Department of Defense

MANUAL

NUMBER 5105.21, Volume 2
October 19, 2012

USD(I)

SUBJECT: Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each serving a specific purpose, and reissues DoD Manual (DoDM) 5105.21-M-1 (Reference (a)). The purpose of the overall Manual, in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (b)), is to implement policy established in DoD Instruction (DoDI) 5200.01 (Reference(c)), and Director of Central Intelligence (DCI) Directive (DCID) 6/1 (Reference (d)) for the execution and administration of DoD Sensitive Compartmented Information (SCI) program. It assigns responsibilities and prescribes procedures for the implementation of DCI and Director of National Intelligence (DNI) policies for SCI.

b. Volume. This Volume addresses the administration of physical security, visitor control, and technical security for SCI facilities (SCIFs).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, except as noted in paragraph 2.c., the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

b. Applies to contractors in SCIFs accredited by the Defense Intelligence Agency (DIA) and to DoD SCI contract efforts conducted within facilities accredited by other agencies and approved for joint usage by a co-utilization agreement.

c. Does not apply to the National Security Agency/Central Security Service (NSA/CSS), National Geospatial-Intelligence Agency (NGA), and the National Reconnaissance Office (NRO), to which separate statutory and other Executive Branch authorities for control of SCI apply.

3. DEFINITIONS. See Glossary.

4. RESPONSIBILITIES. See Enclosure 2 of Volume 1 of this Manual.

5. PROCEDURES. General procedures for SCI administrative security are found in Enclosure 2, Volume 1 of this Manual. Procedures for physical security, visitor control, and technical security for SCI facilities are detailed in Enclosures 2, 3, and 4 respectively of this Volume.

6. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Volume:

a. Is effective October 19, 2012.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (e)). If not, it will expire effective October 19, 2022 and be removed from the DoD Issuances Website.

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Physical Security
3. Visitor Control
4. Technical Security

Glossary

TABLE OF CONTENTS

FIGURE

ENCLOSURE 1

REFERENCES

(a) DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," August 1998 (cancelled by Volume 1 of this Manual)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(c) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
(d) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual," March 1, 1995[1]
(e) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012
(f) Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities," May 26, 2010
(g) Intelligence Community Standard 705-1, "Physical and Technical Security Standards for Sensitive Compartmented Information Facilities," September 17, 2010
(h) Intelligence Community Standard 705-2, "Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information," September 17, 2010
(i) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005
(j) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
(k) Unified Facilities Criteria 4-010-1, "DoD Minimum Antiterrorism Standards for Buildings," 2002
(l) DoD Manual 5200.01, "DoD Information Security Program," Volumes 1-4, February 24, 2012
(m) Volume 6 of U.S. Department of State Foreign Affairs Handbook 12, "OSPB Security Standards and Policy Handbook," July 2006[2].
(n) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
(o) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
(p) DoD Instruction O-5205.11, "Management, Administration, Oversight of DoD Special Access Programs (SAPs)," July 1, 1997
(q) Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy," June 30, 1998
(r) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(s) DoD Directive 5530.3, "International Agreements," June 11, 1987
(t) Intelligence Community Directive 701, "Security Policy Directive for Unauthorized Disclosures of Classified Information," March 14, 2007
(u) Army Regulation 380-27, "Control of Compromising Emanations," May 19, 2010
(v) Air Force Instruction 71-101, Volume 3 "Air Force Technical Surveillance Countermeasures Program," June 1, 2000

[1]Available via http://www.intelink.ic.gov/sites/cps/policystrategy/policy/pages/dcids.aspx [JWICS]
[2] Available via http://source.ds.state.sgov.gov/products/library_FAMsFAHs/FFhome.asp [SIPRNET]

(w) Secretary of the Navy Instruction 3850.4, "Technical Surveillance Countermeasures," December 8, 2000
(x) Joint Staff Manual 5220.01A, "Temporary Restricted Area Access Request," October 1, 1997
(y) Administrative Instruction 30, "Force Protection of the Pentagon Reservation," June 26, 2009
(z) DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM) Program," February 22, 2006
(aa) Intelligence Community Directive 702, "Technical Surveillance Countermeasures," February 18, 2008
(ab) National Security Telecommunications Information System Security Advisory Manual 2-95 & 2-95A, "RED/BLACK Installation Guidance" February 3, 2000
(ac) National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems (PDS)," December 3, 1996
(ad) National Security Telecommunications and Information Systems Security Instruction 7002,"TEMPEST Glossary," March 17, 1995
(ae) National Security Telecommunications and Information Systems Security Instruction 4002, "Classification Guide for COMSEC Information," June 5, 1986

ENCLOSURE 2

PHYSICAL SECURITY

1. GENERAL

a. Physical security standards for the construction and protection of SCIFs are prescribed in Intelligence Community Directive (ICD) 705 (Reference (f)), Intelligence Community Standard (ICS) 705-1 (Reference (g)), and ICS 705-2 (Reference (h)). DoD SCIFs will be established in accordance with those references and this Volume.

(1) Wherever practical, SCIFs will be designated as a restricted area in accordance with DoD Instruction 5200.08 (Reference (i)). The special security officer (SSO) will coordinate to list the SCIF within the post or installation directive that defines and designates all local restricted areas and will post outside the SCIF the proper English and, when appropriate (overseas areas only), foreign language "Restricted Area" signs. If a SCIF is physically located within a restricted area, it does not also need to be designated as a controlled area.

(2) Personnel who work in or have routine or unescorted access to a SCIF must be indoctrinated for the compartments of SCI that is discussed, processed, or stored within the facility.

(a) If a SCIF has multiple SCI control systems that are physically separated by an internal access control device or other similar control system, only SCI-indoctrinated personnel with the appropriate level of access for the facility will escort uncleared personnel. SCIF door combinations and bypass keys, if applicable, must be protected at the same level for which the facility is accredited.

(b) Main entry point combinations and bypass keys, if applicable, will be stored in a different SCIF of the same or higher accreditation.

(c) Access codes to an intrusion detection system and access control device will be limited to personnel who are SCI-indoctrinated and have a need to know. Administrator privileges to intrusion detection systems should be limited to the SSO.

(3) Operations security (OPSEC) principles are critical for protecting the operational activities and security of SCIFs. OPSEC principles should be considered and implemented based on the local security environment.

(a) The facility's location (complete address) and identity as a SCIF shall be protected at a minimum of FOR OFFICIAL USE ONLY (FOUO). Drawings or diagrams identified as a SCIF may not be posted on an UNCLASSIFIED website or transmitted over the Internet without some type of encryption.

(b) SCIFs should be referred to as a controlled space or another terminology so as not to designate it as a SCIF on releasable documents (e.g., bid requests, permit requests, sub-contractor plans).

(c) Refer to DoDD 5205.2 (Reference (j)) for further OPSEC guidance.

(4) All new facilities shall be constructed as directed in References (g) and (h), and in compliance with Unified Facilities Criteria 4-010-1 (Reference (k)). SCIF construction overseas shall also comply with applicable local anti-terrorism and force protection regulations. SCIFs built under Chief of Mission (COM) control will follow Department of State guidelines.

b. Approvals. Reference (f) provides detailed physical security recommendations that should be applied. These recommendations are generally phrased with words such as "should," "may," and "can." In some instances, such as speakerphones, answering machines, and secondary doors, these recommendations are contingent upon accrediting official (AO) (DIA Counterintelligence and Security Office (DAC)) approval. Requests must include adequate details that enable DAC to render an informed decision. DAC may delegate to senior intelligence officials (SIOs) of the Combatant Commands the authority to approve Temporary Secure Working Areas (TSWAs), Temporary SCIFs (T-SCIFs), and concept statements for creation of new SCIFs.

c. Mitigations. Methods identified in the Intelligence Community (IC) Technical Specifications contained in Reference (g) are an accepted way to meet the performance standard, but there may be several ways to achieve the same standard other than what is listed. A different method may be used if it achieves the same performance standard as identified in Reference (f). This mitigation must be identified in the Fixed Facility Checklist (Attachment A to Reference (g)) and requires approval from the AO before implementation.

d. Waivers

(1) Reference (f) provides detailed physical security requirements. These requirements are generally phrased with definitive words such as "will," "shall," and "must." Requirements of this nature require a waiver whenever they cannot be followed and mitigations cannot be applied (i.e., a waiver down). A waiver is also required when these standards are exceeded (i.e., a waiver up).

(2) All waiver requests will be submitted through the cognizant security authority (CSA), their designee, or the DoD Component SIO to DAC for review. If DAC determines that a waiver is warranted, it will process the waiver request for approval.

(3) Waivers down will be guided by the principles of risk management. The request must be signed by the reviewing official (the CSA, their designee, or the DoD Component SIO) and at a minimum must include the following information:

(a) The physical security requirement(s) that cannot be met.

(b) Explanation of why the security requirement cannot be implemented and the mitigations that were considered.

(c) Mission impact if the waiver is disapproved.

(d) Identification of compensatory countermeasures that can be implemented in lieu of the established physical security requirements that can reduce the residual risk.

(e) The time expectation on when the standard can be met and a waiver is no longer required.

(4) Elements requesting waivers up must forward a written request through the CSA, their designee, or the DoD Component SIO to DAC. The request at a minimum must include the following information:

(a) The physical security requirement that will be exceeded.

(b) A statement of documented risk that justifies the need to exceed standards.

(c) Mission impact if the waiver is disapproved.

(d) Identification of the additional security measures being put into place.

(e) The time expectation on when the waiver will no longer be required.

(5) Limitations on Waivers. Waivers are normally granted for a period of up to 1 year or until such time as the waiver is no longer needed. All waivers shall be reported to the Office of the Director of National Intelligence (ODNI) and maintained in the ODNI database. All SCIFs with permanent waivers will be reviewed annually using the current standards to determine if a waiver is still needed or if mitigations can be used instead. Elements requesting co-use of any SCIF with a waiver will be informed of it.

(6) Classification Guidance. Guidance on classification of information related to the accreditation of DoD SCIFs is maintained on the DAC JWICS website (http://www.dia.ic.gov/homepage/da/security/field/index.html). All SCIF documentation classified under DIA classification authority shall be marked and transmitted per DoDM 5200.01 (Reference (l)).

2. SCIF DESIGN AND PLANNING

a. Site Planning

(1) SCIF security begins with the decision to build a SCIF. Adequate planning and design will prevent many of the security risks to SCI and reduce the costs of construction. Site planning should include looking at the standoff distances for AT/FP as well as TEMPEST.

(2) The Service CSA or DoD Component SIO or their designees shall conduct one-time construction project reviews before site acquisition (purchase or lease of a building) for the purpose of making transparent, accountable, and prudent risk management decisions involving security requirements and long-term security risks.

b. Concept Approval

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

(2) Once a need for SCI has been identified, the organization's commander will submit a request for SCI to the Service CSAs, their designees, or DoD Component SIOs. This request will identify the levels and types of SCI desired and certify that the organization is able to support the SCIF (i.e., manning and budget) throughout its lifecycle.

(3) Upon receipt of the request to build a SCIF, the Service CSAs, their designees, or DoD Component SIOs will validate the need for a SCIF and the requirement for the requested level of SCI. The Service CSAs, their designees, or DoD Component SIOs are required to grant concept approval to establish a SCIF, to include contractor SCIFs. They may delegate this approval as deemed necessary. If delegated, the Service CSAs, their designees, or DoD Component SIOs must notify DAC to preclude potential confusion.

(4) The Service CSAs, their designees, or DoD Component SIOs will provide the concept approval and, if applicable, the DD Form 254, "Contract Security Classification Specification," for contractor facilities to DAC with an information copy to the supporting SSO.

c. Diplomatic Facilities

(1) DoD SCIFs established within diplomatic facilities fall under the security responsibility of the COM and must also obtain permission through Department of State channels to build a SCIF. These SCIFs will comply with all requirements of Reference (f) and meet the Overseas Security Policy Board (OSPB) standards in accordance with Volume 6 of U.S. Department of State Foreign Affairs Handbook 12 (Reference (m)).

(2) Where OSPB standards and DoD standards conflict, the more stringent will be applied unless resolved by DAC and the Department of State Bureau of Diplomatic Security.

3. SCIF TYPES

a. Temporary SCIFs

(1) TSWA

(a) A TSWA must not be used more than 40 hours per month and no longer than 12 months in the same location. The 40-hour rule is based on an average use of the TSWA over a 12-month period. The purpose for this requirement is that a TSWA's physical security standards are less than that of a permanently accredited SCIF. If the facility will be used on a more frequent basis, the user of a facility must pursue permanent accreditation. On a case-by-case basis and with sufficient justification, DAC may approve SCI storage (not to exceed 6 months).

(b) The Service CSAs, their designees, or DoD Component SIOs may approve TSWAs for all compartments of SCI. Approval for processing SCI in TSWAs may only be granted by DIA or heads of the intelligence and counterintelligence elements of the Military Services, Combatant Commands, and Defense Agencies according to their respective information system (IS) accreditation authority.

(c) Active TSWA status will be annotated on the DIA JWICs share point site by the applicable Service CSAs, their designees, or DoD Component SIOs.

(2) T-SCIF

(a) T-SCIFs are used in support of tactical, contingency, and field-training operations for a limited time where physical security construction standards associated with permanent facilities are not possible. They may include hardened structures (buildings, bunkers, etc.), truck-mounted or towed military shelters, tents, prefabricated modular trailers or buildings, and areas used on aircraft and surface and subsurface vessels.

(b) The Service CSAs, their designees, or DoD Component SIOs may establish and grant temporary accreditation to operate a T-SCIF. These officials may further delegate this approval, in writing, to a lower level of command providing continued oversight is maintained. No further delegation is authorized. T-SCIF approvals will be valid for up to 1 year. Consideration must be given to establishing a permanent SCIF whenever it is known that the T-SCIF will be required for a period greater than 1 year. Extension beyond the 1-year period must be justified in writing to DAC, which retains approval authority.

(c) Active T-SCIF status will be annotated on the DIA JWICs sharepoint site by the applicable Service CSAs, their designees, or DoD Component SIOs.

(d) Elements establishing or operating a T-SCIF within a deployed theater will notify the respective Combatant Command SSO within 48 hours. Such elements will also provide updates relating to the current location and status of T-SCIF under their control as directed by the Combatant Command SSO.

(e) Refer to Chapter 5, "IC Technical Specifications," of Reference (f) for detailed physical security requirements for T-SCIFs. DAC is the approving authority whenever the application of a specific physical security requirement cannot be achieved in response to an unprecedented or unique operating environment.

(f) The information assurance manager (IAM) must obtain Automated Information System (AIS) accreditations in accordance with Reference (f). The designated approval authority (DAA) shall decide whether to grant accreditation approval to operate a system based on all available documentation and mitigating factors. The DAA may grant approval to operate a system as certified or grant interim approval to operate identifying the steps and any additional controls to be completed prior to full accreditation.

(g) The T-SCIF accrediting authority is responsible for ensuring that the TEMPEST requirements for the T-SCIF are followed. These requirements are outlined in Enclosure 4 of this Volume of this Manual. If these requirements cannot be met, DIA's Certified TEMPEST Technical Authority (CTTA) must be consulted.

b. Permanent SCIF. DAC is the sole accrediting authority for physical and technical (TEMPEST) security for permanent SCI facilities.

(1) Secure Working Areas (SWAs). SWAs are accredited and used for handling, discussing, and processing but SCI is not stored in them. Since there is no time limit on their accreditation, SWAs require a higher level of security than TSWAs and T-SCIFs. The SWA shall be controlled at all times by SCI indoctrinated individuals or secured with a General Services Administration (GSA)-approved pedestrian deadbolt meeting Federal specification FF-L-2890. All SCI used in a SWA shall be moved to an accredited SCIF at the end of each business day or destroyed using CSA approved methods. There shall be a plan to relocate or destroy SCI material in the event of an emergency or natural disaster. This plan shall be tested semi-annually.

(2) Continuous Operations SCIFs. This SCIF is staffed and operated 24 hours a day, 7 days a week. Staffed refers to personnel who possess the appropriate security clearance and are permanently assigned to the SCIF as opposed to the guard force. There should be enough personnel continuously present to observe all areas that provide access to the SCIF to include primary, secondary, and emergency exit doors.

(3) Open Storage SCIFs. Open storage SCIFs allow SCI to be openly stored within the SCIF without using GSA-approved storage containers. Open storage construction requirements shall be met.

(4) Closed Storage SCIFs. All SCI material must be stored in a GSA-approved security container in an accredited facility.

4. CONSTRUCTION SECURITY

a. The renovation of existing SCIFs and the construction of new SCIFs shall meet the security requirements outlined in Reference (f). Any variances of these requirements must be approved by DAC prior to their implementation.

b. An SCI-indoctrinated site security manager (SSM) shall be designated by the component SSO for each new construction or renovation project. The SSM may be a U.S. Government (USG) employee, military member, or contractor, but will not be employed by the construction firm completing the project. The SSM represents the organization constructing or renovating the SCIF for all security matters to both the construction firm and the AO.

(1) The SSM shall develop a construction security plan (CSP) for each project. The plan shall include a risk assessment of the threats against the project to include human intelligence (HUMINT), counterintelligence (CI), technical, and AT/FP. The threat sources identified in Reference (f) must be used, but additional threat assessments from local sources should be utilized to define the total threat.

(2) The complexity and scope of the CSP will depend on the project. Simple modifications may only be a few pages, while the construction of a new building may be several hundred pages. Project work schedule and related documents shall be provided to the SSM in order to adequately consider and implement prudent or required security measures.

(3) The SSM, during the course of the project, shall establish appropriate security files. These files may include work schedules, picture ID cards and access records, local guard incident and other reports, inspection reports, copies of security violations, and similar substantive project documentation as deemed appropriate by the SSM.

(4) SSMs shall have 24-hour unrestricted access to on-site construction offices and areas to conduct security inspections. This does not mean that the SSM has to be on site at all times. During construction or renovations, the SSM shall conduct unannounced security surveys at random intervals to meet appropriate security procedures.

(5) The SSM shall be responsible for access control of the site and verify that the construction site is clear of all uncleared workers during non-duty hours.

c. During the design phase and prior to the start of construction, a CSP shall be developed by the SSM. A CSP template is available on the DIA SCIF JWICS accreditation site (http://www.dia.ic.gov/homepage/da/security/field/index.html).

(1) Security officials overseeing SCIF construction projects shall submit the CSP to DAC at the 30 percent design point along with the completed risk assessment. Based on these two documents, DAC will issue CSP guidance. The SSM will continue to update the CSP as appropriate and develop SOPs for use on the project. Component SSOs will monitor the development and implementation of the CSP. TEMPEST requirements will also be identified during this time in accordance with Enclosure 4 of this Volume.

(2) A facility under the COM, the CSP must be confirmed or certified in accordance with the OSPB in accordance with Reference (m). Assistance in developing a CSP can be obtained through DAC or the local Department of State representative.

d. SCI-indoctrinated escorts are required when uncleared workers have access to SCIF areas. The ratio of escorts will be determined on a case-by-case basis by the SSM. Prior to assuming escort duties, escorts shall receive a briefing outlining their individual responsibilities.

e. Security checks will be performed on construction personnel to the greatest extent practical. Security checks shall, at a minimum, consist of local records checks conducted by military installation visitor and pass and identification offices, local military police, or local CI offices.

(1) Access to the construction site shall be denied or withdrawn by the SSM if any security checks reveal a felony criminal record, or the risk is otherwise too great to permit access to the site. SSM shall notify the installation or corporate access control department to ensure the individual cannot gain further access.

(2) A list of authorized workers should be established and maintained by the SSM.

(3) Prior to obtaining access to the site, construction workers shall be given an unclassified security orientation by a security representative. A security POC shall be provided for construction personnel to report information of a security nature.

f. A unique project site picture ID card and temporary pass system shall be implemented for access control.

(1) Construction site access control must include effective entry and exit screening and search procedures. To the greatest extent possible, a single entry point should be established to aid in this process.

(2) A prominent sign, printed in English and, if applicable, any other language deemed appropriate, shall list all prohibited and restricted items, and shall be posted at all construction area entry points. Personal bags, parcels, or packages shall not be allowed on the construction site by uncleared workers unless procedures are established for searching and safekeeping of such items.

(3) Physical security barriers shall be erected to deny unauthorized access to the controlled areas.

5. SCIF ACCREDITATION

a. The DAC is the accrediting official for DoD SCI facilities, excluding those under NGA, NRO, and NSA cognizance.

b. Refer to Enclosure 4 of this Volume for TEMPEST accreditation and ICD 503 (Reference (n)) for AIS accreditation.

c. The physical accreditation process begins when the DAC AO receives a validated concept approval from a Service CSA or DoD Component SIO or their designee.

d. Upon receipt of the concept approval, DAC will assign a SCIF ID in order to track future correspondence and forward this to the requestor through their chain. The requestor shall appoint an SSM, complete the CSP (see section 4 of this enclosure) and TEMPEST Countermeasures Review worksheet (see Enclosure 4 of this Volume) and begin the fixed facility checklist (FFC). The FFC format is in the technical specifications published under Reference (f).

e. Preconstruction Approval

(1) The SCIF design will consider threats and vulnerabilities against appropriate security measures to reach an acceptable level of risk. Proper security planning for a SCIF is intended to deny foreign intelligence services and other unauthorized personnel the opportunity for undetected entry into these facilities and exploitation of sensitive activities.

(2) Upon receipt of the concept approval and checklists, DAC will conduct a comprehensive risk management review and provide preconstruction advice and assistance. To avoid costly construction pitfalls, no construction should begin until DAC has reviewed the packet.

(3) The FFC included in technical specifications published in accordance with Reference (g) and the Aircraft/UAV Accreditation Checklist and Shipboard (Surface/Subsurface) Accreditation Checklist are the primary documents in the decision-making process for granting a final accreditation. These checklists must provide sufficient detail to enable DAC to determine if the facilities satisfy physical standards detailed in Reference (g). Shipboard and aircraft accreditation checklists are available through the JWICS website at http://www.dia.ic.gov/homepage/da/security/field/index.html.

(4) These documents, along with their enclosures, should be completed and submitted initially around the end of the design phase when sufficient information has been gathered to complete the majority of the FFC. They should be updated periodically during the construction phase. The fully complete FFC and TEMPEST Addendum, along with attachments, should be submitted prior to the completion of the SCIF for the final accreditation.

f. Accreditation. Acceptance of the accreditation package is the last step in obtaining the accreditation of a new SCIF or the reaccreditation of an existing SCIF. The SCI security official will submit one copy each of the accreditation package to DAC through the appropriate CSA, their designee, or the DoD Component SIO.

(1) The accreditation package must include:

(a) The final FFC.

(b) Specification sheets for IDS component parts.

(c) UL 2050 certification for IDS (this requirement does not apply to SCIFs on military installations).

(d) NIST 128 bit certificate for IDS.

(e) IDS test results.

(f) SAP co-utilization agreement (if applicable).

(g) Technical surveillance countermeasure (TSCM) reports (if applicable).

(h) Catastrophic failure plan.

(2) All entries on the changed or "to be determined" items list must be completed and an asterisk placed to the left of each paragraph that changed from the initial FFC.

(3) DAC will review the accreditation package for compliance with SCI physical security standards and will issue a formal written accreditation for the SCIF and notify the requesting SSO and the appropriate CSA, their designee, or the DoD Component SIO once the SCIF satisfactorily meets the standards. In some instances, a pre-accreditation inspection by DIA SCIF accreditors may be required. The SCIF identification number initially assigned by DAC in the preconstruction phase must be used on all future communications with DIA/DAC-2. SCI will not be discussed or introduced into the proposed SCIF until the facility is accredited. The SCI compartments will not be included in the DAC formal written accreditation document.

(4) Accreditation documents transmitted to DAC, to the greatest extent practical, should be in a digital format.

g. Transfer of Security Cognizance. SCIFs transferred from one CSA to another are not required to be reaccredited provided that all the physical security standards remain in place, all accreditation records will be furnished to the new CSA, and all appropriate organizations will be notified. Whenever DIA assumes CSA responsibility, DAC will issue a temporary accreditation with a new SCIF identification number and request that all accreditation documents be updated and submitted to DAC within 90 days. A permanent accreditation will then be issued.

h. Reaccreditation. An existing SCIF must be reaccredited when a change occurs in any of the following areas: SCIF perimeter (i.e., expansion or downsizing), storage requirements (i.e., closed storage to open storage), change from continuous (24 hours) operations to open or closed storage. Furthermore, a reaccreditation may be issued based upon results from a DIA inspection. Reaccreditation is not required whenever a compartment of SCI is moved from one room to another within the SCIF.

i. Modifications

(1) All modifications involving construction work on the perimeter walls or major modifications must have a CSP (see section 4 of this enclosure).

(2) Major modifications to existing SCIFs require prior approval by DAC. These modifications include, but are not limited to, acquisition and installation of new alarm, telephone and intercom systems, changes in exterior doors, windows and locking devices, vent and duct work, and changes in security posture (e.g., closed vice open storage, continuous operations vice closed).

(3) Minor modifications to existing SCIFs require DAC notification. These modifications include, but are not limited to permanent securing of doors, installation of approved phones, changes in occupant or office symbol, room numbers, and interior changes.

(4) For either modification, submit an updated page change of the FFC with applicable drawings. Each page must be fully completed and dated, and an asterisk must be placed beside the changed items. DAC will review the completed FFC for compliance and give a formal reply prior to the modification occurring. For major modifications, the facility may be inspected prior to reaccreditation.

j. Changes to Security Posture. Within 24 hours, the SSO will report to DAC and the appropriate CSA, their designee, or the DoD Component SIO, through SSO chain of command, all changes affecting the security posture of any SCIF. If immediate advice is required, call DAC (703-907-1299 or DSN 283-1299). Examples of changes in security posture include:

(1) Fire, explosion, natural, or other disaster.

(2) Any other situation affecting SCI security.

k. Withdrawal of Accreditation

(1) When a SCIF is no longer required, the local SSO will initiate withdrawal of accreditation and forward a copy of the request to the appropriate head of an intelligence community element (HICE) or designee. Upon notification, DAC will issue appropriate SCI withdrawal correspondence. The SCIF identification number will no longer be valid. The local SCI security official responsible for SCIF security will conduct a closeout inspection of the facility to verify that all SCI material has been removed. Use the guidelines in Appendix 1 to this enclosure.

(2) If DAC determines there is a danger of compromising classified information or security conditions in a SCIF are unsatisfactory, SCI accreditation will be suspended or revoked. All appropriate authorities will be notified of such action immediately.

(a) DAC may approve reaccreditation of a previously accredited SCIF based upon a review of an updated facility accreditation package.

(b) Contractor SCIF accreditation will terminate with the termination of the contract(s) and the time allotted for contract closeout. The contractor SSO (CSSO) will initiate the SCIF closeout and the contracting officer representative (COR) will verify that all SCI material is removed from the SCIF and disposed of according to the contract vehicle and all applicable policy documents. The CSSO will follow guidance in Appendix 1 of this enclosure.

l. Caretaker Status. Caretaker status occurs when a SCIF owner or sponsor identifies a need to temporarily shut down SCI activities. This change in accreditation status, granted by DIA/DAC-2, is usually associated with, but not limited to, major construction projects or operational contingencies requiring the local SCI mission to forward deploy. The SCIF owner or sponsor anticipates resuming normal operations in the future. Once approved for caretaker status, the SCIF has up to 1 year to obtain a reaccreditation and be authorized to resume normal SCI operations. The SCIF owner must provide an estimated activation date when requesting caretaker status. Extensions may be granted on a case-by-case basis by DAC. However, extension requests must specify, in writing, the adjusted estimated activation timeframe.

(1) To implement this change in status, the local SSO must submit a caretaker status request to DAC for review and approval; with a copy forwarded to the HICE or designee. Upon notification, DAC will issue the appropriate caretaker status correspondence. Once approved, the local SSO must verify all SCI material and systems were completely removed from the SCIF. If any other classified materials are to remain, that information must still be protected in accordance with the applicable policy and regulations. At a minimum, the area under caretaker status should be controlled to limit access to authorized personnel only. These controls may include, but are not limited to, key-lock devices, alarms systems, escorts, and construction surveillance technicians.

(2) Reinstituting a facility's SCI accreditation can be accomplished by the SSO submitting an updated FFC or official correspondence requesting reaccreditation to DAC. If no requests for accreditation are made or if the requests are not received within the authorized timeframe, DAC will automatically disestablish caretaker status and withdraw the SCIF identification number.

6. SCIF OPERATIONS

a. Co-utilization of SCIFs

(1) Co-utilization of existing facilities promotes efficiency and achieves financial savings. Elements desiring to co-use a SCIF will accept the current accreditation and any waivers. A co-utilization agreement (CUA) will be established prior to occupancy and any differences shall be resolved prior to its acceptance.

(2) The CSA, their designee, or the DoD Component SIO may coordinate and approve CUAs with other DoD Components (excluding NRO, NGA, and NSA), to include their SCI-related SAPs. In these instances, courtesy copies of the CUAs will be furnished to DAC.

(3) DAC will coordinate CUAs on behalf of DIA with non DoD IC agencies, NRO, NGA, and NSA, to include their respective SCI-related SAPs. In these instances, the CUA will be processed by DAC.

(4) The CSA for the SCIF maintains oversight of the facility unless all parties agree to transfer CSA responsibility. If a transfer occurs, all accreditation records will be furnished to the new CSA and all appropriate organizations will be notified. The gaining CSA will issue a new accreditation or provide written confirmation of the transfer of the facility.

(5) Planned modifications, to include additions of IS or electronic processing equipment, must be approved by the CSA in advance. Before using this equipment for SCI, appropriate accreditations (i.e., TEMPEST and IS) must be obtained from authorized IS accreditation and TEMPEST technical authorities.

b. SAPs Within DIA-accredited SCIFs

(1) Facilities housing SCI-related SAPs shall meet the physical security requirements of Reference (g). Any physical security measures above those described in Reference (f) required by SAP managers should be negotiated between the SSO and SAP security personnel.

(2) If only part of the SCIF will be used for the SAP, it will be treated as a compartmented area in accordance with Reference (f) and a CUA must be established prior to the introduction of a SAP (SCI or non-SCI) into the SCIF. Copies of the CUA will be provided to each signatory and DAC. A CUA for a SAP that occupies several SCIFs will be negotiated between the overall SAP manager and the CSA, their designee, or the DoD Component SIO. The CUA will contain a provision allowing it to be appended by the local SSO and SAP security officer to meet local security conditions.

(3) If the entire SCIF will be used for the SAP, then the SAP program manager will ensure that an individual read on to the SAP is appointed as the SSR and the appointment provided to the SSO as described in Volume 1 of this Manual. The SSO will be responsible for ensuring that SCI is properly protected and for managing the SCIF. The SAP security officer can be the SCIF security officer as long as he or she has SCI and SAP access. The SSR will conduct a self-inspection of their organization's security program and report to the CSA SSO.

(4) If non-SCI SAP material must be stored in a SCIF, a CUA with the SCIF will be completed and include the following requirements:

(a) SAP personnel must meet the eligibility standards for the SAP in accordance with DoDD 5205.07 (Reference (o)) and DoDI O-5205.11 (Reference (p)).

(b) SAP personnel must receive a security briefing regarding protection of the SCI information while in the SCIF.

(c) Non-SCI indoctrinated personnel will be readily identifiable and will be escorted by SCI-indoctrinated personnel while in the SCIF. If access by non-SCI indoctrinated personnel

is required for longer periods of time (e.g., daily), consideration will be given to indoctrinating the individual to SCI.

(5) SCI-SAP materials shall be controlled as SCI and SAP jointly. With the exception of physical security standards, when security standards in this Manual and Reference (p) differ, the more stringent administrative security standard shall be applied. Reference (f) shall regulate physical security standards.

(6) The CSA, his or her designee, or the DoD Component SIO may coordinate and approve, with other DoD Components (excluding NRO, NGA, and NSA), the introduction of DoD SAPs into their respective SCIFs. DIA will coordinate joint authorization with the respective DoD SAPCO for any introduction of SAPs with SCI content from non-DoD IC agencies into a DoD SCIF. The DoD SAPCO will coordinate with the non-DoD agency SIO, their designee, and DIA (if accessed) in approving any introduction of DoD SAPs with SCI content into a non-DoD IC agency SCIF.

(7) The SSO for the SCIF and the SAP manager must maintain open communications. The SSO is responsible and accountable to the SIO for the management of the entire SCIF, while the SAP manager is responsible for administration of the SAP. The SSO can enter into the SAP compartmented area of the SCIF to verify physical, technical, TEMPEST, and other security conditions that may affect the integrity of the SCIF. However, to the extent practicable under the circumstances, the SSO should provide advance notice to the SAP manager so that SAP-related materials or operations may be secured in accordance with Reference (o).

c. Photography Within a SCIF

(1) The SSO may approve unclassified photography inside a SCIF. The area must be cleared of visible classified information prior to the photography and the SSO or SSR must monitor all photography and prevent the inadvertent photography of classified information.

(2) The SSO shall ensure photographic equipment used within the SCIF complies with local portable electronic devices policy.

d. End-of-day Procedures. The SSO must establish a system of written end-of-day security checks to properly protect all classified materials and to ensure that the SCIF is secured. Use standard form (SF) 701, "Activity Security Checklist," to record internal security checks at the end of each day that the facility is occupied. Use SF 702, "Security Container Check Sheet," to record the security checks of the SCIF door, vaults, and containers. This form will document openings, closings, and end-of-day checks, to include those occurring after normal duty hours, weekends, and holidays if the facility is supported by non-duty hour checks conducted by a local guard force. If the SCIF is located in a commercial office building or other location where there is unrestricted public access to the main entry door, do not place the SF 702 on the outer door; instead, place it on the inside of the SCIF. Retain both completed forms for 90 days or as required for investigative purposes. A list of items to be checked at end-of-day is included in Appendix 2 of this Enclosure.

e. After-duty-hours Inspections. Unannounced after-duty-hours security inspections are aimed at heightening the overall security posture for an organization by determining if classified materials are properly protected.

(1) Written procedures must be established, and employees must be briefed to SCI, regardless of the size of the SCIF, amount of personnel working within, or location. Procedures shall be tailored to what is or is not possible and practical for the location. Written procedures should be reviewed by the supporting legal office and be endorsed by the respective CSA, their designee, or the DoD Component SIO prior to implementation.

(2) SSO, SSR, or properly SCI-indoctrinated designees will conduct random inspections at least monthly and annotate the inspection for the record. Whenever possible, they should coordinate with the site IAM if time permits.

(3) Security inspections should include computers, magnetic media, multi-media, security containers, desks, file cabinets, bookcases, and other personal items such as personnel carrying briefcases and packages. Inspections within SAP compartmented areas must not occur without appropriate coordination with the SAP CSA, oversight authority, or program manager in accordance with the governing CUA.

(4) Document the results of the security inspection reports and retain for 6 months. Notify the appropriate SCI chain of command and DIA immediately of any SCI-related security violations. After hours inspection reports may be reviewed by a DAC inspector upon request.

f. Emergency Action Plans (EAPs)

(1) General

(a) Each SCIF will establish and maintain an EAP that addresses long and short term situations. Emergency plans will vary in scope and procedures, depending on the SCIF's geographic location and threat. A sample format for EAPs for SCIFs located within the United States is included in Appendix 3 of this enclosure.

(b) Plans should include task cards so that all areas are covered and coordinated. In addition, all assigned or attached personnel will become familiar with destructive devices employed or maintained for such plans.

(c) EAPs involving SCI will be coordinated with or incorporated into the host command's emergency plans. This coordination will provide for the effective and secure evacuation, storage, or destruction in the event of an emergency. Total destruction of priority one material is more desirable than partial destruction of several items.

(d) EAPs will be practiced annually and updated when a change in condition renders a portion of the EAP impossible, infeasible, or unduly burdensome. All personnel must be familiar with the plans and their part in them as either a primary or alternate duty. The SIO or SSO's

annual review must be documented. For contractor SCIFs, the COR or designee of the USG organization who has the contract will validate the EAP.

(e) The SSO, SSR, or CSSR must alert their command SSO and DAC whenever the EAP is activated.

(f) All materials will be identified for emergency destruction or removal by labeling. Labeling can be accomplished by any matter as long as it provides a clear visual means of destruction priority and is consistent throughout the SCIF. Labels should not identify the priority levels (i.e., do not label the security container "Destruction Priority One"), but rather use something generic such as a shape or icon. Priority levels include:

1. Priority One. All cryptographic equipment and related documents.

2. Priority Two. All operational SCI or SAP codeword material and multi-media that might divulge targets and successes, documents dealing with U.S. SCI activities, and documents concerning compartmented projects and other sensitive intelligence materials and TOP SECRET collateral.

3. Priority Three. Less sensitive administrative SCI material and collateral classified material.

(2) Requirements for all EAPs. EAPs will account for fire, natural disaster (e.g., floods, hurricanes, tornados), labor strife, intrusion detection system (IDS) or alarm outage, entry of emergency personnel (e.g., host country police and firemen) into the SCIF, and the physical protection and safety of those working in such SCIFs. Planning should address the adequacy and condition of components necessary to the plan succeeding such as:

(a) Location of fire-fighting equipment.

(b) Assignment of specific responsibilities by duty position, rather than by name, with alternates designated.

(c) Authorization for the senior individual present to implement the plan.

(d) Periodic review of assigned duties by all personnel.

(e) Location of SCI material by storage container.

(f) Location of safe combinations.

(g) Procedures for admitting uncleared emergency personnel into the SCIF and provisions for safeguarding SCI material during such access.

(h) Removal of SCI document accounting records to facilitate the post-emergency inventory.

(i) Emergency evacuation procedures for equipment, material, and personnel, as appropriate.

(j) Emergency storage procedures, if appropriate.

(k) Provisions for precautionary and complete destruction, if appropriate.

(l) Designation of evacuation site and alternate site.

(m) Designation of primary and alternate travel routes.

(n) Provision of packing, loading, transporting, and safeguarding SCI material.

(3) SCIFs Located Outside the United States. In areas where political instability, terrorism, host country environment, or criminal activity suggests the possibility that a SCIF might be overrun by hostile forces, EAPs will provide for the secure destruction or removal of SCI under adverse circumstances, such as loss of electrical power, non-availability of open spaces for burning or chemical decomposition of material, and immediate action to be taken if faced with mob attack. Where the risk of overrun is significant, SCI holdings will be reduced to, and kept at, the minimum needed for current working purposes. In addition to subparagraph 5.f.(2) of this enclosure, the following will be considered:

(a) Location of destruction equipment.

(b) Periodic checks of all incendiary devices.

(c) Minimum retention of SCI material.

(d) Close coordination with, or incorporation into, host command's emergency contingencies.

(4) Precautionary Actions

(a) When a possible emergency is anticipated, action must be taken to reduce SCI holding to the minimum necessary to continue operations. This action will facilitate initiation of the EAP should it become necessary. Precautionary actions could take the same form as emergency actions. The SIO, in coordination with the SSO, determines the material that will be retained to continue effective operations and when to store, remove, or destroy material not required.

(b) If material is destroyed as a precautionary measure, the appropriate issuing office must be advised. This office then can replace the material destroyed when the danger period has passed.

(5) Initiation of Plan. Measures that may be taken in the event of an emergency include evacuation, secure storage, and destruction. For SCIFs located in the United States, evacuation or secure storage shall be considered before destruction.

(a) Evacuation

1. Evacuation will be executed in a systematic manner under the direction of a responsible individual. Every effort will be made to prevent loss or unauthorized access to SCI until the return of the material to its original location or the SCI material is relocated to an alternate SCIF. Factors that may influence the decision to evacuate the SCIF include:

a. Time available.

b. Future requirement for the SCI material.

c. Degree of hazard involved in the removal.

d. Safety of the new location.

e. Means of transportation available.

f. Transportation routes available.

2. When implementation of emergency plans results in abandonment of SCI material, the commander or SIO will make every reasonable effort to recover the material as soon as possible. Recovery will be based on the likelihood of success without subjecting personnel to undue danger. SCI or residue will be collected and placed under the control of SCI-indoctrinated individuals until disposition instructions are received.

(b) Secure Storage. Secure storage consists of securing the SCI material in other SCIFs or safes before evacuating the area. Presence of a guard does not satisfy secure storage requirements; however, placement of guards by stored material is required when possible. Secure storage is not an effective emergency measure overseas in areas under the threat of enemy or terrorist attack. Factors that may influence the decision to secure the SCI area include:

1. Time available.

2. Nature of the emergency (whether by human or natural causes).

3. Seriousness of the emergency.

4. Likelihood of returning to the site.

5. Bulk or weight of the material (in deciding whether to store or evacuate).

(c) Destruction

1. Selection of an adequate destruction method should be based on a comprehensive evaluation of conditions at a specific SCIF. Destruction of SCI equipment should be by one of the following means:

a. Acetylene torches.

b. Incendiaries.

c. Although not as effective, destruction or disassembling, smashing, or scattering components may be accomplished when incendiaries or acetylene torches are not available. Equipment also may be jettisoned into water deep enough to minimize the possibility of salvage.

2. Documents and other flammable material may be destroyed by burning. Kerosene, gasoline, and sodium nitrate are effective means of destroying documents. They should be used with extreme care for personal safety. Documents also may be destroyed by:

a. Pulverizing.

b. Pulping.

c. Enclosing in a weighted, perforated bag, and jettisoning into water deep enough to minimize the possibility of recovery.

(d) Emergency Destruction. Emergency destruction is authorized if a craft containing SCI material or equipment is wrecked or stranded in unfriendly territory, in neutral territory where capture appears imminent, and under any other circumstances when it appears unlikely that the information can be properly safeguarded. SCI material should be shredded or burned as completely as possible and dispersed. SCI equipment should be smashed or burned beyond repair and dispersed.

(6) After-Action Report. The following actions are required after initiation of EAPs:

(a) The SIO will submit a written report as soon as possible to the next higher headquarters, with an information copy to the HICE or designee and DAC. If the action involved an SCI incident, requirements of Enclosure 5 of Volume 3 of this Manual apply.

(b) Reports will, at a minimum, indicate:

1. Material destroyed and method used.

2. Circumstances that caused the plan to be implemented.

g. Off-site Conferences. Conferences, training courses, meetings, or other such gatherings where SCI is presented, disseminated, or discussed is strictly limited to accredited USG or USG-

cleared contractor SCIFs. Classified conferences and similar meetings, at any level, will not be held at hotels or other commercial facilities without Under Secretary of Defense for Intelligence approval.

h. Destruction. Destroy SCI in a manner that prevents reconstruction. Approved methods include burning, disintegrating, crosscut shredding or pulping for paper, and burning, disintegrating, and chemical alteration for non-paper.

(1) Crosscut shredders contained on the NSA Evaluated Products List for High Security Crosscut Paper Shredders (EPL 02-01) for the terminal destruction of communications security (COMSEC) paper products may be used for the destruction of SCI. This list may be obtained from the NSA National Information Assurance Service Center at 1-800-688-6115 (select option 3) or via DSN at 238-4399.

(2) SCIF personnel may continue to use previous NSA-approved shredders for the destruction of classified information, excluding COMSEC material. However, these devices must be discontinued when the cutting heads require replacement. Budget plans for the procurement of a new shredder, conforming to the new standard, should be considered prior to the replacement need.

(3) There is no special requirement for marking shredders with the highest level of classified information they are authorized to destroy.

i. Foreign National SCIF Access. This section prescribes essential safeguards relating to the integration or visit of foreign nationals to include foreign exchange officers, foreign liaison officers, or embedded foreign officers within DIA accredited SCIFs. Any deviations must be addressed with the responsible foreign disclosure officer (FDO), the supporting CI element and be approved by the respective HICE or their designee. If information systems are involved, the DAA for the particular network must give their approval.

(1) Non-SCI-indoctrinated Foreign Nationals. Foreign nationals without appropriate SCI indoctrinations shall not be admitted inside a SCIF unless special approval is obtained in advance by the HICE or designee.

(2) Disclosures to SCI-indoctrinated Foreign Nationals. SCI-indoctrinated foreign nationals may be granted access to a SCIF either as a visitor or an embedded part of the organization per agreement between their government and the USG. However, SCIF access does not constitute approval to release or allow access to any SCI material to a foreign national. Release of SCI materials to foreign nationals must be approved by the responsible FDO in accordance with Director of Central Intelligence Directive 6/7 (Reference (q)). Foreign nationals with SCI access are only authorized access to information releasable to their country at the level to which they are granted access.

(3) SCIF Access by SCI-indoctrinated Foreign Nationals. Whenever SCI-indoctrinated foreign nationals are provided general access to a SCIF as part of their official daily duties, the organization will ensure that compensatory security measures aimed at protecting against the

inadvertent or deliberate release of non-releasable information, both foreign government and USG, is taken and foreign disclosure guidelines must be followed. These measures shall be guided by a risk assessment which weighs the benefit to the USG of foreign national personnel in the SCIF against the risk that security measures will not adequately protect against unauthorized disclosure. Results from this risk assessment shall be provided to DAC for review. A risk assessment for each visit is not required provided one has been done for visits as a whole. The servicing SSO will certify the foreign national's SCI accesses and the following procedures are applied.

(a) Areas within the SCIF will be segregated to the greatest extent practical to minimize the likelihood that foreign nationals are inadvertently exposed to non-releasable information. At no time will they be afforded access to areas where IC information and systems, which are not previously approved for disclosure, are located. Such areas will be protected with adequate physical security devices consistent with IC directives.

(b) Foreign nationals shall not be permitted to escort personnel.

(c) A sufficient amount of U.S. SCI-indoctrinated personnel who can properly monitor the safeguards put into place will be present whenever the foreign nationals are present. Automated or non-automated access control devices should be installed in internal SCIF areas where processing, discussion, and storage of U.S.-only information, material, or systems occur as a layer of internal security. However, such devices cannot be used in lieu of the requirement for sufficient U.S. SCI-indoctrinated personnel.

(d) Unique security procedures must be developed and clearly documented in the local standard operating procedure (SOP). Each U.S. SCI-indoctrinated person working within the SCIF must be briefed annually on the SOP and its contents as part of the Security Awareness Training Program. This program will also include CI training to include the indicators of espionage and insider threat.

(e) Foreign nationals will not be provided access to combinations to the SCIF entrance and exit doors or security containers that contain non-releasable information, and codes or functions associated with the SCIFs IDS or master codes associated with automated access control devices.

(f) U.S. SCI-indoctrinated personnel working within the SCIF must be periodically reminded to consistently exercise caution to protect against the inadvertent release of non-releasable information and to promptly report security concerns and issues. Discussions (person to person, secure telephones, video teleconference (VTC), etc.) offer a great challenge when internal rooms (where conversations are held) are not constructed to a sound transmission class (STC) 45 level, or STC-50 if the room is used for VTC (amplified audio). These standards essentially are reached when loud speech amplified audio can be faintly heard, but cannot be understood in immediate adjacent areas.

(g) U.S. SCI-indoctrinated personnel must take appropriate measures to secure non-releasable documents when not used, preferably in an approved security container.

(h) Computer displays for classified systems must be positioned to afford adequate screening and password protection for screen savers must be applied. Consult with local IAM for further IS security guidance.

(i) Printers connected to U.S.-only systems, faxes, etc., must be located in an area that affords the greatest amount of U.S. controls.

(j) Inform any co-use agency operating within your SCIF about the presence of the foreign officers, and consider, as appropriate, notifying security officials in adjacent areas outside the SCIF.

(k) Foreign nationals granted access to IS must comply with Reference (n).

(4) CUA with Foreign Governments. A CUA, based on the governing bilateral SCI agreements between the U.S. and appropriate foreign government, is required for DoD SCIFs resident within a foreign government SCIF and for foreign government SCIFs within a DoD SCIF. Accreditation and oversight of such DoD facilities remains with DAC. The following additional guidelines apply:

(a) Procedures for controlling access (access rosters, badges, access control device codes), hours of access, restrictions on the introduction of prohibited items, protocols for visits, access to U.S.-only areas within the SCIF, destruction of classified waste, and other appropriate SCI security guidelines required to maintain positive control of U.S. SCI information, material, equipment, operations, and sources and methods must be documented in the CUA.

(b) FDO concurrence shall be obtained before finalizing the CUA to meet the provisions of DoDD 5230.20 (Reference (r)) for the country concerned.

(c) A copy of the CUA will be forwarded via secure channels (e.g., messaging, secure fax, or secure e-mail) to the appropriate HICE or designee.

(d) Physical security guidelines contained in this enclosure must be followed. Careful attention must be given to ensure unencrypted classified communication lines do not transit the area exclusively occupied by the foreign nationals.

(e) The local supporting SSO (through the SSR) will monitor the execution of the CUA and report violations and security concerns to both the FDO and respective CSA and SIO. The CSA will advise the HICE and provide recommended corrective actions as appropriate. The CSA shall report security incidents to the head of the appropriate element of the IC in accordance with Enclosure 5 of Volume 3 of this Manual.

j. IDS. IDSs will comply with basic requirements contained in References (g) and (h) unless otherwise approved by DAC. The following additional guidelines are provided:

(1) Underwriters Laboratories (UL) 2050 Standards for USG or Contractor SCIFs. All IDS installed in DIA accredited SCIFs will meet UL 2050 standards, unless otherwise approved. Contractor SCIFs are required to have a UL 2050 certificate. UL 2050 certification is not required for USG SCIFs utilizing USG-managed systems until the monitoring or IDS head is replaced. A copy of the UL certificate must be provided to DAC. USG SCIFs are not required to have a UL certificate if the alarm system was installed by USG alarm technicians. If the alarm system was installed by a contractor, a copy of the UL 2050 certificate is required.

(2) Use of Existing IDS Systems on U.S. Military Installations. IDS located on U.S. military installations and accredited under the previous guidelines (Reference (q), which was superseded by Reference (f)) may continue to be used until a major modification is made.

(3) Line Supervision. Line supervision for all intrusion detection equipment (IDE) components of an IDS (USG and contractor facilities) will employ 128-bit (or greater) encryption whenever the signal line leaves the SCIF. This includes signal lines between any IDE, premise control unit (PCU), and monitoring stations. All lines employing line supervision require certification of the algorithm by the National Institute of Standards and Technology (NIST) (i.e., a NIST certificate). An alternate form of line supervision may be approved on a case-by-case basis.

(4) Monitoring Stations. Monitoring stations must be continuously supervised and staffed by U.S. personnel. These personnel do not need to be SCI-indoctrinated unless the system was configured to allow them to reset or shunt an alarm condition.

(5) Alarm Response Times. Response time is based upon accreditation and security-in-depth. If the response force cannot meet the required response time, additional security requirements (i.e., additional barriers, adding cameras, going to closed storage) must be added.

k. Government-owned, Contractor-operated (GOCO) SCIFs. The GOCO SCIF will be accredited as a USG facility. The local SIO must ensure that the contractor operating the facility meets the industrial security requirements outlined in Enclosure 3 of Volume 3 of this Manual.

Appendixes

1. SCIF Closeout Guidelines
2. SCIF End of Day Security Check
3. EAPs for SCIFs within the United States

APPENDIX 1 TO ENCLOSURE 2

SCIF CLOSEOUT GUIDELINES

1. Inspect storage containers and furniture. Remove and inspect each drawer, leaf, or part, including areas under drawers and cushions or other parts that might conceal classified material. Ensure the container or furniture does not contain classified, official, or Government-related material.

2. Reset combination safes to the manufacturer's setting (50-25-50) and lock them.

3. Lock key-lockable containers and tape the key to the drawer or door handle.

4. Affix a certification form (may be locally produced) that reflects the date of inspection, name and signature of inspector, and a statement that the inspector certifies that classified, official, or Government-related material is not contained therein. Remove the form when the item is reissued or released outside the agency.

5. Remove typewriter and printer ribbons and dispose of them as SCI material.

6. Ensure reproduction equipment does not contain classified information or latent images of such.

7. Dispose of SCI equipment and media, including hard drives and portable storage media, according to approved procedures and request withdrawal of AIS security accreditation. Coordinate these actions with the site IAO.

8. Inspect entire SCIF to ensure all SCI material has been removed, properly disposed of, or destroyed.

9. Request accreditation withdrawal from accreditation authority.

10. Receive formal withdrawal from accreditation authority.

11. If facility will be used for another mission or project that requires alarms, transfer alarm service to the new activity. If facility will not be used for another mission or project, discontinue the alarm service, including removal of alarms and the wiring system.

12. If applicable, change the combination on the entrance door to 50-25-50, and account for all keys.

13. Debrief personnel, if required.

APPENDIX 2 TO ENCLOSURE 2

SCIF END OF DAY SECURITY CHECK

1. The individual assigned to conduct the SCIF security check for the day will check the following items (as required).

a. Check SF 702 to ensure all appropriate entries for locking and checking has been made for each security container.

b. Check desk tops, cabinets, and safe tops, shelves, stands, tables, and other furniture and equipment for unsecured classified material.

c. Check wastebaskets for classified material. Ensure all burn bags are properly secured.

d. Check typewriters to ensure that all typewriter ribbons used in the preparation of classified material have been removed and secured.

e. Check AIS, word processing, or recording equipment to ensure all recording media have been removed and properly stored.

f. Check charts, maps, blackboards, clipboards, and other items hanging on the walls that might contain classified information.

g. If applicable, check all windows and access to ensure they are properly secured.

h. Check the intrusion detection system, if applicable, to ensure that it is properly set and activated.

i. Check other items on SF 701. Initial the form when checks are completed.

j. Check SF 702 at the SCIF entrance to ensure that the “locked by” and “checked by” columns have been completed. Recheck the door to ensure it is locked.

APPENDIX 3 TO ENCLOSURE 2

EAPs FOR SCIFs WITHIN THE UNITED STATES

CONUS EAPs shall conform to the format as indicated in the Figure of this Appendix.

Figure. Sample EAP Format

This Emergency Action Plan (EAP) establishes policies, outlines responsibilities and general procedures for (organization) personnel for the safeguarding, evacuation or destruction of SCI and other classified material during emergency situations. This plan is required for Sensitive Compartmented Information Facilities (SCIF) by DoD 5105.21-M-V2 and will be reviewed at least annually with the review annotated at Attachment 11 of this EAP.

1. GENERAL. A potential enemy is capable of conducting bombing or guided missile attacks, conventional or nuclear, without warning. The (organization) office could be affected by a natural disaster occurring on or near (location) caused by earthquakes, windstorms, explosives, epidemics, fires, strikes, riots, or any combination thereof.

a. Assumptions. That it is possible for this unit's facility to be rendered inoperative, either totally or partially, by enemy attack, acts of sabotage, or by natural catastrophes such as fire, wind, flood, earthquake, etc.

b. Threats. All forces, man-made or natural, that are capable of endangering life and property, and disrupting civil and military control or leadership.

c. Friendly Forces. U.S. Military Forces in the vicinity of (location).

2. MISSION. To safeguard personnel and property; to restore the essential operations of (organization). To establish actions necessary to prevent loss or compromise of classified information in emergency situations.

3. EXECUTION

a. Concept of Operations. (Organization) is not manned or equipped to cope with fires or other emergencies of any magnitude. Major disasters could destroy the capability of this office to carry out essential functions of the present location. The intent of this plan is to assure that, in the event of any emergency, immediate action is taken to safeguard and assist (organization) personnel to minimize property damage or loss and to prevent loss or compromise of classified information. Lists of actions to take in the event of possible emergency situations are attached.

b. Task of (Organization) Personnel

(1) (Organization) personnel will be prepared to implement this plan upon notification by the appropriate (organization) or local law enforcement personnel.

(2) (Organization) personnel will be familiar with defensive readiness conditions (DEFCON) procedures and responsibilities.

c. Coordination. This plan has been coordinated with (organization) collateral security office, local military police organization, local fire protection organization, and local Special Security Office.

4. Emergency Evacuation Support. Support for emergency evacuation will be provided by (organization) per Attachment 1.

5. Fire Protection Support. Support for fire protection will be per Attachment 4 and local military police and local fire protection personnel. Support for Bomb Threats will be per Attachment 5 and local military police.

Signature of Local SCI Security Official Date

Signature of Local Commander Date

ANNEXES

A. Emergency Destruction Procedures
B. Fire Protection
C. Bomb Threat
D. Natural Disasters
E. Sabotage or Terrorist Attack
F. Riots or Civil Disorders
G. Loss of Utilities
X. Additional Annexes as Needed

ATTACHMENTS

1. (Organization) Evacuation Rally Point Maps
2. Emergency Transportation or Material for Destruction Plan
3. Emergency Exit Routes
4. Fire Protection
5. Bomb Threat Checklist
6. Emergency Phone Numbers
7. Notification Alert Checklist-Evacuation
8. Notification Alert Checklist-Emergency Destruction
9. Notification Alert Checklist-Secure Storage
10. Notification Alert Checklist-Fire Notification
11. Annual Review of EAP by Assigned Personnel Signature Sheet
X. Additional Attachments as Needed

ENCLOSURE 3

VISITOR CONTROL

1. GENERAL. The SSO is the primary POC for verification of SCI accesses. Use of the approved DoD clearance verification system (i.e., Joint Personnel Adjudication System (JPAS) or the IC Security Clearance Repository (Scattered Castles)) is the preferred method for verification of clearances and accesses.

a. The host facility will limit the access of visitors to areas and information to that required for official business. The host of a classified conference, meeting, discussion, or video teleconference is responsible for verifying the identity, access, and need to know of each person prior to disclosure of any classified information. The host will advise all attendees of the access level and dissemination controls or restrictions for the meeting. Access verification procedures will be established by the local SSO.

b. Individuals visiting a facility in which there is no capability to verify accesses using JPAS or Scattered Castles are responsible for requesting their SSO certify their security clearances and accesses to the host facility well in advance of the meeting. Visitors who have not been certified or are not reflected within JPAS or Scattered Castles, regardless of the affiliation or position of the visitor, will not be allowed access to SCI. Entrance to SCI facilities requires escort control until certification is obtained.

2. BADGE RECIPROCITY IN THE METROPOLITAN WASHINGTON, D.C., AREA (MWA)

a. Selected agencies of the IC in the MWA have signed MOAs granting official badge reciprocity privileges to personnel visiting their facilities. This precludes the requirement to validate clearance and access via JPAS or Scattered Castles. The SSO will establish local procedures to maintain need to know by the visitor's sponsor. Personnel should consult their local SCI security official for details.

b. The IC Badge Interoperability Program streamlines facility access throughout the IC. The badge is issued only to fully adjudicated and indoctrinated Government civilian personnel, assigned U.S. Military personnel, and USG contractor personnel and is accepted as evidence of security clearance and access authorization at the TOP SECRET//SI/TK level. Personnel granted SCI based on an interim are not eligible to receive this badge.

3. CERTIFICATION OF CLEARANCES AND SCI ACCESSES. The SSO will retain a record of certification for the duration of the visit for personnel who do not appear in JPAS or Scattered Castles.

a. SSO Certifications. The SSO may approve permanent certifications of DoD personnel and contractor personnel not to exceed 36 months or duration of the contract, whichever is less. Duration of contract refers to the base year(s) or period of the contract. Certifications will not include optional years or period until the option is officially accepted by the USG. SSOs are authorized to certify SCI accesses directly to a CSSO. If an individual is debriefed from access while permanently certified, the SSO will immediately update JPAS and cancel all certifications of the individual.

b. CSSO Certifications

(1) The CSSO is authorized to certify TS/SI/TK clearances and accesses to the DoD Components, less NSA, and other DoD contractors, as specified in subparagraph 3.b.(2) of this enclosure, for contractor personnel for whom they maintain documented proof of indoctrinated status. The certifications will not exceed 36 months or duration of the contract, whichever is less; CSSO certifications to the NRO are limited to 12 months or duration of contract, whichever is less. Duration of contract refers to the base year(s) or period of the contract. Certifications will not include optional years or period until the option is accepted by the USG. Documented proof may include JPAS or Scattered Castles entry, access rosters or other access notifications provided by the supporting SSO, contractor indoctrination records if the CSSO is authorized to conduct indoctrination briefings, or other documentation that certifies SCI access. SCI accesses other than SI/TK will be certified through the supporting DoD SSO.

(2) The following CSSO certifications do not require COR approval:

(a) Visits to DoD activities, less NSA, to receive briefings based on DoD's determination of need to know.

(b) Attendance at conferences or symposia where the contractor will not present information.

(c) Visits to other DoD contractors where there is a contractual relationship as determined by the COR and stated in DD Form 254 or other written documentation.

(3) The following CSSO certifications require COR approval. COR approval shall be specified in DD Form 254 or provided in separate written documentation:

(a) Visits to DoD activities, less NSA, to present contract-generated information.

(b) Visits other than those specified in subparagraph 3.b.(2) of this enclosure.

(4) Visit certifications for contractor management, pre-contract, or technical personnel must be at the USG's request or based on contractual relationship between two companies.

(5) Upon notification from the USG CSA that an individual's SCI accesses have been suspended or terminated or upon departure or reassignment of an individual from the specified contract, the CSSO will immediately cancel all certifications and immediately notify the USG

CSA or supporting SSO, as appropriate, of such action. Individuals will be debriefed as appropriate.

(6) Contractor implementation of access certifications will be reviewed during USG inspections and staff assistance visits.

c. Certification Content. If an individual's accesses are not in the approved DoD clearance verification system, the following applies: Certifications will include the person's name; social security number; clearance level and SCI accesses; dates of visit; purpose of visit, including company name and contract number if applicable; and the name and telephone number of the POC at the visit location. CSSOs will include their name and telephone and will use official company stationery.

d. Certification Transmission. Certifications may be transmitted electronically or by facsimile consistent with the security classification of the information. Certifications will include the statement "This message contains compartmented access certifications. Release of information is limited to personnel authorized commensurate degree of access. Disregard digraphs and trigraphs not authorized to your facility."

e. Certification Classification. Certifications using the authorized DNI digraphs and trigraphs are normally unclassified. Digraphs and trigraphs should be disclosed only to personnel who understand the sensitivity and requirement for appropriate protection. Certain circumstances such as the relationship of two organizations may require classification of the certification. The SSO will provide SCI-briefed personnel cognizance of operational security concerns and potential classification when digraphs and trigraphs are associated with program information, activities, or locations.

f. Certification Extension. Circumstances may occur that alter a travelers' scheduled arrival or departure date at an official temporary duty (TDY) location. Receiving SSOs will honor alteration to visit certifications based on the following:

(1) At the request of USG and contractor personnel, receiving SSOs will honor visit certifications up to 2 calendar days prior to the beginning date on the visit certification. Early arrival must be for the same purpose as stated in the visit certification.

(2) At the request of USG personnel, receiving SSOs will extend visit certifications at the TDY location for a period not to exceed 7 calendar days beyond the last date of the original certification.

(3) For contractor personnel, the POC at the TDY location, as named in the original visit certification, may determine the need to know for the contractor to extend the visit, not to exceed 7 calendar days beyond the last date of the original certification. Extensions of visit certifications for contractors must be for same purpose as stated on the original certification. Extensions will not be granted for non-related purposes.

g. Emergency Certifications. Under emergency conditions, the SSO may certify SCI visit certifications for assigned personnel by telephone to another SSO.

h. Recertification Authority. Recertification authority exists to allow USG and contractor employees on official TDY to accomplish their mission. Circumstances may arise at a TDY location that requires an employee to visit other organizations for official business. DoD SSOs are authorized to recertify USG and contractor personnel clearances and SCI accesses to organizations within the SSO's local travel area. The POC at the TDY location, as named in the original visit certification, may determine the need to know for the contractor to visit another organization. COR and CSSO approval is not required for such recertifications. Recertifications will not exceed 7 calendar days beyond the last visit date of the original visit certification. Recertification by CSSOs is not authorized.

i. Visits to Foreign-owned Facilities. For DoD military, civilian, and contractor personnel visiting foreign SCIFs, SCI accesses will be certified to the appropriate HICE or designee as part of the liaison visit approval process. Adequate lead-time must be provided to recertify SCI accesses to the appropriate agencies. Contractor visit requests must specifically identify the type of work being accomplished and how it relates to the SCI contract.

j. Visits by Members of Congress. See Enclosure 4 of Volume 3 of this Manual.

4. VISITS BY FOREIGN NATIONALS. In addition to the requirements outlined in DoDDs 5230.20 and 5530.3 (References (r) and (s)), visitor access to U.S.-controlled SCIFs by foreign nationals will be approved by the activity's SIO based on operational need. Foreign national access to U.S.-controlled SCIFs for an open house, tour, orientation visit, or similar activity is prohibited unless specifically approved by the appropriate HICE or designee, Combatant Command SIO, or another appropriate IC authority (e.g., the Director, NSA).

a. Certification. The appropriate HICE or designee will certify to the servicing SSO the SCI accesses of foreign nationals authorized to visit DoD-accredited SCIFs. Any other certifications are invalid and will not be accepted. The servicing SSO will certify the accesses locally to the appropriate SCIFs being visited.

b. SCIF Access. SCIF personnel will maintain a low profile of SCIF functions and activities to preclude expectations or requests for access. The following procedures apply:

(1) Keep the number of foreign nationals to a minimum. Give the local SCI security official a minimum of 24 hours advance notice of the visit.

(2) Sanitize the SCIF and brief all SCIF personnel prior to the entrance of the foreign national to not conduct or discuss SCI or mission business during the visit. The existence of clandestine, SAP, or other sensitive operations in the facility must not be exposed or otherwise acknowledged to the visitor(s).

(3) Issue foreign visitors escort required badges and keep them under escort at all times.

(4) The SSO shall monitor the use of electronic equipment within the SCIF so that it complies with the established policies.

(5) Record the names of the visitor(s) as required by paragraph 10.b. of this enclosure. VIP visitor(s) are not required to sign the register, but their names will be recorded after the visit.

5. FOREIGN LIAISON AND INTEGRATED PERSONNEL. Foreign government representatives' access to classified information is governed by the terms of accreditation in the agreement between the United States and the represented foreign government and in accordance with Reference (r).

6. CERTIFICATION FOR PART-TIME EMPLOYMENT. The SSO may certify SCI accesses for DoD employees working part-time for a USG contractor. The certification will not exceed one year and will be certified to the CSSO. Only the accesses required to perform the duties of the contract are authorized for certification.

7. NON-INDOCTRINATED PERSONS

a. SCIF access by non-SCI-indoctrinated persons is discouraged. SCIF personnel should conduct official business with non-indoctrinated visitors outside the SCIF. When necessary to grant SCIF access to non-indoctrinated persons (e.g., for building or equipment maintenance), secure all SCI material, including any SCI displayed on IS; do not discuss SCI; and assign an escort to the visitor. Inform SCIF personnel, either verbally or through visual notification methods that the facility will be non-secure. Notify SCIF personnel when the non-indoctrinated persons have departed. A flashing or rotating light is an excellent measure to indicate the continued presence of non-SCI-indoctrinated personnel in the SCIF. Non-SCI indoctrinated personnel should not be granted unescorted access or permitted to use the SCIF as a primary or alternate work site.

b. Open houses, promotion ceremonies, family orientations, etc., in DoD SCI areas will be held to a minimum to reduce security risks. The organization SIO may authorize, in writing, such events based on a justification explaining why the proposed function or visit must be in a DoD SCI area.

(1) Security procedures will be implemented to prevent the unauthorized disclosure of classified information.

(2) All SCIF personnel must receive a security awareness briefing prior to the visit on what can be revealed to visitors either as part of a briefing or in response to questions and to inform them of the special security procedures for the event.

(3) Visits will be limited to sanitized administrative, conference, equipment rooms, and operations rooms. Visits are not permitted in communications centers. Areas not part of the tour will be clearly delineated and persons indoctrinated for SCI must be stationed so that no visitors enter.

(4) Visitors, regardless of age, will be escorted at all times.

(5) SCIF access logs must be kept on all visitors in accordance with paragraph 10.b. of this enclosure.

(6) The SSO shall monitor the use of electronic equipment within the SCIF so that it complies with current policies.

8. CONTRACTORS AND CONSULTANTS. DoD contractors and consultants who have TOP SECRET/SCI access may be given unescorted access to or be allowed to work alone in DoD SCIFs if all proprietary information or other special program materials to which the contractor may not have access under the terms of the contract are secured, as appropriate.

a. The contractor must possess a final TOP SECRET security clearance and be indoctrinated into SCI in order to be left alone within a SCIF.

b. The statement of work or DD Form 254 must authorize the contractor to work past routine working hours as they are described in the contract. The CORs concurrence is required prior to allowing contractors to work past routine working hours.

9. ESCORTS. Only DoD civilian, military personnel, and contractors whose principal place of work is within the SCIF are authorized to escort non-indoctrinated USG and contractor personnel within the USG SCI area. Within contractor facilities, contractor personnel with the appropriate SCI accesses will escort non-indoctrinated persons. Individuals must be thoroughly briefed on their responsibilities as an escort prior to performing the duty.

a. Escorts will announce that an uncleared visitor is in the area; so that co-workers turn over, cover, or store classified material; walk with the individual under escort; and visually observe the individual under escort until the visitor leaves the SCIF or another escort assumes the duty.

b. Waivers to escort policy and procedures may be granted by the HICE or designee on a case-by-case basis.

10. ACCESS CONTROL. Technical specifications published under Reference (f) provide physical access control standards. Access controls for a SCIF should be tailored to fit the local threat, the number of personnel requiring access, the geographic location of the SCIF, and the ability of the hosting organization to provide support. Visitors will be positively identified.

a. Access Rosters. Access rosters listing all persons authorized access to the facility will be maintained at or near the SCIF point of entry. Electronic systems, including coded security identification cards or badges, may be used in lieu of security access rosters. Access rosters will contain the following data elements: name, rank or grade, service, social security number, organizational unit, security clearance, and level of SCI access using only authorized digraphs/trigraphs (such as SI/G/TK). Access rosters are marked "FOR OFFICIAL USE ONLY" and are annotated as containing Privacy Act data.

b. Visit Certifications. Each SCIF will have written procedures for identifying and controlling visitors and will maintain a visitor log with the following information: name of visitor, organization, citizenship, purpose of visit, POC, and date/time of the visit. Visitor logs shall be marked "FOR OFFICIAL USE ONLY." Retain visitor logs for 1 year after the date of the last entry.

ENCLOSURE 4

TECHNICAL SECURITY

1. GENERAL. This enclosure provides basic information and requirements relating to TSCM support and TEMPEST accreditation.

a. TSCM involves techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to National Security Information (NSI), restricted data, and sensitive but unclassified information.

b. TEMPEST is a short name referring to investigation, study and control of compromising emanations from telecommunications and automated IS equipment. The aim is to minimize the likelihood that these emanations will ever be intercepted by adversaries of the United States.

2. TSCM SURVEYS AND EVALUATIONS

a. Overview. The technical surveillance threat to sensitive defense information is real. Technical surveillance devices have been discovered in U.S. facilities worldwide. A technical threat to classified information and controlled unclassified information is posed by foreign intelligence services and others, to collect information from sensitive U.S. facilities and activities or against select individuals. Technological advances make the detection of technical surveillance devices and technical security hazards possible only by highly trained personnel using specialized techniques and equipment.

(1) TSCM threats are generally categorized into three basic levels:

(a) Technical Penetration. The deliberate compromise of information using technical means.

(b) Technical Hazard. The unintentional but exploitable transmission of information from the activity.

(c) Security Vulnerability. Any condition that would facilitate the penetration or exploitation of the activity.

(2) Due to limited resources, once TSCM support is requested it could be quite some time before contact by a TSCM technician for coordination. In some instances, there may be no contact by the TSCM team prior to the date the support begins in order to accommodate OPSEC requirements and planning.

(a) OPSEC is paramount to a successful TSCM support. Any discussion, announcement, or e-mail concerning the TSCM support within the area to be inspected may alert an adversary monitoring the area and allow them to thwart detection by turning off devices and

possibly removing them from the area until after the TSCM team departs. Therefore, knowledge of the scheduled support must be kept to a minimum, and any planning surrounding it should be made in a secure location outside the facility.

(b) A number of factors or events will nullify the TSCM investigation, and should be considered during coordination.

1. Ongoing or planned construction or renovation of the inspected area.

2. Ongoing or future introduction of new equipment or furniture into the area.

3. Current or future unaccompanied access by uncleared persons.

4. Compromise of the TSCM team or mission OPSEC.

(c) The TSCM team will investigate the area or activity using a least-alerting to most-alerting sequence of events to maximize OPSEC and probability of detecting. It is ideal for personnel who work in the area to ignore TSCM agents during the initial investigation and continue normal operations.

(d) TSCM team members are authorized unescorted access to the area being investigated. All agents hold a current TOP SECRET security clearance with SCI access. If a read-on to a SAP is necessary, this should be accomplished prior to the mission. The complexity and time required to complete a TSCM investigation requires advance coordination to satisfy approval for all required compartments/programs.

(e) The TSCM investigation is intrusive in nature. TSCM team members will try to minimize interference with normal activities. Facility personnel must not be alarmed that TSCM team members may be present or monitoring meetings or business of a sensitive or confidential nature. It is during these activities that a listening device will most likely be active and can be better detected by the TSCM team. The security and privacy of personnel working within the facility will be honored.

(f) DO NOT alter work schedules based on conduct of a TSCM investigation or presence of TSCM personnel. This may alert personnel engaged in illegal monitoring of the facility.

(g) The TSCM team may have a large amount of equipment and will need a secure space within the facility to securely store it. This equipment will be permitted inside the SCIF without delay.

b. TSCM Support Requirements. Any area where SCI is discussed or processed should be considered for TSCM support to the greatest extent possible. Priority of support must be threat-driven due to the limited resources available to conduct TSCM evaluations.

(1) Routine Requests. Routine evaluation requirements must be considered when there is new construction or major renovation of a SCIF. There is no requirement that SCIFs located within the United States and its territories must be swept prior to accreditation, although support should be requested as soon as possible. Priority for support is given to SCIFs located in high-threat areas such as deployed and OCONUS environments. For these facilities, TSCM support shall be scheduled upon accreditation of the SCIF.

(2) Emergency Requests. If there is evidence of physical, technical penetration, or monitoring, the SSO will immediately:

(a) Cease classified discussion and activity to the greatest extent possible, while preserving OPSEC.

(b) Strictly limit the number of individuals with knowledge of the event.

(c) Promptly report the incident in accordance with ICD 701 (Reference (t)).

(d) Include preferred methods of notifications to program manager, CI office, and DAC (e.g., secure telephone, secure e-mail, message, or fax). Notify DAC as soon as possible, ensuring this notification does not negatively impact any ensuing investigation. Provide the SCIF DIA designation, what happened and when, and pertinent information. Transmit this information via secure communications from a location other than where the problem exists.

(e) If a suspected surveillance device is discovered, leave it in place and continue normal office activity until guidance is obtained from the supporting counterintelligence office or TSCM activity, and DAC.

(3) Coordinating TSCM Support. The DoD Components and DoD contractors should request TSCM evaluations through their respective TSCM program managers. In the event this is not possible, requests should be sent to DAC. When preparing the request, follow the format required by the supporting activity as listed in the TSCM support activity regulations and instructions.

(a) USA – Army Regulation 380-27 (Reference (u)).

(b) USAF – Volume 3 of Air Force Instruction 71-101 (Reference (v)).

(c) USN and USMC – Secretary of the Navy Instruction 3850.4 (Reference (w)).

(d) The Joint Staff – Joint Staff Manual 5220.01A (Reference (x)).

(e) OSD – Administrative Instruction 30 (Reference (y)).

(f) All other DoD Components – DoDI 5240.05 (Reference (z)).

(g) DoD Components of the IC-ICD 702 (Reference (aa)).

(h) The Combatant Commands. Contact the supporting counterintelligence office to determine the applicable TSCM support activity.

(i) Contractors. Contact DAC.

(4) TSCM Reports. A copy of all TSCM reports shall be retained in the local SCIF files until superseded by a new report. Additionally, a copy of these reports shall be provided to DAC. Any physical security recommendations identified by TSCM personnel that affect the physical security or technical security (TEMPEST) of a DIA accredited SCIF must be validated by DAC prior to implementation or expenditure of funds.

c. Classifying TSCM-Related Information. Classification guidance related to TSCM inspections of SCIF spaces is maintained on the DAC JWICS website (http://www.dia.ic.gov/homepage/da/security/field/index.html).

3. CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

a. Accreditation Authority. DAC is the TEMPEST accreditation authority for DoD SCIFs processing SCI, with the exception of those under NSA, NGA, and NRO cognizance. Officials delegated the authority to accredit T-SCIFs are responsible for ensuring those facilities meet the TEMPEST requirements of section 6 of the National Security Telecommunications Information System Security Advisory Manual 2-95 and 2-95A (Reference (ab)).

b. TEMPEST Accreditation Overview

(1) Each SCIF requires a TEMPEST countermeasures review (TCR), performed by DAC CTTA, as part of the SCIF construction process. Based on the results of the TCR, the CTTA shall determine the most cost-effective countermeasures that will contain the compromising emanations within the inspectable space and will document these requirements in writing. These TEMPEST countermeasures are based upon risk management principles using factors such as location, volume of information processed, sensitivity, and perishability of information, physical control, and the TEMPEST profile of equipment used.

(2) The CTTA will issue the TEMPEST accreditation upon acknowledgment by the facility that the countermeasures have been implemented. The TEMPEST accreditation remains valid until such time that a major modification of the facility occurs or the TEMPEST profile of the facility changes.

(3) A major modification is anything that changes or negates a TEMPEST countermeasure. Examples of a major modification would include changing the SCIF‘s overall space, adding RED equipment, changing the locations of transmitters, altering the building’s construction and any change affecting the RED/BLACK separation. An explanation of RED/BLACK separation principles is listed in subparagraph 3(c)(2) of this section.

(4) A change in the TEMPEST profile is anything that will alter the inspectable space, the level of TEMPEST threat, or the technology used to electronically process the SCI. This may include having a foreign entity move in next to the facility, having the local threat levels change, moving a transportable SCIF into an existing structure, changing from separate equipment for each classification to a single multi-level processing device, or adding secure video teleconferencing capability, etc. Electronic processing of SCI shall not occur until this accreditation is obtained. The TEMPEST accreditation satisfies one of the three accreditations required for a SCIF that will process SCI electronically. The other two are physical security and IT accreditation (see Enclosure 2 of this Volume and Enclosure 5 of Volume 1 of this Manual).

(5) The local SSO will use the TEMPEST addendum to the FFC to request a TCR. For an initial TCR, the addendum will be submitted to DAC during the planning phase of the construction. While some specific information may not be known prior to construction, as much information as possible must be provided in order to minimize costly changes. After the SCIF receives its initial TEMPEST accreditation, any modification to the facility must be documented as a modification and sent to DAC. Place an asterisk adjacent to each item changed in the addendum and date each page. Any changes to section A, administrative data, should be sent to DAC and marked as a "page change."

(6) The commander or corporate officer with oversight responsibility for a SCIF must assure compliance with TCR requirements. DAC must be contacted for additional guidance whenever a TEMPEST requirement (i.e., RED/BLACK separation guidance or TCR countermeasure requirements) cannot be implemented. The Department or agency head or their designee may elect not to apply a requirement; however, they must document this decision in writing based upon their acceptance of the risk of compromise. A copy will be sent to DAC prior to the facility receiving its TEMPEST accreditation.

(7) DIA may require SCIFs that have limited inspectable space, or plan to use equipment with known or suspected high TEMPEST profiles, to have an instrumented TEMPEST evaluation performed as part of the TCR.

(8) A copy of the TEMPEST addendum, the TCR, and any other accreditation material will be made available to inspectors upon request.

c. General TEMPEST Protection Overview

(1) Countermeasures. TEMPEST countermeasures (TEMPEST-suppressed equipment, radio frequency (RF) shielded enclosures, filters (power, signal, telephone, etc.), nonconductive conduit or duct sections, or other potentially expensive TEMPEST countermeasures) will not be applied without DAC approval. Normally, SCIFs located on military installations within the United States do not require additional countermeasures beyond their inspectable space and implementing RED/BLACK separation guidance. However, facilities that are located OCONUS, off a military installation or in close proximity with a foreign entity; or facilities that share a common wall, floor, or ceiling with a non-government element most likely will require them.

(2) RED/BLACK Separation. Each SCIF must apply fundamental RED/BLACK separation to prevent the inadvertent transmission of classified data over telephone lines, power lines, signal lines, and electrical components, circuits, and communication media. The application of RED/BLACK separation establishes areas where equipment processing classified information (RED) are unique or isolated from areas where equipment processing unclassified (BLACK) are located. Separation includes physical and electrical and is detailed in Reference (ab). In addition, any component of a RED or BLACK system is also considered to be RED or BLACK.

(a) New Facilities. New facilities that will process SCI will be engineered for compliance with Reference (i), RED/BLACK installation guidance and, if applicable, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003 (Reference (ac)) prior to construction.

(b) Existing Structures. For existing structures, DAC may require compliance with Reference (o) and NSTISSI 7002 (Reference (ad)) or portions thereof as part of the TCR.

(c) Transmitters and Wireless Devices

1. Wireless transmission devices that employ RF technologies present potential security risks to SCI processing. Therefore, these devices should be prohibited from classified processing areas to the greatest extent practical. If a mission requirement or space limitation necessitates the installation of such devices within a SCIF, they shall not be powered from the same circuits as RED processors unless power line filters are used. In addition, these devices will be separated from RED processors by a minimum of 3 meters. SCIFs that require large RF communications systems (combat net radios, microwave systems, air to ground, or ship to shore) should be designed so to place them as far away from RED processors as possible.

2. Wireless transmission devices that employ infrared (IR) technologies may be used within a SCIF for unclassified processing only. If required for classified processing, DAC approval is required. If processing involves IT, IAM approval must be obtained.

(d) Fortuitous Conductors. Metallic conductors (copper or steel wires and cables used for IT, telecommunications, electrical power, etc.) and other electrically conductive materials that exit the inspectable space are potential carriers of compromising emanations. Various isolation techniques can be used to protect against these potential compromising emanations. The use of fiber optical cables is always highly recommended whenever possible since they do not create compromising emanations.

1. Power line conduction occurs when plain text information is transferred onto the power line by RED equipment, or radiated through free space and coupled onto the power lines. The power requirements for a facility are divided into two areas: power supporting mission equipment (technical) and power supporting services (non-technical), which includes lighting, heating, ventilating, and air conditioning. By providing a separate service feeder dedicated to the technical equipment and controlling its distribution, the potential for power line conduction is reduced.

2. Heating, ventilating, and air conditioning systems air ducts, water pipes and gas pipes may require protection depending on their proximity to RED equipment and their exposure outside uncontrolled areas. Since these items are made of metal, they are likely to become fortuitous conductors of TEMPEST signals into uncontrolled areas. Insertion of nonconductive sections in the plumbing or duct work at the boundary of the inspectable space of the RED equipment may be required. However, when required, national, State, and local building and fire codes must be followed.

(e) Cables. Separate dedicated cables must be used for SCI circuits. All metal cables, except coaxial cable, installed in the signal distribution system must have a minimum of one overall nonferrous shield. Coaxial cable must use a separate insulated shield. Multilevel (i.e., SCI, non-SCI, and Unclassified) wire lines should not use a common distribution vehicle. Multilevel optical fiber lines may use a common distribution vehicle providing that they are not mixed within the same fiber tube. SCI cables must use a separate patch panel or breakout box, etc., when leaving the distribution vehicle. All cables should be clearly marked, labeled, or tagged according to classification level to maintain complete accountability. Unused optical fiber cables should be disconnected from the patch panel. Unused metallic cables should be removed or stripped, bound together, and grounded.

(f) Administrative Support Equipment. Administrative support equipment includes administrative telephones, paging systems, alarm detection systems, building utilities, radio and television receivers, and miscellaneous unclassified computer and communications equipment such as facsimiles, television monitors, video cassette recorders, portable computers, modems and local area network components. This equipment can provide a conductive path for compromising emanations to exit a SCIF if not installed according to RED/BLACK criteria. Local procedures should be established to control the location and use of administrative support equipment within a SCIF. If the equipment is installed consistent with Reference (ab) and the TCR guidelines, additional approval from DAC is not required prior to installation. However, the local SCI security official must submit a modification to the TEMPEST Addendum to DIA upon completion of the installation.

(g) Multilevel Switches and Multiple Circuit Equipment. Multilevel refers to a single piece of equipment used to process multiple levels of information such as SCI, collateral, unclassified, etc. This equipment includes signal multiplexers, video and audio switches, KVM switches and other administrative equipment (fax machines, copiers, printers, etc.) that are used to process both RED and BLACK information. Multiple circuit equipment refers to numerous pieces of equipment which are connected to each other forming one large processing system. While individual circuits may not require TEMPEST equipment, connecting them together may require TEMPEST countermeasures. These types of equipment may be used if the item was approved by a certified TEMPEST testing facility. For all other equipment, coordinate with DAC for further guidance.

(h) Protected Distribution Systems (PDSs). PDSs are used to transmit unencrypted NSI through non-SCI areas. When employed, they must be configured to provide adequate electrical, electromagnetic, and physical security safeguards to protect against compromising

emanations and surreptitious exploitation. Therefore, all PDSs (SCI or collateral) entering and exiting a SCIF must be approved by DAC prior to installation and modification.

d. Equipment and Systems Installation Guidance for Ships. The primary TEMPEST vulnerability on ships is NONSTOP. (See the TEMPEST glossary in Reference (ad)). The ship itself qualifies as the inspectable space when processing occurs within the ship's hull, the equipment/systems have been installed according to section 9 of Reference (ab), the PDSs have been installed in accordance with Reference (ac), and it meets one of the following conditions:

(1) Processing is in open water, that is, not at the pier or anchorage.

(2) Processing is at the pier or anchorage of a U.S. port, but not within 100 meters of a foreign vessel.

(3) Processing is at the pier or anchorage of a foreign port, but not within 200 meters of a foreign controlled vessel or building. High and medium threat areas listed in the Director, NSA, Technical Threat Assessment may require additional countermeasures.

e. Equipment and Systems Installation Guidance for Aircraft. The primary TEMPEST vulnerability of aircraft systems (fixed wing, rotary wing, and remotely piloted vehicles) is NONSTOP. Proper grounding of equipment on an aircraft is critical. This equipment must be installed in accordance with Federal Aviation Administration requirements and Reference (ab).

(1) Airborne Operations. Aircraft systems will be installed in accordance with Recommendation I of Table 3-1 of Reference (ab). In addition, the following requirements apply:

(a) RED wiring or cabling shall be shielded and insulated overall.

(b) RED processors shall be separated by one meter from any BLACK equipment with wire lines that exit the inspectable space or are connected to an RF transmitter.

(2) Ramp Operations. Guidance for airborne operations applies for ramp operations. Ramp operations with foreign aircraft or entities within 200 meters, or from locations outside the U.S. affect the aircraft's inspectable space. The management of inspectable space and the control of conductors leaving the inspectable space must be incorporated in the ramp operations physical security plan. If the aircrafts presence is temporary, electronic processing should be suspended. If the aircraft will be operating from the location for an extended period of time, a DAC CTTA should be consulted.

f. Transportable Systems in a Tactical Environment. The primary TEMPEST vulnerability of transportable systems operated within a tactical environment is NONSTOP. Transportable systems shall be installed in accordance with Recommendation I of Table 3-1 of Reference (ab). In addition, the following requirements apply:

(1) RED wire cables shall be shielded and insulated overall.

(2) RED processors should be separated by 1 meter from any BLACK equipment with wire lines that exit the inspectable space or are connected to an RF transmitter.

(3) When deploying equipment to tents or buildings, any TEMPEST shielding provided by the transportable system may be lost due to field expedient installations. Furthermore, many fortuitous conductors (visible or hidden) may exist with these buildings. Whenever installation is within a building for more than 60 days, a DAC CTTA must be consulted to determine the need for additional TEMPEST countermeasures.

(4) The management of inspectable space and the control of conductors leaving the inspectable space must be incorporated in the tactical physical security plan.

g. Exceptions to Inspectable Space Requirements. Exceptions to inspectable space requirements are not permitted without approval by the DAC Certified TEMPEST Technical Authority (CTTA).

4. CLASSIFYING TEMPEST RELATED INFORMATION. Annex C of NTISSI 4002 (Reference (ae)) is the classification authority for TEMPEST related matters, in accordance with the following applicable guidance.

a. The completed TEMPEST addendum to the FFC and all associated documentation is classified at a minimum of CONFIDENTIAL when compiled. This documentation will be declassified when the SCIF accreditation is withdrawn.

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

c. Any compilation of documents that would allow vulnerabilities or countermeasures to be connected to a specific SCIF's physical location is classified at a minimum of CONFIDENTIAL. Examples include attaching a transmittal sheet with the facility's address or telephone number, referring to a vulnerability or countermeasure that affects ALL SCIFs, or storing the SCIF data in a file folder with the SCIF ID number.

d. Specific vulnerabilities and countermeasures may be classified in and of themselves due to their nature or sensitivity. Their use will make a document classified at the same level the vulnerability or countermeasure is classified. Classification authority and declassification instructions will be the same as the vulnerability or countermeasure.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AIS	automated information system
AO	accrediting official
AT/FP	antiterrorism/force protection
CAA	controlled access area
CI	counterintelligence
COM	Chief of Mission
COMINT	communications intelligence
COMSEC	communications security
CONUS	continental United States
COR	contracting officer representative
CSA	cognizant security authority
CSP	construction security plan
CSS	Central Security Service
CSSO	contractor special security officer
CTTA	certified TEMPEST technical authority
CUA	co-utilization agreement
DAA	designated approval authority
DAC	DIA Office of Counterintelligence and Security
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSN	Defense Switches Network
EAP	emergency action plan
E.O.	Executive order
FDO	foreign disclosure officer

FFC	fixed facility checklist
FOUO	For Official Use Only
GOCO	Government-owned contractor operated
GSA	General Services Administration
HICE	head of an Intelligence Community element
HUMINT	human intelligence
IAM	information assurance manager
IC	Intelligence Community
ICD	Intelligence Community directive
ICS	Intelligence Community standard
IDE	intrusion detection equipment
IDS	intrusion detection system
IR	infrared
IS	information system
JPAS	Joint Personnel Adjudication System
MWA	metropolitan Washington, D.C., area
NGA	National Geospatial-Intelligence Agency
NIST	National Institutes of Standards and Technology
NRO	National Reconnaissance Office
NSA	National Security Agency
NSI	National security information
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
ODNI	Office of the Director of National Intelligence
OPSEC	operations security
ORCON	originator controlled
OSPB	Overseas Security Policy Board
PCU	premise control unit

PDS	protected distribution system
POC	point of contact
RF	radio frequency
SAP	special access program
SAPF	special access program facility
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SF	standard form
SI	special intelligence
SIO	senior intelligence officer
SOP	standard operating procedure
SSM	site security manager
SSO	special security officer
SSR	special security representative
STC	sound transmission class
TCR	TEMPEST countermeasures review
TDY	temporary duty
TK	TALENT KEYHOLE
TS	TOP SECRET
T-SCIF	temporary sensitive compartmented information facility
TSCM	technical surveillance countermeasures
TSWA	temporary secure working area
UL	Underwriters Laboratories
VIP	very important person
VTC	video teleconference

PART II. DEFINITIONS

BLACK equipment. A term applied to equipment that processes only unclassified or encrypted information.

BLACK optical fiber line. An optical fiber that carries a BLACK signal or that originates or terminates in a BLACK equipment or system.

BLACK line. An optical fiber or a metallic wire that carries a BLACK signal or that originates or terminates in a BLACK equipment or system.

BLACK wire line. A metallic wire that carries a BLACK signal or that originates or terminates in a BLACK equipment or system.

closed storage. The storage of classified information in properly secured GSA approved security containers.

construction surveillance technician. A TOP SECRET/SCI-cleared U.S. citizen who is experienced in construction, and assigned to a project for the purpose of ensuring the security integrity of a site, building, SCIF, and materials and items that are scheduled for use or inclusion in a SCIF.

continuous SCIF operation. A SCIF that is staffed and operated on a 24 hours a day, 7 days a week basis.

controlled area. Any area to which entry is subject to restrictions or control for security reasons.

EAP destruction priorities

Priority 1. Material that should be destroyed first in the event that emergency destruction of classified material becomes necessary. Material to be considered Priority 1 includes all cryptographic equipment and documents.

Priority 2. Material that should be destroyed following destruction of Priority 1 material in the event that emergency destruction of classified material becomes necessary. Types of material to be considered Priority 2 include all operational SCI material which might divulge targets, documents concerning compartmented projects, and collateral TOP SECRET material.

Priority 3. Material that should be destroyed following destruction of Priority 1 and 2 material in the event that emergency destruction of classified material becomes necessary. Types of material to be considered Priority 3 include administrative SCI material and any collateral classified material (e.g., SECRET or CONFIDENTIAL material) not included under Priority 1 or Priority 2.

electronic processing. The capture, storage, manipulation, reproduction, or transmission of data in all forms by any electronically-powered device. Equipment is considered to be electronically

processing if it is manipulating data, not just because it is turned on. The classification level processed depends on the classification level of the data, not the accredited classification level of the system. This definition includes, but is not limited to, computers and their peripheral equipment, word processors, office equipment, telecommunications equipment, facsimiles, and electronic accounting machines.

fixed facility checklist. Checklist used by CSAs to determine whether construction requirements for permanent SCIFs as required in Reference (g) have been met.

GOCO SCIF. A SCIF owned by the USG and operated under contract by a non-government entity.

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

open storage. Storage of classified information within an approved facility where securing classified information in GSA approved storage containers while the facility is not occupied by authorized personnel is not required.

PDS. A wire line or fiber optics telecommunications system with adequate electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted SCI through lesser classified or uncontrolled areas.

permanent SCIF. Permanent structures (buildings, offices, etc.) built to SCIF standards, including semi-permanent structures (truck-mounted or towed military shelters, prefabricated modular trailers, or buildings), aircraft, and surface and subsurface vessels.

RED/BLACK concept. Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED) in electrical form from those that handle non-national security information (BLACK) in the same form. Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between, such items as circuits, components, equipment, and systems and also the areas where they are contained.

RED equipment. A term applied to equipment that processes unencrypted NSI that requires protection during electrical or electronic processing.

RED optical fiber line. An optical fiber that carries a RED signal or that originates or terminates in a RED equipment or system.

RED line. An optical fiber or a metallic wire that carries a RED signal or that originates or terminates in a RED equipment or system.

RED wire line. A metallic wire that carries a RED signal or that originates or terminates in a RED equipment or system.

restricted area. A CAA established to safeguard classified material that, because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

STC. A single number rating used in industry that describes the sound attenuation of an acoustic barrier and consolidates its performance across a specified frequency range. An STC rating of 45 indicates that loud speech is not audible. An STC rating of 50 indicates that very loud sounds such as music or speech amplified through speakers can only be faintly heard.

SSM. A designated TOP SECRET/SCI-cleared USG representative responsible to the COR for all site security matters involving SCIF construction projects.

TEMPEST. Defined in Reference (ac).

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

TSWA. A facility temporarily accredited to handle, process, or discuss classified information, to include SCI. The facility may not be used more than 40 hours per month and the accreditation may not exceed 12 months at any given location. SCI information may not be stored in a TSWA.

threat rating criteria

critical. Indicates that a definite threat to U.S. assets exists because the adversary has the capability and intent to attack and the assets are targeted on a fairly recurring basis.

high. Indicates that a credible threat to U.S. assets exists based on knowledge of the adversary's capability and intent to attack and on related incidents at similar facilities.

medium. Indicates that a potential threat to U.S. assets exists because of the adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability to attack through a third party who has demonstrated such a capability in related incidents.

low. Indicates that little or no threat exists because of the absence of credible evidence of capability, intent, or history of actual or planned attack against U.S. assets.