longer provides essential monitoring service (e.g., loss of line security, inoperable Intrusion Detection Equipment (IDE), or loss of power), SCI-indoctrinated personnel shall physically occupy the SCIF until the system is returned to normal operation. As an alternative, the outside SCIF perimeter may be continuously monitored by a response or guard force.

   e) IDS failure shall be addressed in the SCIF emergency plan.

2. System Requirements

   a) IDS installation related components and monitoring stations shall comply with Underwriters Laboratories (UL) Standard for National Industrial Security Systems for the Protection of Classified Material, UL 2050.

   b) Installation shall comply with an Extent 3 installation as referenced in UL 2050.

   c) Systems developed and used exclusively by the USG do not require UL certification, but shall nonetheless comply with an Extent 3 installation as referenced in UL 2050.

   d) 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 consisting of UL 639 listed motion sensors and UL 634 listed High Security Switches (HSS) that meet UL Level II requirements and/or other AO-approved equivalent sensors. All new SCIF accreditations shall use UL Level II HSS. Existing UL Level I HSS are authorized until major IDS modifications/upgrades are made.

   e) IDE cabling that extends beyond the SCIF perimeter shall employ Encrypted Line Security or be installed in a closed and sealed metal conveyance defined as a pipe, tube or the like constructed of ferrous Electrical Metallic Tubing (EMT), ferrous pipe conduit or ferrous rigid sheet metal ducting. All joints and connections shall be permanently sealed completely around all surfaces (e.g. welding, epoxy, fusion, etc.). Set screw shall not be used. The seal shall provide a continuous bond between the

components of the conveyance. If a service or pull box must be utilized, it must be secured with a GSA approved combination padlock or AO approved key lock.

f) SCIFs that share common or contiguous perimeter and support the same IC Element, or have an established Co-Use-Agreement (CUA), may have the Premise Control Unit (PCU) programmed into multiple logical units or partitions, of the same PCU, that function as individual control units for the intrusion detection system installed in multiple areas or rooms operated independently of one another. All conditions of compliance that apply to a PCU and IDS apply equally to the partitions of the PCU. The PCU shall be independent of IDS safeguarding non-UL 2050 certified areas.

g) If a monitoring station is responsible for more than one IDS, there shall be an audible and visible annunciation for each IDS.

h) IDS's shall be separate from, and independent of, fire, smoke, radon, water, and other systems.

i) If the IDS incorporates an access control system (ACS), notifications from the ACS shall be subordinate in priority to IDS alarms.

j) System key variables and passwords shall be protected and restricted to U.S. SCI-indoctrinated personnel.

k) IDS technical drawings, installation instructions, specifications, etc., shall be restricted as determined by the AO and documented in the CSP.

l) Systems shall not include audio or video monitoring without the application of appropriate countermeasures and AO approval.

m) Monitoring systems containing auto-reset features shall have this feature disabled.

n) Alarm activations shall remain displayed locally until cleared by an authorized SCI-cleared individual.

o) The AO shall approve all system plans. Final system acceptance testing shall be included as part of the SCIF accreditation package.

p) False alarms shall not exceed one alarm per 30-day period per IDS partition. False alarms are any alarm signal transmitted in the absence of a confirmed intrusion that is caused by changes in the environment, equipment malfunction or electrical disturbances. If false alarms exceed this requirement, a technical evaluation of the system shall be conducted to determine the cause, repaired or resolved, and documented.

3. System Components

a) Sensors

(1) All system sensors shall be located within the SCIF, except as noted in 3.a.(2) below.

(2) With AO approval, sensors external to the SCIF perimeter may be installed in accordance with paragraph A.2.e.

(3) Failed sensors shall cause immediate and continuous alarm activation until the failure is investigated and corrected by procedures as documented in the SCIF SOP or Emergency Action Plan.

(4) Dual technology sensors are authorized when each technology transmits alarm conditions independent of the other technology.

(5) A sufficient number of motion detection sensors shall be installed to meet the requirements of paragraph A.2.d or shall be approved by the AO. However, for facilities outside the U.S. and in Category I and II countries, motion detection sensors above false ceilings or below false floors may be required by the AO.

(6) When the primary entrance door employs a delay to allow for changing the system mode of access, the delay shall not exceed 30 seconds.

(7) SCIF perimeter doors shall be protected by an HSS and a motion detection sensor.

(8) Emergency exit doors shall be alarmed and monitored 24 hours per day.

b) Premise Control Units (PCUs)

(1) PCUs shall be located within a SCIF and only SCIF personnel may initiate changes in access modes.

(2) Operation of the access/secure switch shall be restricted by using a device or procedure that validates authorized use.

(3) Cabling between all sensors and the PCU shall be dedicated to the system, be contained within the SCIF, and shall comply with national and local electric codes and 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.b.(10) below.

(4) Alarm status shall be continuously displayed with an alphanumeric display at the PCU and/or monitoring station.

(5) Every effort shall be made to design and install the alarm-monitoring panel in a location that prevents observation by unauthorized persons.

(6) The monitoring station or PCU shall identify and display activated sensors.

(7) Immediate and continuous alarm annunciations shall occur for the following conditions.

(a) Intrusion Detection
(b) Failed Sensor
(c) Tamper Detection
(d) Maintenance Mode (a maintenance message displayed in place of an alarm)
(e) IDE Sensor Points shunted or masked during maintenance mode

(8) A change in power status (AC or backup) shall be indicated locally and at the monitoring station.

(9) All system events shall be reset by authorized SCI-indoctrinated personnel after an inspection of the SCIF and a determination for the cause of the alarm. Any auto-alarm reset feature of the IDS shall be disabled.

(10) IDS transmission lines leaving the SCIF to the monitoring station, must meet National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) for certified encrypted lines. The FIPS standard employed must be noted on the UL 2050/CRZH Certificate or other certificate employed. 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. Alternative methods shall be approved by the AO and noted on the IDS Certificate

(11) The SCI cleared IDS Administrator(s) shall change maintenance and master profiles, PINs or passcodes from their default settings to a unique PIN or passcode.

c) Integrated IDS and Remote Terminal Access.

(1) US government LAN or WAN requires the AO's Chief Information Officer (CIO) to be consulted before connecting an IDS. The system hosting the IDS shall be issued Authority to Operate (ATO) by the agency CIO, following the FISMA Risk Management Framework as outlined in NIST SP 800-53.

(2) For IDS that have been integrated into a networked system (local area network (LAN) or wide area network (WAN)), the requirements below shall be met.

(a) IDS System software shall be installed on a host computing device that is logically and physically restricted to corporate/government security elements cleared to the SCI level. The host device shall be located in a Physically Protected Space, which is defined as a locked room with walls, floor and ceiling that are fixed in place forming a solid physical boundary to which only SCI-cleared personnel have access. If uncleared personnel or personnel with less than SCI indoctrination require access to this space, they shall be escorted by authorized SCI-cleared personnel. The door(s) shall use Commercial Grade 1 hardware fitted with high security key cylinder(s) in compliance with UL 437. This room will be protected by a UL Extent 3 burglar alarm system and access control unless manned 24 hours.

(b) All system components and equipment shall be isolated in a manner that may include, but are not limited to firewalls, Virtual Private Networks, Virtual Routing Tables, Application Level security mechanisms or similar enhancements, that are configured to allow secure and private data transfers only between the PCU, host computer, remote terminal and monitoring station.

(c) If any component of the IDS is remotely programmable, continuous network monitoring is required. Continuous network monitoring includes auditing and reporting of network intrusion detection and prevention systems used in A.3.c.2.b.

(d) A secondary communication path may be utilized to augment an existing data communication link to reduce investigations of data communication failures of less than five minute duration. The supervision provided by the secondary communication path shall be equivalent to that of the primary communication path. The secondary communications path may only be wireless if approved by the AO in consultation with the CTTA and/or the appropriate technical authority.

(e) A unique user ID and password is required for each individual granted access to the system host computing devices or remote terminal. Passwords shall be a minimum of twelve characters consisting of alpha, numeric, and special characters, and shall be changed every six months or utilize US Government Personal Identity Verification (PIV) Card or Common Access Card (CAC) with two factor certificate authentication.

(f) Individuals with IDS administrative access shall immediately notify the AO or designee of any unauthorized modifications.

(g) All transmissions of system information over the LAN/WAN shall be encrypted using National Institute of Standards and Technology (NIST) FIPS 140-2, VPN, or closed and sealed conveyance (see A.2.e). FIPS-197 (AES) may be used with AO approval.

(h) Remote System terminals shall:

- Utilize role based user permissions (e.g. Super User, SO, Guard) as approved by the AO. USG installations shall be in compliance with paragraph 7.A.3.c.1Prohibit Non SCI Cleared personnel from modifying the IDS or ACS.

- Require an independent user ID and password in addition to the host login requirements. Requirements for IDS Systems Software Passwords shall be: a unique user ID and password for each individual granted access to the remote terminal. Passwords shall be a minimum of twelve characters consisting of alpha, numeric, and special characters and shall be changed every six months or utilize US Government Personal Identity Verification (PIV) Card or Common Access Card (CAC) with two factor certificate authentication if supported by the application.

- Host systems shall log and monitor failed login attempts. All remote sessions shall be documented and accessible to AO upon request.
- All Host systems and PCUs shall be patched and maintained to implement current firmware and security updates. USG systems shall be in compliance with Information Assurance Vulnerability Alert (IAVA) guidance.

B. IDS Modes of Operation

1. General Information

   a) The system shall operate in either armed or disarmed mode.

   b) There shall be no remote capability for changing the mode of operation by non-SCI cleared personnel.

   c) Changing arm/disarm status of the system shall be limited to SCI-indoctrinated personnel.

2. Requirements for Disarmed Mode

   a) When in disarmed mode, normal authorized entry into the SCIF, in accordance with prescribed security procedures, shall not cause an alarm.

   b) A record shall be maintained that identifies the person responsible for disarming the system.

   c) Tamper circuits and emergency exit door circuits shall remain in the armed mode of operation.

   d) The PCU shall have the ability to allow alarm points to remain in armed status while other points are in disarmed status.

3. Requirements for Armed Mode

   a) The system shall be placed into armed mode when the last person departs the SCIF.

   b) A record shall be maintained identifying the person responsible for arming the system.

   c) Each failure to arm or disarm the system shall be reported to the responsible SCIF Security Manager. Records of these events shall be maintained for two years.

   d) When in the armed mode, any unauthorized entry into the SCIF shall cause an alarm to be immediately transmitted to the monitoring station.

4. Requirements for Maintenance and Zone Shunting/Masking Modes

   a) When maintenance is performed on a system, the monitoring station must be notified and logged. The initiation of system maintenance can only be performed by an SCI cleared IDS administrator or SCIF Security Officer (SO).

b) When an IDE point is shunted or masked for reasons other than maintenance, it shall be displayed as such at the monitoring station throughout the period the condition exists.

c) Any sensor that has been shunted shall be reactivated upon the next change in status from armed to disarmed.

d) All maintenance periods shall be archived in the system.

e) A Personal Identification Number (PIN) is required, for maintenance purposes, to be established and controlled by the SCI cleared IDS administrator or SCIF SO. Procedures shall be documented in the SCIF SOP.

f) Portable Electronic Devices (PEDs) are allowed attachment to system equipment either temporarily or permanently for the purposes of system maintenance, repair and reporting (See A.3.c). In addition, when utilizing a stand-alone device, the requirements below shall be met.

(1) Such devices shall be kept under control of SCI-cleared personnel.

(2) When not in use, the PED shall be maintained in a Physically Protected Space (see A.3.c.2.a).

(3) Mass storage devices containing SCIF alarm equipment details, configurations, or event data will be protected at an appropriate level approved by the AO.

g) After the initial installation, the capability for remote diagnostics, maintenance, or programming of IDE shall be accomplished only by SCI-cleared personnel and shall be logged or recorded.

5. Requirements for Electrical Power

a) In the event of primary power failure, the system shall automatically transfer to an emergency electrical power source without causing alarm activation.

b) Twenty-four hours of uninterruptible backup power is required and shall be provided by batteries, an uninterruptible power supply (UPS), generators, or any combination.

c) An audible or visual indicator at the PCU shall provide an indication of the primary or backup electrical power source in use.

d) Equipment at the monitoring station shall visibly and audibly indicate a failure in a power source or a change in power source. The individual system that failed or changed shall be indicated at the PCU or monitoring station as directed by the AO.

6. Monitoring Stations

a) Monitoring stations shall be government-managed or one of the following in accordance with UL 2050:

(1) AO-operated monitoring station.

(2) Government contractor monitoring station (formerly called a proprietary central station).

(3) National industrial monitoring station.

(4) Cleared commercial central station (see NISPOM, Chap. 5).

b) Monitoring station employees shall be eligible to hold a U.S. SECRET clearance.

c) Monitoring station operators shall be trained in system theory and operation to effectively interpret system incidents and take appropriate response action.

d) Records shall be maintained shall be maintained in accordance with Chapter 12 section L.

C. Operations and Maintenance of IDS

1. Alarm Response

a) Alarm activations shall be considered an unauthorized entry until resolved.

b) The response force shall take appropriate steps to safeguard the SCIF, as permitted by a written support agreement, until an SCI-indoctrinated individual arrives to take control of the situation.

c) An SCI indoctrinated individual must arrive in accordance with UL 2050 requirements (60 minutes) or the response time approved by the AO, after receipt of the alarm signal to conduct an internal inspection of the SCIF, attempt to determine the probable cause of the alarm activation, and reset the IDS prior to the departure of the response force.

2. System Maintenance

a) Maintenance and repair personnel shall be escorted if they are not TOP SECRET-cleared and indoctrinated for SCIF access.

b) Repairs shall be initiated by a service technician within 4 hours of the receipt of a trouble signal or a request for service.

c) The SCIF shall be continuously manned by SCI-indoctrinated personnel on a 24-hour basis until repairs are completed or alternate documented procedures approved by the AO are initiated.

d) The following apply to emergency-power battery maintenance:

(1) The battery manufacturer's periodic maintenance schedule and procedures shall be followed and documented in the system's maintenance logs and retained for two years. Batteries should be replaced per manufacture's recommendations or as environmental conditions dictate.

(2) If the communications path is via a network, the local uninterruptible power source for the network shall also be tested.

(3) If a generator is used to provide emergency power, the manufacturers recommended maintenance and testing procedures shall be followed.

e) Network Maintenance

(1) System administrators shall maintain configuration control, ensure the latest operating system security patches have been applied, and configure the operating system to provide a high level of security.

(2) Inside the U.S., network maintenance personnel within a SCIF shall be a U.S. person and be escorted by cleared SCIF individuals.

(3) Outside the U.S., network maintenance personnel shall be U.S. TOP SECRET-cleared or U.S. SECRET-cleared and escorted by SCIF personnel.

D. Installation and Testing of IDS

1. Personnel Requirements

a) Installation and testing within the U.S. shall be performed by U.S. companies using U.S. citizens.

b) Installation and testing outside of the U.S. shall be performed by personnel who are U.S. TOP SECRET-cleared or U.S. SECRET-cleared and escorted by SCIF personnel.

2. Installation Requirements

All system components and elements shall be installed in accordance with requirements of this document, UL 2050, and manufacturer's instructions and standards.

3. Testing

a) Acceptance testing shall be conducted on systems prior to operational use to provide assurance that they meet all requirements of this section prior to SCIF accreditation.

b) Semi-annual IDS testing shall be conducted to ensure continued performance.

c) Records of testing and test performance shall be maintained in accordance with documentation requirements.

d) Motion Detection Sensor Testing

(1) All motion detection sensors shall be tested to ensure activation of the sensor at a minimum of four consecutive steps at a rate of one step per second; that is, 30 inches ± 3 inches or 760 mm ± 80 mm per second. The four-step movement shall constitute a "trial."

(2) The test shall be conducted by taking a four-step trial, stopping for three to five seconds, and taking another four-step trial.

(3) Trials shall be repeated throughout the SCIF and from different directions.

(4) An alarm shall activate at least three out of every four consecutive trials made by moving progressively through the SCIF.

e) HSS Testing

All HSS devices shall be tested to ensure that an alarm signal activates before the non-hinged side of the door opens beyond the thickness of the door from the closed position, e.g., the sensor initiates before the door opens 1¾ inch for a 1¾ inch door.

f) Tamper Testing

(1) Each IDS equipment cover shall be individually removed or opened to ensure there is alarm activation at the PCU or monitoring station in both the secure and access modes.

(2) Tamper detection devices need only be tested when installed.

(3) The AO may require more frequent testing of tamper circuits.

This page intentionally left blank.

Chapter 8. Access Control Systems (ACS)

A. SCIF Access Control

1. Guidelines

a) SCIFs shall be controlled by SCI-indoctrinated personnel or by an AO- approved ACS to ensure access is restricted to authorized personnel.

b) Personnel access control shall be utilized at all SCIFs.

c) Visual recognition of persons entering the SCIF by an SCI-indoctrinated person at the entrance to a SCIF is the ideal access control.

d) Entrances where visitor control is conducted shall be under continuous visual observation unless the SCIF is properly secured.

e) When the SCIF is an entire building, access control shall occur at the building perimeter.

2. ACS Requirements if Continuous Visual Observation is Not Possible

a) An automated personnel ACS that verifies an individual's identity before the individual is permitted unescorted access shall be utilized when personal recognition and verification is not used. Automated verification shall employ **two** of the following three technologies:

(1) Identification (ID) badge or card used in conjunction with the access control device that validates the identity of the person to whom the card is issued. Compromised or lost access cards shall be reported immediately and updated in the system to reflect "no access."

(2) A personal identification number (PIN) that is entered into the keypad by each individual. The PIN shall consist of four or more random digits, with no known or logical association to the individual or which can be derived from the person or system generated. Compromised PINs shall be reported immediately to the facility Security Officer (SO) or SCIF SO and updated in the system to reflect "no access."

(3) Biometric personal identity verification using unique personal characteristics such as fingerprint, iris scan, palm print, etc.

b) The automated personnel ACS shall ensure that the probability of an unauthorized individual gaining access is no more than one in ten thousand while the probability of an authorized individual being rejected access is no more than one in one thousand. Manufacturers must certify in writing that their system meets these criteria.

B. ACS Administration

1. ACS administrators shall be SCI-indoctrinated.

2. Remote release buttons that by-pass the ACS shall be inside the SCIF and in a location that provides continuous visual observation of personnel entering the SCIF.

3. ACSs shall not be used to secure an unoccupied SCIF.

4. When not occupied, SCIFs shall be alarmed and in secure mode in accordance with Chapter 7 and secured with an approved GSA FF-L-2740A combination lock.

5. Authorized personnel who permit another individual to enter the SCIF shall verify the individual's authorized access.

6. SCIF access authorization shall be removed when the individual is transferred, terminated, or the access approval is suspended or revoked.

C. ACS Physical Protection

1. Card readers, keypads, communication interface devices, and other access control equipment located outside the SCIF shall be tamper-protected and be securely fastened to a wall or other fixed structure.

2. Electrical components, associated wiring, or mechanical links shall be accessible only from inside the SCIF.

3. 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 AES certified encrypted lines. If this communication technology is not feasible, transmission lines shall be installed as approved by the AO.

4. Equipment containing access-control software programs shall be located in the SCIF or a SECRET controlled area.

5. Electric door strikes installed in conjunction with a personnel ACS shall have a positive engagement and be approved under UL 1034 for burglar resistance.

D. ACS Recordkeeping

1. Records shall reflect the active assignment of ID badge/card, PIN, level of access, entries, and similar system-related information.

2. Records and information concerning encoded ID data, PINs, Authentication data, operating system software, or any other data associated with the personnel ACS shall be secured in an open-storage facility or, when unattended, secured in a GSA-approved container in a closed-storage facility. Access to such data shall be restricted to only SCI-indoctrinated personnel responsible for the access control system.

3. Records of personnel removed from the system shall be retained for two years from the date of removal.

4. Records of security incidents (violations/infractions) regarding ACS shall be retained by the SO for five years from the date of an incident or until investigations of system violations and incidents have been resolved.

E. Using Closed Circuit Television (CCTV) to Supplement ACS

1. CCTV may be used to supplement the monitoring of a SCIF entrance for remote control of the door from within the SCIF. The system shall present no technical security hazard.

2. The remote control device shall be within the interior of the SCIF.

3. The system shall provide a clear view of the SCIF entrance and shall be monitored/operated by SCI-indoctrinated personnel within the SCIF.

4. CCTV communication lines should be located within the SCIF. Communication lines that must run external to the SCIF shall be installed to prevent tampering as approved by the AO.

F. Non-Automated Access Control

1. Non-automated access control devices (mechanical, electric, or electromechanical) may be approved by the AO to control access to SCIFs where the number of personnel that require access is low and there is only one entrance.

2. Combinations shall consist of four (4) or more random digits.

3. The use of pass keys to bypass such devices should be avoided except when local fire/safety codes require them. Any pass keys for such devices must be strictly controlled by SCI-indoctrinated personnel.

4. Mechanical access control devices (e.g., UNICAN, Simplex) shall be installed to prevent manipulation or access to coding mechanisms from outside the door.

5. The following shall apply to electric or electromechanical access control devices:

   a) The control panel or keypad shall be installed in such a manner to preclude unauthorized observation of the combination or the actions of a combination change.

   b) The selection and setting of combinations shall be accomplished by the SO and shall be changed when compromised or deemed necessary by the SO.

   c) The control panel in which the combination and all associated cabling and wiring is set shall be located inside the SCIF and shall have sufficient physical security to deny unauthorized access to its mechanism.

This page intentionally left blank.

Chapter 9. Acoustic Protection

A. Overview

1. This establishes DNI guidelines to protect classified conversations from being inadvertently overheard outside a SCIF.

2. This is not intended to protect against deliberate technical interception of audio emanations.

B. Sound Group Ratings

The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC). To satisfy the normal security standards of SCIFs, the following transmission attenuation groups have been established:

- Sound Group 3 - STC 45 or better. Loud speech from within the SCIF can be faintly heard but not understood outside of the SCIF. Normal speech is unintelligible with the unaided human ear.
- Sound Group 4 - STC 50 or better. Very loud sounds within the SCIF, such as loud singing, brass music, or a radio at full volume, can be heard with the human ear faintly or not at all outside of the SCIF.

C. Acoustic Testing

1. Audio tests shall be conducted to verify standards are met. Tests may be instrumental or non-instrumental as approved by the AO. Test method used shall be detailed in the CSP.

2. Instrumental Acoustic Tests

a) Only those with training on audio testing techniques shall conduct instrumental acoustic tests

b) With all SCIF doors closed, all perimeter walls and openings (e.g., air returns, doors, windows, etc.) shall be tested along multiple points to ensure that either Sound Group 3 or 4 is met.

c) Audio test sources shall have a variable sound level output.

d) The output frequency range shall include normal speech.

e) Test speakers shall be placed six feet from the test wall and 4 feet off the floor.

f) Audio gain of the test source shall produce “loud or very loud speech” as defined by Sound Group 3 and 4 levels respectively.

g) As an alternative, instrumented testing may be performed to Noise Isolation Class (NIC) standards. Results shall comply with NIC 40 for Sound Group 3 and NIC 45 for Sound Group 4.

3. Non-Instrumental Acoustic Tests

All non-instrumental tests shall be approved by the AO.

D. Construction Guidance for Acoustic Protection

1. The SCIF perimeter shall be designed and constructed to meet Sound Group 3 or better standards. (See construction drawings for Wall A, B, or C.)

2. Areas that provide for amplified conversations, such as conference centers, video teleconference (VTC) rooms, or similar areas, shall be designed and constructed to meet Sound Group 4 standards. (See construction drawings for Wall A, B, or C.)

3. Utility (e.g., power, signal, telephone) distribution shall be surface mounted to a sound-treated wall and shall not completely penetrate the sound-engineered structure.

E. Sound Transmission Mitigations

1. Construction of walls as described in Chapter 3 (Wall types A, B and C) or with brick, concrete, or other substantive material and acoustically treating penetrations, walls and doors should provide the necessary acoustic protection for Sound group 3.

2. When Sound Group 3 or 4 cannot be met with normal construction, supplemental mitigations to protect classified discussions from being overheard by unauthorized persons may include but not be limited to the following:

a) Structural enhancements such as the use of high-density building materials (i.e., sound deadening materials) can be used to increase the resistance of the perimeter to vibration at audio frequencies.

b) Facility design can include a perimeter location or stand-off distance which prevents non-SCI-indoctrinated person(s) traversing beyond the point where SCI discussions become susceptible to interception. For example, use of a perimeter fence or protective zone between the SCIF perimeter walls and the closest "listening place" is permitted as an alternative to other sound protection measures.

c) Sound masking devices, in conjunction with an amplifier and speakers or transducers, can be used to generate and distribute vibrations or noise; noise sources may be noise generators, tapes, discs, or digital audio players.

d) Speakers/transducers must produce sound at a higher level than the voice conversations within the SCIF.

e) Speakers/transducers shall be placed close to, or mounted on, any paths that would allow audio to leave the area, including doors, windows, common perimeter walls, vents/ducts, and any other means by which voice can leave the SCIF.

f) Wires and transducers shall, to the greatest extent possible, be located within the perimeter of the SCIF.

g) The sound masking system shall be subject to inspection during TSCM evaluations.

h) If the AO determines risk to be low, a speaker may be installed outside the SCIF door if the following conditions are met:

- The cable exiting the SCIF shall be encased within rigid conduit.
- The sound masking system shall be subject to review during TSCM evaluations.

i) For common walls, the speakers/transducers shall be placed so the sound optimizes the acoustical protection.

j) For doors and windows, the speakers/transducers shall be placed close to the aperture of the window or door and the sound projected in a direction facing away from conversations.

k) Once the speakers or transducers are optimally placed, the system volume shall be set and fixed. The volume level for each speaker shall be determined by listening to conversations outside the SCIF or area to be protected, and the speaker volume adjusted until conversations are unintelligible from outside the SCIF.

l) Sound-source generators shall be permanently installed and not contain an AM/FM receiver and shall be located within the SCIF.

m) Any sound-source generator within the SCIF that is equipped with a capability to record ambient sound shall have that capability disabled.

n) Examples of government-owned or government-sponsored sound-source generators are given below:

- Audio amplifier with a standalone computer (no network connection).
- Audio amplifier with a cassette tape player, compact disc (CD) player, or digital audio player, or with a digital audio tape (DAT) playback unit.
- Integrated amplifier and playback unit incorporating any of the above music sources.
- A noise generator or shift noise source generator using either white or pink noise.

This page intentionally left blank.

Chapter 10. Portable Electronic Devices with Recording Capabilities and Embedded Technologies (PEDs/RCET)

A. Approved Use of PEDs/RCET in a SCIF

1. DNI Executive Correspondence, ES 2017-00043, Wireless Technology in the Intelligence Community, should be referred to in all cases dealing with Portable Electronic Devices with Wireless capabilities.

2. Heads of IC elements will institute and maintain mitigation programs (countermeasures) if they allow introduction of PEDs/RCETs with recording capabilities into SCIFs under their cognizance. Such decisions are not reciprocal or applicable to facilities under the cognizance of other heads of IC elements.

3. Medical devices. Approval for medical devices will comply with all applicable laws and oversight policies, including the Rehabilitation Act, and the latest IC medical device approval process. As a minimum, the medical device must be reviewed to determine any technical security issues introduced by the device. Based on the security/technical review, medical devices may be approved by the AO for introduction and use within a SCIF.

4. Recording capabilities and restricted technologies are technologies that introduce vulnerabilities to information and therefore impact SCIF security. These technologies include, but are not limited to, radio frequency transmitters, audio and video recorders, cameras, microphones, data storage devices, computing devices, memory sticks, thumb drives or flash memory and devices with USB connectivity.

5. Any approval for radio frequency transmitters shall require the AO and the Certified TEMPEST Technical Authority (CTTA) collaborate and approve (as required) the introduction and use of PEDs/RCETs into a SCIF where there is a valid mission related requirement.

6. The AO, and when appropriate, the information systems (ISs) authorizing official(s), shall collaborate and approve (as required) the introduction and use of PEDs/RCETs into a SCIF when there is a valid mission related requirement.

7. Outside the U.S., heads of intelligence elements may approve PED/RCET usage by waiver and include the following:

- Defined mission need for PED/RCET usage.
- Defined period of time.
- Statement of residual risk

8. Within the U.S., if the AO determines the risk from PEDs/RCET to SCI under their cognizance is acceptable, taking a PED/RCET into the SCIF may be allowed with the following restrictions:

a) A comprehensive risk assessment addressing each vulnerability, security concern and the component of risk must be completed.

b) Only PEDs/RCET with low risk may be allowed entry to a SCIF.

c) Mitigation shall be applied to PEDs/RCET evaluated to be high and medium risk to reduce the PED/RCET risk to low before the device may be allowed entry.

d) Assessments may result in an AO determination to prohibit specific PEDs/RCET.

B. Prohibitions

1. Personally-owned PEDs/RCETs are prohibited from processing SCI. Connecting personally-owned PEDs/RCETs to an unclassified IS inside SCIFs may only be done when wireless capability is physically disconnected and has the approval of the AO for the IS.

2. Personally-owned PEDs/RCETs are prohibited in SCIFs outside the U.S. If the AO determines that mission requirements dictate a need, government- or contractor-owned PEDs/RCETs may be permitted in a SCIF by specific exception or if the AO determines the risk is low.

3. If a PED/RCET is transported outside the U.S. and left unattended or physical control is lost, that device shall not be reintroduced into a SCIF.

C. PED/RCET Risk Levels

1. General Information

a) Levels of risk are based on the functionality of PEDs/RCET.

b) The AO and appropriate authorizing official for the IS (when a portable IS is involved) will determine risk level and mitigation requirements for devices not addressed.

2. Low-, Medium-, and High-risk PEDs/RCET.

a) Low-risk PEDs/RCET are devices without recording or transmission capabilities and may be allowed into a SCIF by AO without mitigation. Low-risk PEDs/RCET include, but are not limited to, the following:

- Electronic calculators, spell checkers, language translators, etc.
- Receive-only pagers.
- Audio and video playback devices with no storage capability.
- Radios (receive-only).
- Infrared (IR) devices that convey no intelligence data (e.g., text, audio, video, etc.), such as an IR mouse or remote control.

b) Medium-risk PEDs/RCET are devices with built-in features that enable recording or transmitting digital text, digital images/video, or audio data; however, these features can be physically disabled. Medium-risk PEDs/RCET may be allowed in a

SCIF by the AO with appropriate mitigations. Examples of medium-risk PEDs/RCET include, but are not limited to, the following:

- Voice-only cellular telephones.
- Portable ISs, such as personal digital assistants (PDAs), tablet personal computers, etc.
- Devices that may contain or be connected to communications modems
- Devices that have microphones or recording capabilities

c) High-risk PEDs/RCET are those devices with recording and/or transmitting capabilities that require more extensive or technically complex mitigation measures to reduce the inherent risk or those that cannot be sufficiently mitigated with current technology. The AO may approve entry and use of government- and contractor-owned PEDs/RCET for official business provided mitigation measures are in place that reduces the risk to low. Examples include, but are not limited to, the following:

- Electronic devices with RF transmitting (IEEE 802.11, Bluetooth, etc.).
- Photographic, video, and audio recording devices.
- Multi-function cellular telephones.

D. Risk Mitigation

1. Heads of IC elements shall establish risk mitigation programs if high- or medium-risk PEDs/RCET are allowed into SCIFs.

2. Risk mitigation programs shall contain the following elements:

a) Formal approval process for PEDs/RCET.

b) Initial and annual refresher training for those individuals with approval to bring PEDs/RCET into a SCIF.

c) Device mitigation compliance documents listing the specific PEDs/RCET, their permitted use, required mitigations, and residual risk after mitigation.

d) A user agreement that specifies the following:

(1) The USG or a designated representative may seize the PED/RCET for physical and forensic examination at the government's discretion.

(2) The USG and the designated representative are not responsible for any damage or loss to a device or information stored on personally-owned PEDs/RCET resulting from physical or forensic examination.

3. Risk mitigation programs may include the following elements:

a) Registration of PED/RCET serial numbers.

b) PED/RCET security training program.

c) Reporting procedures for loss or suspected tampering.

d) Labeling approved PEDs/RCET for easy identification.

e) Electronic detection equipment to detect transmitters/cell phones.

Chapter 11. Telecommunications Systems

A. Applicability

1. This guidance is compatible with, but may not satisfy, security requirements of other disciplines such as Information Systems Security, Communications Security (COMSEC), Operational Security (OPSEC), or TEMPEST.

2. This section outlines the security requirements that shall be met to ensure the following:

- Protection of information.
- Configuration of unclassified telecommunications systems, devices, features, and software.
- Access control.
- Control of the cable infrastructure.

B. Unclassified Telephone Systems

1. A baseline configuration of all unclassified telephone systems, devices, features, and software shall be established, documented, and included in the SCIF FFC.

2. The AO shall review the telephone system baseline configuration and supporting information to determine if the risk of information loss or exploitation has been suitably mitigated.

3. When security requirements cannot be met, unclassified telephone equipment shall be installed and maintained in non-discussion areas only.

4. When not in use, unclassified telephone systems shall not transmit audio and shall be configured to prevent external control or activation, technical exploitation, or penetration.

5. Unclassified telephone systems shall incorporate physical and software access controls to prevent disclosure or manipulation of system programming and data. The following specific requirements shall be met:

a) On-hook and off-hook audio protection shall be provided by equipment identified by the National Telephone Security Working Group within TSG-6/CNSSI 5006, National Instruction for Approved Telephone Equipment, or an equivalent TSG 2/ CNSSI 5002:

(1) The purpose of a TSG-2 or CNSS 5002 Computerized Telephone Switch (CTS) installation is to prevent manipulation of telephone instruments to obtain audio from within the SCIF while the instrument is in an "on-hook" condition.

(2) When isolation is provided by a CTS installed IAW TSG-2 or CNSS 5002, the AO accepts the risk on-hook audio from the SCIF may be present on all instrument wiring until it reaches the CTS due to instrument configuration, design, or breakdown. *(TSG-2/CNSS 5002 does not address procedures to determine security of the station itself.)*

(3) To provide the necessary level of security, the Physically Protected Space (PPS) where the CTS is installed must meet equivalent security and access control standards as the SCIF it supports to provide positive physical protection for the CTS and all of its parts. *(CNSSI 5002 para 7.A.(1))*. This includes all instruments, cables, lines, intermediate wiring frames, and distributed CTS modules necessary for the functioning of the instruments.

(4) The AO may require all instrument wiring exiting between the SCIF and PPS which is not at the SCIF level be contained in a closed and sealed metal conveyance as defined in Chapter 7.A.2 to ensure physical security of the instrument wiring.

(5) Telephones or instruments not type-accepted will be presumed to have on-hook audio available at the mounting cord until determined otherwise. Determining telephone stations do not have on-hook audio hazards requires a technical investigation and specific equipment. These investigations and determinations may only be conducted by a TSCM team or National Telephone Security Working Group (NTSWG) authorized telephone laboratory.

b) If a Computerized Telephone System (CTS) is selected for isolation, it shall be installed and configured as detailed in TSG 2 with software and hardware configuration control and audit reporting (such as station message detail reporting, call detail reporting, etc.).

c) System programming shall not include the ability to place, or keep, a handset off-hook.

d) Configuration of the system shall ensure that all on-hook and off-hook vulnerabilities are mitigated.

e) When local or remote CTS administration terminals are not contained within a controlled area and safeguarded against unauthorized manipulation, the use of CNSSI 5006 approved telephone instruments shall be required, regardless of the CTS configuration.

f) Speakerphones and audio conferencing systems shall not be used on unclassified telephone systems in SCIFs. Exceptions to this requirement may be approved by the AO when these systems have sufficient audio isolation from other classified discussion areas in the SCIF and procedures are established to prevent inadvertent transmission outside the SCIF.

g) Features used for voice mail or unified messaging services shall be configured to prevent access to remote diagnostic ports, internal dial tone, and dial plans.

h) Telephone answering devices and facsimile machines shall not contain features that introduce security vulnerabilities, e.g., remote room monitoring, remote programming, or other similar features that may permit off-premise access to room audio.

i) All unclassified telephone systems and associated infrastructure shall be physically isolated from classified information and telecommunications systems in accordance with DNI and CNSS TEMPEST guidance.

j) TSG6/CNSSI 5006 approved instruments or compliance with CNSSI 5000 is required for installation in SCIFs for Voice over Internet Protocol (VoIP) systems installed in a SCIF. TSG6/CNSSI 5006 approved instruments must be installed following the manufacturer's requirements. For non-TSG6/CNSSI 5006 approved instruments, the security requirements and installation guidelines contained in the National Telecommunications Security Working Group (NTSWG) publication CNSSI 5000 shall be followed for Voice over Internet Protocol (VoIP) systems installed in a SCIF.

C. Unclassified Information Systems

1. Unclassified information systems shall be safeguarded to prevent hardware or software manipulation that could result in the compromise of data.

2. Information systems equipment with telephonic or audio features shall be protected against remote activation and/or removal of audio (analog or digitized) information.

3. Video cameras used for unclassified video teleconferencing and video recording equipment shall be deactivated and disconnected when not in use.

4. Video devices shall feature a clearly visible indicator to alert SCIF personnel when recording or transmitting.

D. Using Closed Circuit Television (CCTV) to Monitor the SCIF Entry Point(s)

1. CCTV may be used to supplement the monitoring of a SCIF entrance and to record events for investigation.

2. The system shall present no technical security hazard to the SCIF.

3. The system and all components, including communications and control lines, shall be exterior to the SCIF perimeter.

4. The system may provide a clear view of the SCIF entrance but not enable the viewer to observe classified information when the door is open nor external control pads or access control components that would enable them to identify PINs.

E. Unclassified Wireless Network Technology

1. The use of devices or systems utilizing wireless technologies pose a high risk and require approval from the AO, CTTA, and IT systems approving authority prior to introduction into the SCIF.

2. Wireless systems shall meet all TEMPEST and TSCM requirements and shall be weighed against the facilities overall security posture (i.e., facility location, threat, as well as any compensatory countermeasures that create SID) when evaluating these systems.

3. All separation and isolation standards provided in TEMPEST standards are applicable to unclassified wireless systems installed or used in SCIFs.

F. Environmental Infrastructure Systems

1. The FFC shall include information on whether or not environmental infrastructure systems (also referred to as building maintenance systems) are located in the SCIF. Examples include the following:

- Premise management systems
- Environmental control systems
- Lighting and power control units
- Uninterrupted power sources

2. The FFC shall identify all external connections for infrastructure systems that service the SCIF. Examples of the purpose of external connections include the following:

- Remote monitoring
- Access and external control of features and services
- Protection measures taken to prevent malicious activity, intrusion, and exploitation.

G. Emergency Notification Systems

1. The introduction of electronic systems that have components outside the SCIF perimeter is prohibited, with the following exceptions:

a) The system is approved by the AO.

b) The system is required for security purposes.

c) The system is required under life safety regulations.

2. If required, and speakers or other transducers are part of a system that is not wholly contained in the SCIF but are installed in the SCIF for life safety or fire regulations, the system must be protected as follows:

a) All incoming wiring shall breach the SCIF perimeter at one point. TEMPEST or TSCM concerns may require electronic isolation and shall require review and approval by the CTTA.

b) One-way (audio into the SCIF) communication systems shall have a high gain amplifier.

c) Two-way communication systems shall only be approved when absolutely necessary to meet safety/security requirements. They shall be protected so that audio cannot leave the SCIF without the SCIF occupants being alerted when the system is activated.

d) All electronic isolation components shall be installed within the SCIF and as close to the point of SCIF penetration as possible.

H. Systems Access

1. Installation and maintenance of unclassified systems and devices supporting SCIF operations may require physical or remote access. The requirements outlined in this section shall apply to telecommunications devices located within the SCIF or in a controlled area outside the SCIF.

2. Installation and maintenance personnel requiring physical access shall possess the appropriate clearance and access, or will be escorted and monitored at all times within the SCIF by technically knowledgeable, U.S. SCI-indoctrinated personnel.

3. Remote maintenance shall be protected against manipulation or activation.

4. All capabilities for remote maintenance and diagnostic services shall be specified in the FFC.

5. The FFC shall identify all procedures and countermeasures to prevent unauthorized system access, unauthorized system modification, or introduction of unauthorized software.

6. Remote maintenance and diagnosis may be performed from a SCIF or an adjacent controlled area over a protected link in accordance with FIPS AES standards.

7. Telephone systems only may be accessed over an unclassified telephone line as specified in TSG 2 Standard, Section 4.c.

I. Unclassified Cable Control

1. To the extent possible, all telecommunications cabling shall enter the SCIF through a single opening and allow for visual inspection.

2. Cable, either fiber or metallic, shall be accounted for from the point of entry into the SCIF.

   a) The accountability shall identify the precise use of every cable through labeling.

   b) Log entries may also be used.

   c) Designated spare conductors shall be identified, labeled, and bundled together.

3. Unused conductors shall be removed. If removal is not feasible, the metallic conductors shall be stripped, bound together, and grounded at the point of ingress/egress.

4. Unused fiber shall be uncoupled from the interface within the SCIF, capped, and labeled as unused fiber.

J. Protected Distribution Systems

1. Unencrypted communication cables transmitting SCI between accredited SCIFs shall be installed in a Protective Distribution System that complies with standards established in CNSSI 7003, Protected Distribution System.

2. PDS used to protect SCI shall be approved by the CSA AO.

K. References

1. Overview

   a) The NTSWG publishes guidance for the protection of sensitive information and unclassified telecommunications information processing systems and equipment.

   b) NTSWG documents are currently in transition from TSG/NTSWG documents to Committee on National Security Systems (CNSS) publications.

   c) The List of References is provided for use by personnel concerned with telecommunications security.

2. List of References

   a) TSG Standard 1 (Introduction to Telephone Security). Provides telephone security background and approved options for telephone installations in USG sensitive discussion areas.

   b) TSG Standard 2 (TSG Guidelines for Computerized Telephone Systems) and Annexes. Establishes requirements for planning, installing, maintaining, and managing CTS, and provides guidance for personnel involved in writing contracts, inspecting, and providing system administration of CTS.

   c) TSG Standards 3, 4, 5, and CNSSI 5001. Contains design specifications for telecommunication manufacturers and are not necessarily applicable to facility security personnel.

   d) CNSSI 5000. Establishes requirements for planning, installing, maintaining, and managing VoIP systems.

   e) CNSSI 5006. Lists approved equipment which inherently provide on-hook security.

   f) NTSWG Information Series (Computerized Telephone Systems). A Review of Deficiencies, Threats, and Risks, December 1994). Describes deficiencies, threats, and risks associated with using computerized telephone systems.

   g) NTSWG Information Series (Executive Overview, October 1996). Provides the salient points of the TSG standards and presents them in a non-technical format.

   h) NTSWG Information Series (Central Office (CO) Interfaces, November 1997). Provides an understanding of the types of services delivered by the local central office and describes how they are connected to administrative telecommunications systems and devices.

i) NTSWG/NRO Information Series (Everything You Always Wanted to Know about Telephone Security…but were afraid to ask, 2nd Edition, December 1998). Distills the essence of the TSG standards (which contain sound telecommunications practices) and presents them in a readable, non-technical manner.

j) NTSWG/NRO Information Series (Infrastructure Surety Program…securing the last mile, April 1999). Provides an understanding of office automation and infrastructure system protection that contributes to SCIF operation.

k) NTSWG Information Series (Computerized Telephone Systems Security Plan Manual, May 1999). Assists to implement and maintain the "secure" operation of CTSs as used to support SCIF operations. (The term "secure" relates to the safe and risk-free operation, not the use of encryption or a transmission security device.)

l) Director of National Intelligence, Intelligence Community Directive 702, Technical Surveillance Countermeasures.

m) Director of National Intelligence, Intelligence Community Directive 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.

n) SPB Issuance 00-2 (18 January 2000). Infrastructure Surety Program and the Management Assessment Tool.

This page intentionally left blank.

Chapter 12. Management and Operations

A. Purpose

To establish safeguards and procedures necessary to prevent the unauthorized disclosure of SCI and other classified national security information in SCIFs. To define administrative processes that shall provide a secure operating environment and enable adequate security oversight, management, and operations of SCIFs.

B. SCIF Repository

1. As required by ICD 705, the DNI shall manage an inventory of information on all SCIFs which shall be reported to the DNI via the SCIF repository not later than 180 days after the effective date of ICD 705 and updated no later than 30 days after changes occur thereafter.

2. Reportable SCIF Administrative Information:

- SCIF ID
- AO ID
- Location of SCIF
  - In U.S.
  - Outside U.S.
  - Under COM
- SCIF Type
  - Closed Storage
  - Open Storage
  - SWA
  - TSWA
  - T-SCIF
- SID
- Initial Accredited Date
- Re-Accreditation Date
- Review date
- Waivers
- Date waiver approved
- Waiver approval authority/ID
- Exceeded standards
- Does not meet standards
- Date waiver expires

C. SCIF Management

1. SO Responsibilities:

a) The SCIF SO shall be responsible for all aspects of SCIF management and operations to include security policy implementation and oversight.

b) The SO shall prepare a comprehensive Standard Operating Procedure (SOP) that documents management and operations of the SCIF.

c) The SO shall review the SOP at least annually and revise it when any aspect of SCIF security changes.

d) The SO shall issue and control all SCIF keys. Locks shall be changed when a key is lost or is believed to be compromised.

e) The SO shall conduct annual self-inspections to ensure the continued security of SCIF operations, identify deficiencies, and document corrective actions taken. Inspection results shall be forwarded to the AO and copies retained by the SO until the next inspection.

f) The SO shall create an emergency plan to be approved by the AO. Plans shall be reviewed and updated annually and all SCIF occupants shall be familiar with the plans. Drills shall be conducted as circumstances warrant, but at least annually. The emergency plan may be an extension of an overall department, agency, or installation plan.

(1) For SCIFs within the U.S., emergency plans shall address the following:

- Fire
- Natural disaster
- Civil unrest
- Intrusion detection system failures
- Admittance of emergency personnel
- The protection of SCIF occupants and classified information
- Evacuation requirements and emergency destruction

(2) For SCIFs outside the U.S., emergency plans shall address all of the above and shall include instructions for the emergency destruction or removal of SCI where political instability, terrorism, host country attitudes, or criminal activity suggest the possibility that a SCIF may be overrun.

g) The SO shall control passwords to access the maintenance mode of copiers and other office equipment.

h) The SO shall develop an SOP that addresses actions to be taken when IDS maintenance access is required.

2. Required SCIF Documentation

a) Copies of all documents relating to SCIF accreditation shall be maintained by the SCIF SO and include, but not limited to, the following:

- SCIF accreditation
- Fixed facility checklist
- Construction security plan
- CTTA evaluation
- IS accreditation
- SOPs
- The results of the final acceptance test of the original system installation and any tests to system modifications made thereafter
- Emergency plan

b) As applicable, the following documents shall be maintained by the SCIF SO:

- TSCM reports
- Co-utilization agreements
- Memoranda of agreement
- Self-inspection reports
- Compartmented area checklist
- Shipboard SCIF checklist
- Aircraft/UAV checklist
- A copy of the CRZH certificate (UL 2050)
- Pre-Construction Checklist Form

D. SOPs

1. A comprehensive SOP that documents management and operations of the SCIF shall be prepared by the SO.

2. The SOP shall be included in the accreditation package and approved by the AO.

3. All individuals assigned to, or having unescorted access to, the SCIF shall be familiar with and adhere to the SOP.

4. All SOP revisions shall be provided to the AO for approval.

5. SOPs shall be tailored to a specific SCIF.

6. SOPs shall include specific areas of security concern as defined by program or mission requirements.

7. The following are examples of subjects that should be addressed in an SOP:

- Self-inspections
- Security incidents and violations
- Alarm systems and response requirements
- Opening and closing procedures
- Access controls
- Visitor access
- Escort procedures
- Equipment maintenance procedures

- Handling, processing, and destruction of classified material
- Badge procedures
- End-of-day security procedures
- Personnel and package inspection procedures
- Secure communications device instructions

E. Changes in Security and Accreditation

1. Changes affecting the security posture of the SCIF shall be immediately reported by the SO to the AO to include any corrective or mitigating actions taken.

2. If an AO determines that SCIF security conditions are unsatisfactory, SCIF accreditation may be suspended or revoked.

   a) All appropriate authorities and SCIF occupants shall be immediately notified and the SCIF closed until deficient conditions are corrected.

   b) All SCI material shall be relocated to another SCIF.

F. General

1. Except for law enforcement officials or other personnel required to be armed in the performance of their duties, firearms and other weapons are prohibited in SCIFs.

2. Photography, video, and audio recording equipment are restricted but may be authorized for official purposes as documented in the SOP.

3. Procedures shall be established to control IT storage media upon entering or exiting a SCIF in accordance with ICD 503 (Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation).

4. SCIF perimeter doors shall remain closed and controlled at all times. When a door needs to be open, it shall be continually monitored by an SCI-indoctrinated individual.

5. All SCIF occupants shall be familiar with emergency plans and drills shall be conducted as circumstances warrant, but at least annually.

6. Where the risk of hostile action is significant, SCI materials shall be maintained at an absolute minimum.

G. Inspections/Reviews

1. SCIF inspections shall be performed by the AO, or designee, prior to accreditation.

2. The AO, or designee, shall conduct periodic security inspections/reviews to ensure the efficiency of SCIF operations, identify deficiencies, and document corrective actions taken. All relevant documentation associated with SCIF accreditation, inspections, and security administration may be subject to review.

3. Periodic inspections/reviews shall be conducted based on threat, facility modifications, sensitivity of programs, past security performance, or at least every five years.

4. SOs shall conduct annual self-inspections to ensure the continued security of SCIF operations, identification of deficiencies, and to document corrective actions taken. Inspection results shall be forwarded to the AO and copies retained by the SO until the next inspection.

5. Authorized inspectors shall be admitted to a SCIF without delay or hindrance when inspection personnel are properly certified to have the appropriate level of security clearance and SCI indoctrination for the security level of the SCIF.

6. Short-notice or emergency conditions may warrant entry without regard to the normal SCIF duty hours.

7. Government-owned equipment needed to conduct SCIF inspections will be admitted into the SCIF without delay. Specifically, equipment for TEMPEST or Technical Surveillance Countermeasures (TSCM) testing shall be admitted to a SCIF as long as the personnel operating the equipment are certified to have the appropriate level of security clearance and SCI indoctrination.

8. Technical Surveillance Countermeasures (TSCM) activities in SCIFs will only be conducted by USG TSCM teams established or sponsored by a USG element. USG TSCM teams consist of USG military or civilian personnel or USG contractors who have successfully completed approved TSCM training.

H. Control of Combinations

1. Combinations to locks installed on security containers/safes, perimeter doors, windows, and any other opening should be changed in the following circumstances:

   a) When a combination lock is first installed or used.

   b) When a combination has been subjected, or believed to have been subjected, to compromise.

   c) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock.

   d) At other times when considered necessary by the SO.

2. When the lock is taken out of service, it will be reset to 50-25-50.

3. All combinations to the SCIF entrance doors should be stored in a different SCIF. When this is not feasible, alternative arrangements shall be made in coordination with the AO.

I. De-Accreditation Guidelines

SCIF closeouts and de-accreditations shall comply with the following procedures:

1. Inspect all areas, storage containers, and furniture for the presence of classified, sensitive, or proprietary information, and remove any found.

2. Reset safe combinations to 50-25-50 and lock the containers.

3. Affix written certification to all storage containers that the container does not contain classified, sensitive, or proprietary information. The certification shall include the date of inspection and the name and signature of the inspector.

4. Ensure that reproduction and printing equipment is decertified or disposed of in accordance with AO guidance.

5. Dispose of, or relocate, SCI computer equipment, media, hard drives, and portable storage media as approved by the AO.

6. Request revocation of Automated Information Systems (AIS) accreditation.

7. Request revocation of SCIF accreditation.

8. If the SCIF will be used for another mission or project that requires alarms, transfer alarm service to the new activity.

9. If the SCIF will not be used for another mission or project and all classified, sensitive, or proprietary information has been removed, the following shall occur:

   a) Alarm service shall be discontinued.

   b) Combinations on the entrance door and any GSA containers shall be changed to 50-25-50.

   c) All keys shall be accounted for.

J. Visitor Access

1. General Requirements

   a) Visitor logs shall be used to record all SCIF visitors and include the following information:

   - Visitor's full name
   - Organization
   - Citizenship
   - Purpose of the visit

- Point of contact
- Date/time of the visit

b) Government-issued identification shall be required as a means of positive identification.

c) Visitor logs shall be retained for two years after the date of the last entry.

d) Visitor clearance verification shall be accomplished using the DNI Scattered Castles database to the greatest extent possible.

e) Visitors whose clearances have not been verified may be permitted, under escort, entry into the SCIF; however, access to and/or discussion of classified information shall be denied pending clearance verification.

f) Visitors, SCIF occupants, and their possessions may be subject to screening and inspections to deter the unauthorized removal of classified material or the introduction of prohibited items or contraband.

g) Screening and inspection procedures shall be documented and approved by the AO.

2. SCIF Access by Uncleared and Emergency Personnel

a) Uncleared personnel shall be escorted at all times by cleared personnel.

b) The ratio of cleared escorts to uncleared personnel shall be determined on a case-by-case basis by the SO.

c) Prior to assuming escort duties, all escorts shall receive a briefing by the SO or designee outlining their responsibilities.

d) Uncleared personnel shall be kept under observation at all times while in the SCIF. Escorts shall ensure precautions are taken to preclude inadvertent access to classified information.

e) Lights, signs, or other alerting mechanisms or procedures shall be used to alert SCIF occupants of the presence of uncleared personnel.

f) Emergency personnel and equipment shall be allowed access to SCIFs and be escorted to the degree practical. If exposed to classified information, they shall sign an inadvertent disclosure statement when feasible.

K. Maintenance

1. SCI-indoctrinated maintenance personnel shall be used to the extent possible.

2. Procedures for performing maintenance on office equipment, including the use of diagnostic equipment, shall be documented in the SCIF SOP.

3. Computerized diagnostic equipment, to include associated hardware and software, shall be kept under control within a SCIF and shall be managed to prohibit the migration of classified data when connected to classified systems. Procedures shall be documented in the SOP.

4. Passwords to access the maintenance mode of copiers and other office equipment shall be controlled by the SO.

5. Office equipment that is no longer serviceable, such as copiers and classified fax machines, shall be sanitized by having volatile memory erased and non-volatile memory and disk storage removed for terminal destruction.

L. IDS and ACS Documentation Requirements

The following documents and records shall be maintained by the SCIF SO:

1. System Plans such as system design, equipment, and installation documentation.

2. If applicable, agreements established for external monitoring, response, or both, and which shall include the following information:

   - Response time for response forces and SCI indoctrinated personnel.
   - Responsibilities of the response force upon arrival.
   - Maintenance of SCIF points of contact.
   - Length of time response personnel are required to remain on-site.

3. Monitoring Station SOP and/or a copy of the monitoring station UL certificate.

4. Maintenance access SOP.

5. Records, logs, and archives.

6. Records of system testing (for two years) shall include the following information:

   - Testing dates
   - Names of individuals performing the test
   - Specific equipment tested
   - Malfunctions detected
   - Corrective actions taken

7. Records of guard or response force personnel testing as required by the AO.

8. The PCU shall contain a secured, non-volatile event (alarm) log capable of storing at least six months of events, or a printer shall be installed that provides real-time recording of openings, closings, alarms, trouble alarms, and loss of communications.

a) If the system has no provision for automatic entry into archive, the AO may authorize a manual logging system.

b) Monitoring personnel shall record the time, source, type of alarm, and action taken.

c) The SCIF SO shall routinely review the historical records.

d) Results of investigations and observations by the response force shall also be maintained at the monitoring station.

e) Records of alarm annunciations shall be retained for two years.

f) Shunting or masking of any zone or sensor shall be logged in the system archives.

g) All maintenance periods shall be archived into the system.

h) An archive shall be maintained for all remote service mode activities.

9. Access Control Systems Records which include:

a) The active assignment of ID badge/card, PIN, level of access, entries, and similar system-related information

b) Records of personnel removed from the system which shall be retained for two years from the date of removal.

10. Records of security incidents (violations/infractions) regarding automated systems shall be retained by the SO for five years from the date of an incident or until investigations of system violations and incidents have been resolved.

M. Emergency Plan

1. The SO shall create an emergency plan.

2. The emergency plan shall be approved by the AO and maintained on-site for each accredited SCIF.

3. The emergency plan may be an extension of an overall department, agency, or installation plan.

4. The emergency plan shall address the following:

- Fire
- Natural disaster
- Civil unrest
- Intrusion detection system failures
- Admittance of emergency personnel into a SCIF
- The protection of SCIF occupants and classified information

- Evacuation requirements and emergency destruction

5. Plans shall be reviewed at least annually and updated as necessary.

6. All SCIF occupants shall be familiar with the plans and drills shall be conducted as circumstances warrant, but at least annually.

7. Where political instability, terrorism, host country attitudes, or criminal activity suggests the possibility that a SCIF may be overrun, emergency plans shall include instructions for the secure destruction or removal of SCI under adverse circumstances and include contingencies for loss of electrical power and non-availability of open spaces for burning or chemical decomposition of material.

8. Where the risk of hostile actions are significant, SCI holdings and reference materials shall be maintained at an absolute minimum required for current working purposes. If reference or other material is needed, it shall be obtained from other activities and returned or destroyed when no longer needed.

N. SCIF Co-Use and Joint Use

1. Any SCIF that has been accredited by an AO or designee shall be reciprocally accepted for use as accredited by all IC Elements when there are no waivers to the requirements established in ICS 705-1, ICS 705-2 and the IC Tech Specs.

2. Reciprocity is a condition that occurs when there is a requirement to share an accredited SCIF or a portion thereof with a compartment, program or special activity that is sponsored by an IC Element or organization other than the current SCIF CSA.

3. Reciprocal use requires a Co-Use (or Joint Use) agreement (CUA) which:

-Identifies responsibilities of the tenant and host

-Identifies the proposed use/activity

4. All CUA require completion of the SCIF Co-Use Request form.

5. CUA are considered Joint Use when the tenant desires to use the host information system.

6. CUA are routed through and approved by designated Co-Use Coordinators. These are the only individuals another Co-Use Coordinator will accept a CUA form from for processing.

7. The burden to initiate a CUA falls to the tenant. Information accuracy in the request is the responsibility of the tenant/host to facilitate; not the CUA coordinator.

8. CUA are NOT required when sharing a SCIF by two or more components under the cognizance of the same IC Element.

9. CUA are coordinated with the Information System security representatives if the tenant intends to bring an IT system into the host SCIF. Joint Use requires Information System security representative coordination as well.

O. CUA Form and Instructions

1. The following provides a guide on required information to ensure a CUA form is completed sufficiently and can be approved by both the tenant and host Co-Use Coordinators. Information accuracy on the form is the responsibility of the tenant and host mission areas to validate prior to the form being routed to the requesting (tenant) Co-Use Coordinator to initiate the approval process.

2. Overall classification of the CUA will usually be to the host security classification guide, unless the tenant mission is a higher classification.

3. All processing of a CUA should use the current form and be conducted on a classified system. Obtain the current CUA form from your agency Co-Use Coordinator. Legacy forms will not be accepted by the Co-Use Coordinator. Information necessary for a complete form includes:

-Block 1: Host Agency/Department

-Block 2: Tenant Agency/Department POC's (POC's are NOT the CUA Coordinator)

-Block 3: Provide complete and accurate information, to include the complete address and SCIF ID; this is how a coordinator validates information. Ensure the room numbers are accurate. This is important for IS installation. Site POC could be someone from host mission area or SO.

-Block 4: Ensure accuracy; one box must be checked.

-Block 5: Ensure accuracy; this is how a coordinator validates information.

-Block 6: This is the Host Information Security POC. Ensure the Co-Use or Joint Use categories and use criteria is accurate and clarified with Tenant/Host before the form is filled out.

-Block 7: Ensure all required information is filled out for an Industry site. Most Government locations are "Indefinite", however IC Elements AO or Designee may have designated time limits.

-Block 8: Most instances are "Intel Related". If you check "Other" ensure that a full and thorough description is provided in Block 9.

-Block 9: Ensure any information is clarified and input here; don't use for "filler". Classify as needed and portion mark properly.

-Tenant/Host Concur Blocks: Do NOT digitally sign; these are for CUA Coordinator use.

-Classification Block: Ensure the document is classified properly and this block is filled out properly; most likely to the Host classification guides.

P. CUA Cancellation

1. When a CUA is no longer desired or necessary a CUA cancellation form is required.

2. The burden to initiate the CUA cancellation form falls to the tenant.

3. The following provides a guide on required information to ensure a CUA cancellation form is completed sufficiently.

-Block 1: Host Agency/Department

-Block 2: Tenant Agency/Department POC's (POC's are NOT the CUA Coordinator)

-Block 3: Provide complete and accurate information, to include the complete address of the facility hosting the CUA/JUA

-Block 4: Ensure the SCIF ID is accurate.

-Block 5: Ensure the room numbers are accurate. This is important for IS removal (if applicable).

-Block 6: Ensure any pertinent information is clarified and input here.

-Tenant CUA Coordinator will digitally sign and date

-Classification Block: Ensure the document is classified properly and this block is filled out properly.

This page intentionally left blank.

Chapter 13. Second Party Integree and Second Party Liaison Spaces within U.S. Sensitive Compartmented Information Facilities (SCIF)

A. Applicability:

1. This chapter applies only to U.S. SCIFs where Sensitive Compartmented Information (SCI) -indoctrinated Second Party Integree (2PI) officers or SCI-indoctrinated Second Party Liaison (2PL) officers are permitted access or are assigned workspaces in accordance with authorized U.S. and Second Party agreements.

2. This chapter does not apply to foreign officers other than Second Parties, defined below.

3. The mitigations listed in this chapter shall be coordinated with the other SCIF tenants, as applicable.

B. Definitions:

1. Second Party (also known as Five Eyes): Australia, Canada, New Zealand, and the United Kingdom.

2. Second Party Integree (2PI): A Second Party citizen who is employed by a Second Party government who works in support of a United States Government (USG) objective at a USG organization, under the supervision and direction of USG personnel within a USG facility with a co-utilization agreement, or

- A Second Party citizen who works under a USG contract, in support of a USG objective at a USG organization, under the supervision and direction of USG personnel within a USG facility or Second Party facility with a co-utilization agreement.

3. Second Party Liaison (2PL): A Second Party citizen who is employed by, works in support of a mission of, represents the equities of, and works under the supervision of their government or other foreign entity rather than the USG. These individuals act as immediate points of contact for

official interaction between their government or foreign entity and the USG organization to which they are assigned.

4. Unescorted: An individual unaccompanied or unattended in a space, or otherwise without line of sight observation by a SCI-indoctrinated U.S. person.

5. Non-releasable Information: Includes, but not limited to, all No Foreign National (NOFORN), For Official Use Only (FOUO), or any other program information that is not releasable to foreign nationals.

C. General Guidelines:

1. This chapter establishes procedures for implementing mitigations for the assignment of 2PI and 2PL officers within, or granting of access by 2PI and 2PL officer to IC accredited SCIFs.

2. 2PI and 2PL officers may be given unescorted access, with AO approval, to U.S. SCIFs that contain only information and information systems (IS) that is releasable to them without any additional mitigations.

3. IC elements must adhere to all policy standards and guidance noted below before permitting 2PI and 2PL access or assignment to U.S. SCIFs:

- Intelligence Community Directive (ICD) 704, *Personnel Security Standards and Procedures for Access to SCI*
- Intelligence Community Standard (ICS) 704-02, *Waiver Requests for Access to SCI*
- ICS 503-04, *Managing Non-U.S. Personnel Access to Information Systems*
- ICD 705, *Sensitive Compartmented Information Facilities*
- ICS 705-01, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*
- ICS 705-02, *Standards for Accreditation and Reciprocal Use of SCIFs*

- ICD/ICS 705, *Technical Specifications for Construction and Management of SCIFs*
- ES-2016-00816, *Second Party Integree Access to the Intelligence Community (IC) Information Environment*. This chapter establishes procedures for implementing mitigations for the assignment of 2PI and 2PL officers within IC-accredited SCIFs.

At a minimum, and prior to placement, the U.S. host organization will ensure:

a. All 2PI and 2PL officers assigned to U.S. SCIFs have the appropriate security clearance equivalent to Top Secret (TS)/SI/TK
b. Agreements, through which the officer has been authorized, have been executed
c. All necessary approvals, as specified in paragraph D.1, have been received, and mitigations as specified in paragraph D.2 have been implemented

4. All requirements established in ICS 503-04, *Managing Non-U.S. Personnel Access to Information Systems* will be implemented and adhered to. This applies to all U.S. or partnership IS that store, process, or transmit U.S. intelligence information, as defined in ICS 503-04.

5. Every effort will be made to place 2PI officers outside of U.S. SCIF space where non-releasable information or IS is processed, stored, or located.

6. 2PL officers shall not be placed in or given unescorted access to U.S. SCIF space where non-releasable information or IS is processed, stored, or located.

7. 2PI or 2PL officers shall not be placed in or given unescorted access to a U.S. SCIF that also contains open storage of Special Access Program information.

8. 2PI officers shall not be given unescorted access to U.S. SCIFs or SCIF areas in which they do not have assigned workspaces unless that SCIF or SCIF area is the most direct walk-path to their assigned workspace. If the most direct walk-path must transverse these areas, all standards, mitigations, and outlined requirements within this chapter also are extended to any hallways or open SCIF cubicle/work areas that the 2PI must traverse to reach their assigned work location.

9. Intent to permit access, or assign approved 2PI or 2PL officers within an existing accredited U.S. SCIF shall be immediately reported by the Security Officer or Mission Owner to the Accrediting Official (AO), to include any mitigating actions for AO and Authorizing Official, for approval. Chief Information Security Officer (CISO) consultation is recommended. The host agency AO shall notify all co-use tenants in writing at least 30 days prior to the assignment of 2PI or 2PL personnel to the SCIF and provide a list of mitigations that will be implemented to prevent access to non-releasable information for the duration of the 2PI or 2PL's assignment. Co-use tenants are responsible for any additional mitigations above and beyond those mitigations in place or recommended that are particular to the protection of their information. The additional mitigations will be adhered to by any other tenants and by the host if they require access to the tenant's information. 2PI or 2PL officer assignment to the specific SCIF will be annotated in the IC SCIF Repository.

10. If an AO determines that required SCIF security mitigations, as specified in paragraph D.1 and D.2 have not been met or if 2PI or 2PL officers are placed or provided access without the necessary approvals, immediate corrective action is required and may include: exclusion of 2PI or 2PL officers from general or unescorted access to the space; suspension or revocation of SCIF accreditation; removal of all non-releasable information and IS, or; other action as determined by the AO.

11. IC Elements must implement the AO-approved mitigations listed herein within 45 days of issuance of this chapter. SCIF AOs may provide an extension for SCIFs already accredited to allow elements additional time to

implement the listed mitigations. The additional timeline will be determined by the AO.

D. Approvals, Mitigations, and Procedures

This section provides guidance on procedures and mitigations to support placement of TS/SI/TK or equivalent cleared 2PI officers within U.S. SCIFs where non-releasable information or IS are processed, stored, or located.

1. Approvals:

   a. AO approval is required when some or all the mitigations outlined in section D.2.a. are implemented. If mitigations other than those listed in section D.2.a. are implemented or changed, approval by the host IC element head or their designee, and notification to any affected tenants or agencies with co-use agreements is required. Any alternate mitigations must meet the requirement of ICD 705 that SCI be protected from unauthorized disclosure, which includes the unauthorized disclosure of non-releasable information to 2PI officers.

   b. All applicable authorizing officials (e.g., AO and CISO) for non-releasable IS must determine their risk tolerance based on the implemented mitigations. If the SCIF is co-use by other tenants, the authorizing officials from those other agencies also must review the mitigations and determine risk tolerance.

Note: In accordance with ICD 705, waivers must be approved by the IC element head. When approving assignment of 2PI officers within SCIFs the IC element head may only approve waivers and accept risk as it relates to the SCI information processed and IS for which their IC element is responsible. In accredited SCIFs where 2PI have been granted physical access to the space, and where SCI information is processed or IS that belong to more than one IC element are present, all affected elements **must be informed of any waivers**, and decide to accept the risk, remove their systems, or implement additional mitigations as necessary.

In addition, each 2PI or 2PL shall be assigned a Control Officer (CO)/Mission Sponsor (MS) who is responsible for ensuring the 2PI or 2PL does not receive access to any information not authorized as outlined in the Designated Disclosure Letter by the IC element's International Program Office or equivalent. AOs are responsible for documenting 2PI and 2PL and CO/MS assignments and ensuring that the documentation is accessible to all tenants within the SCIF.

2. Mitigations:

a. The AO shall minimize access to non-releasable information by implementing the following mitigations (if applicable):

- Segregating 2PI-releasable and non-releasable areas of the SCIF to the greatest extent practical
- Using access control systems to restrict 2PI access to only those SCIF areas to which they are assigned and/or must traverse on the most direct walk-path to their assigned workspace consistent with their agreements
- Using partitions and/or signs to designate SCIF locations where 2PI officers are assigned or traverse
- Using partitions and signs, or colored tape on the floor to designate U.S.-only areas
- Locking computer screen(s) (throughout the day) or logging out of system(s) (at end of day) and conducting security check of area before departing
- Implementing security education and awareness program(s) with annual refresher training for SCIF occupants

b. Minimize the likelihood of accidental visibility by implementing the following:

- Using polarizing privacy screens
- Positioning computer screens aimed away from doorway, cubicle openings, walk paths, and common spaces

- Positioning non-releasable information or IS away from doorways, cubicle openings, walk-paths, and common spaces, and co-locating non-releasable information or IS with other like compartmented non-releasable or IS
- Using cover sheets for classified information at all times
- Ensuring that all classified information printing/reproduction equipment that processes non-releasable information uses identity verification (e.g., pin to print)
- Implementing clean desk policies and securing non-releasable information when not in use
- Ensuring that discussion of non-releasable information does not takes place in areas where 2PI are assigned or traverse, and placing "no-discussion" signs in prominent places on the walls
- Ensuring equipment with Top Secret video/teleconference capability is located in an authorized space which meets STC 50 (in accordance with ICD/ICS 705, *Technical Specifications for Construction and Management of SCIFs)*, and uses a mitigation to preclude unauthorized use by 2PI personnel (e.g., PIN-enabled)

c. All attempts should be made to separate 2PI office space from U.S. office spaces. To prevent inadvertent disclosure, sound masking devices or sound batting shall be installed between the offices and above false ceilings (in accordance with Chapter 9E). Additionally, office doors shall be closed when discussing non-releasable information if FVEY personnel are present or have access to the area, and speaker phones located in non-enclosed areas shall be disabled.

3. <u>Procedures</u>:

a. If appropriate mitigations are implemented and approvals obtained as described in this chapter, the AO may approve:

1) Assigned SCI-indoctrinated 2PI officers to move unescorted to/from their assigned space(s) via designated walk-paths when properly cleared U.S. personnel are present within the workspace.

2) Assigned SCI-indoctrinated 2PI officers to escort SCI-indoctrinated visitors to/from the 2PI assigned work areas only when U.S. SCI-indoctrinated personnel are present in the workspace.

3) Assigned SCI-indoctrinated 2PI officers to escort 2P visitors, who are either uncleared or whose 2P clearance has not been verified, to/from the 2PI officer's assigned work areas only if all of the following are met:

- U.S. SCI-indoctrinated personnel are present in the workspace
- All inhabitants are made aware of visitor presence via auditory or visual means
- The visit duration is limited to one day, unless approved for longer period, at which time the visit shall be revalidated

b. The AO may authorize an SCI-indoctrinated assigned 2PI person to have lock combinations and/or intrusion detection system (IDS) arming/disarming codes of a U.S. SCIF perimeter door only when:

1) There is a validated mission requirement

2) All information and IS processed, stored, or located within the SCIF space are FVEY-releasable, or non-releasable information is stored in a GSA-approved security container when there are not SCI-indoctrinated U.S. personnel present in the workspace

3) All SCIF organizational tenants and agencies with co-utilization agreements with this or any adjacent SCIF have been notified in writing of the 2PI integration and been provided an opportunity to raise concerns.