INTELLIGENCE COMMUNITY STANDARD NUMBER 705-1

PHYSICAL AND TECHNICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (EFFECTIVE: 17 SEPTEMBER 2010)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; Executive Order 13526; Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities;* and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community Standard sets forth the physical and technical security standards that apply to all sensitive compartmented information facilities (SCIF), including existing and new construction, and renovation of SCIFs for reciprocal use by all Intelligence Community (IC) elements and to enable information sharing to the greatest extent possible.

2. The standards contained herein facilitate the protection of sensitive compartmented information (SCI), including protection against compromising emanations, inadvertent observation or overhearing, disclosure by unauthorized persons, forced entry, and the detection of surreptitious and covert entry.

3. The Assistant Deputy Director of National Intelligence for Security (ADDNI/SEC) shall, in consultation with IC elements, develop and establish technical specifications to implement SCIF standards that include descriptions of best practices. The ADDNI/SEC shall, in consultation with IC elements, review and update the *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (hereinafter "*IC Tech Spec*") on an ongoing basis.

C. APPLICABILITY

1. This Standard applies to the IC, as defined by the National Security Act of 1947, as amended; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department of agency concerned, as an element of the IC.

2. IC elements shall fully implement this Standard within 180 days of its effective date.

a. Facilities under construction or renovation as of the effective date of ICD 705 shall be required to meet these standards or request a waiver to the standards.

b. SCIFs accredited as of the effective date of ICD 705 shall continue to be operated in accordance with the physical and technical security requirements applicable at the time of the most recent accreditation or re-accreditation.

c. SCIFs that have been de-accredited for less than one year but continuously controlled at least at the Secret level (in accordance with 32 CFR Parts 2001 and 2004) may be re-accredited one time, based upon the standards used for the previous accreditation.

D. Reciprocal Use

These standards are designed to ensure the protection of SCI and provide a secure environment for information sharing and reciprocal use of SCIFs. Any SCIF that has been accredited by one IC element head or designee shall be reciprocally accepted by all IC elements when there are no waivers to these standards. Standards for reciprocal use are detailed in IC Standard 705-2, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities*. A waiver may be necessary only in extraordinary circumstances when these standards cannot be met. Waivers are detailed in section H of this Standard.

E. Risk Management

1. Analytical risk management is the process of assessing threats against vulnerabilities and implementing security enhancements to achieve the protection of information and resources at an acceptable level of risk, and within acceptable cost. The Accrediting Official (AO) must ensure the application of analytical risk management in the SCIF planning, design and construction process.

2. Security in Depth

a. Security in Depth (SID) is the acceptance of the AO of external and/or internal SCIF factors that enhance the probability of detection before actual penetration to the SCIF occurs by the existence of a layer or layers of security that offer mitigations for risks.

b. To qualify for SID, at least one layer identified in the *IC Tech Spec* shall be applied.

c. SID inside the United States will allow Cognizant Security Authorities (CSA) to use less stringent construction techniques, and increase the alarm response times.

d. SID is mandatory for SCIFs located outside the United States due to increased threat.

F. SCIF Planning and Design

1. SCIF security begins with the planning and design phase. To ensure security oversight is applied throughout development and accreditation, all SCIF planning shall begin with sponsorship by an AO.

2. Facility Types. Determining where the SCIF will be located and how it will be used is necessary in determining what security enhancements may be necessary. Reciprocal use of the SCIF shall be based upon the type of facility and its current use. (For example, a facility

accredited for closed storage and non-amplified discussions is not reciprocal for open storage and amplified discussions.)

a. Secure Work Area is an area accredited for use, handling, discussing, and/or processing of SCI but where SCI is not stored.

b. Temporary Secure Working Area is a facility where the handling, discussing, and/or processing of SCI is limited to less than 40 hours per month but where SCI is not stored.

c. Continuous Operation is a SCIF that is staffed and operated 24 hours a day, seven days a week.

d. Temporary SCIF is a facility determined to be necessary for a limited time to meet tactical, emergency, or immediate operational requirements.

e. Open Storage accreditation allows SCI to be openly stored and processed within the SCIF without using Government Services Administration (GSA) approved storage containers.

f. Closed Storage accreditation requires all SCI material to be stored in a GSA approved security container in an accredited facility

3. For each SCIF construction project, a Construction Security Plan (CSP) shall be developed to address the application of security to the SCIF planning, design, and construction efforts. The specific format and content of the CSP may be developed by the AO based upon the extent of the SCIF construction and security concerns related to the SCIF.

4. Construction plans and all related documents shall be handled and protected in accordance with the CSP. If classification guides dictate, plans and related documents may require classification. Under no circumstances should plans, diagrams, etc. that are identified for a SCIF be sent or posted on unprotected information technology systems or Internet venue without encryption.

5. Construction and design of SCIFs shall be performed by U.S. companies using U.S. persons (an individual who has been lawfully admitted for permanent residence as defined in 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3)). The AO shall ensure mitigations are implemented when using non-U.S. citizens. These mitigations shall be documented in the CSP. See additional guidance in the *IC Tech Spec* for overseas SCIFs built within facilities under Chief of Mission (COM) authority.

6. SCIF design and construction shall be compliant with Fire code National Fire Protection Association 1, Life safety code NFPA 101, The Americans with Disabilities Act 28 CFR Part 36, and the Uniform Federal Accessibilities Standard where applicable.

7. SCIF Construction Security:

a. A Site Security Manager (SSM) shall be identified to the AO as the single point of contact regarding SCIF security and the individual responsible for all security aspects of the SCIF construction.

b. Construction Surveillance Technicians (CST) shall only be required outside the United States when cleared contractors are not used.

c. Cleared American Guards (as defined by Department of State Foreign Affairs Handbook 12 FAH 6, as Top Secret-cleared U.S. citizens who are selected, professionally

trained, and assigned to a project for the purpose of ensuring the security integrity of a site, building, and/or material/items) may be required when the threat warrants as determined by the AO. See additional guidance in the *IC Tech Spec* for overseas SCIFs built within facilities under COM authority.

d. When SCIF renovations require that construction personnel enter an operational SCIF, they shall be cleared or be escorted by personnel cleared to the level of the SCIF. See additional guidance in the *IC Tech Spec* for overseas SCIFs built within facilities under COM authority.

e. SCI indoctrinated escorts may not be required when a barrier has been constructed to protect the SCIF from the areas identified for construction.

f. Access control to the construction site is required and shall be addressed in the CSP.

G. Physical and Technical Security Standards

1. Physical Security for SCIFs

a. Perimeter

(1) The perimeter of the SCIF includes all perimeter walls, windows and doors as well as the ceiling and floor.

(2) The perimeter of the SCIF shall provide a physical barrier to forced, covert and surreptitious entry.

(3) Walls, floor and ceiling shall be permanently and solidly constructed and attached to each other. Raised floors and false ceilings shall not be used to anchor wall support materials. All construction, to include above the false ceiling and below a raised floor, shall be constructed to provide visual evidence of unauthorized penetration.

(4) When RF shielding is required by Certified TEMPEST Technical Authority (CTTA) evaluation, it should be planned for installation during initial construction as costs are significantly higher to retrofit after construction is complete.

(5) SCIFs that require discussions of SCI shall provide acoustic protection to prevent conversations from being inadvertently overheard outside of the SCIF.

(6) Details for the construction of the perimeter to meet standards shall be provided within the *IC Tech Spec* for SCIFs.

2. Technical Security Standards for SCIFs

a. RF transmitters shall not be introduced into a SCIF unless evaluated and mitigated to be a low risk to classified information by a competent authority (e.g., CTTA) and approved by the AO.

b. Access Control Systems

(1) Access to SCIFs is restricted to authorized personnel. Access control methods shall be approved by the AO.

(2) Access control methods may include any one of the following but are not approved for securing SCIF entrances when the SCIF is unoccupied:

(a) Automated access control systems using at least two technologies (badge, PIN, biometric, etc.)

(b) Electromechanical, mechanical or personal recognition (in small facilities and/or where there is a single monitored entrance)

c. Intrusion Detection System

(1) Intrusion Detection System (IDS) shall detect attempted or actual unauthorized human entry into a SCIF.

(2) IDS installation, related components, and monitoring stations shall comply with Underwriters Laboratories (UL) 2050 Extent 3 standards. Systems developed and used exclusively by the U.S. Government do not require UL certification but shall comply with UL 2050 Extent 3 standards for installation.

(3) Contractor SCIFs shall maintain a current UL certificate of installation and service. Any changes to the IDS after the certificate is issued shall require renewal of the certificate.

(4) SCIFs accredited prior to the effective date of ICD 705 are not required to upgrade to current IDS standards. IC elements shall ensure that upon re-accreditation the SCIF is compliant with current IDS standards, unless a waiver is granted in accordance with ICD 705.

(5) Response times for IDS shall meet 32 CFR Parts 2001 and 2004 for protecting Top Secret information.

(6) For SCIF construction under COM authority, IDS installations shall be coordinated with the Department of State (DoS), Overseas Building Operations and the Bureau of Diplomatic Security.

d. Unclassified Telecommunications Systems

(1) Any unclassified telecommunications system introduced into the SCIF shall be evaluated by the CTTA and AO for technical surveillance countermeasures and TEMPEST concerns.

(2) Unclassified telephone systems introduced within the SCIF shall meet National Telephone Security Working Group requirements for security. See *IC Tech Spec* for details.

e. Portable Electronic Devices

(1) Portable Electronic Devices pose a risk to SCI since they often include capabilities to interact with other information systems and can enable hostile attacks targeting classified information in SCIFs.

(2) The *IC Tech Spec* provides details and guidance for PED restrictions within SCIFs.

3. Temporary SCIF Standards: Temporary SCIFs that are required for emergency, tactical or other immediate operational needs often require additional security considerations including OPSEC. These facilities are addressed as a separate topic in the *IC Tech Spec*.

4. Overseas SCIFs

a. Overseas SCIFs may be:

(1) SCIFs constructed within facilities under COM authority, or

(2) SCIFs under Department of Defense (DoD) authorities and the construction of which may be affected by Status of Forces Agreements.

b. SCIFs that fall under COM authority shall comply with Overseas Security Policy Board (OSPB) standards as well as the standards herein. When a conflict occurs between OSPB and these standards, the more restrictive standard shall apply. For overseas SCIFs built within facilities under COM authority, see additional guidance for standards in the *IC Tech Spec*.

c. The DoS's *Security Environment Threat List* (SETL) shall be used in the selection of appropriate construction security criteria based on technical threat ratings.

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

e. All new facilities housing a SCIF shall be in compliance with DoD antiterrorism guidelines for military installations or OSPB standards for facilities under COM authority.

f. U.S. citizens and U.S. firms shall be used to the greatest extent practical for construction and oversight.

g. U.S. Secret cleared personnel shall perform finish work (work that includes closing up wall structures; installing, floating, taping and sealing wallboards, installing trim, chair rail, molding, floorboards; painting; etc.) unless escorted or other mitigations are applied and documented in the CSP.

h. CSTs shall be used as described in the *IC Tech Spec*.

i. The procedures for securely procuring, shipping, storing or inspecting construction material (see *IC Tech Spec* for details) shall be detailed within the CSP.

j. Open Storage

(1) In low and medium threat areas, shall only be allowed when the SCIF is under continuous operation or in which the host facility is staffed 24 hours per day by a cleared U.S. presence.

(2) In high and critical threat areas, the head of the IC element or CSA shall certify mission essential need, and approve open storage on case-by-case basis.

H. Waivers

1. A waiver shall only be considered under exceptional circumstances (i.e., only when the standards cannot be met or mitigated), or when there is a documented risk-based mission need to exceed the standards. A waiver for standards that cannot be met removes a SCIF from mandatory reciprocal use.

2. The AO shall request waiver approval of the IC element head or designee, pursuant to ICD 705.

a. A waiver request submitted when a standard cannot be met shall include the following:

(1) The standard that cannot be met

(2) The mitigation techniques considered that are not sufficient to meet the standard

(3) Justification for the waiver

(4) A statement of residual risk

(5) Guidelines, policies and/or procedures that will be implemented to reduce risk caused by the waiver

(6) Time expectation when the standard will be met and the waiver will no longer be required.

(7) A statement of acceptance of reciprocal use.

b. A waiver request submitted when a standard will be exceeded shall include the following:

(1) The standard that will be exceeded

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

(3) Time expectation that the waiver will no longer be required

(4) A statement of acceptance of reciprocal use

3. Within 30 days of approval, waivers shall be reported to the Assistant Director of National Intelligence for Policy, Plans, and Requirements (ADNI/PPR) via the IC SCIF repository.

I. Operations and Management

Once accredited and operational, the operations and management of a SCIF provides a continuous security posture. The *IC Tech Spec* provides standards for operational and management efforts that enable continuing security.

J. Roles and Responsibilities

1. The ADDNI/SEC shall:

a. Develop and establish technical specifications to implement this IC Standard.

b. Provide programmatic oversight of the implementation of this IC Standard.

c. Resolve disputes between and among SCIF stakeholders with this IC Standard.

d. Identify and incorporate IC best practices into the *IC Tech Spec* established pursuant to section B.3 of this IC Standard.

e. Develop training to ensure a common understanding of these standards and mitigations.

f. Recommend, in consultation with IC elements, to the ADNI/PPR substantive or technical amendments to this IC Standard, as appropriate.

2. Heads of IC Elements shall:

a. Implement the provisions of this Standard.

b. Approve waivers to this Standard, as appropriate.

3. CSAs shall:

a. Provide oversight of the SCIF construction and accreditation program under their security purview.

b. Ensure the timely input of required SCIF data to the IC SCIF repository.

4. AOs shall:

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

b. Review and approve the design concept, CSP, and final design for each construction project prior to the start of construction.

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

d. Accredit SCIFs under their cognizance.

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

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

g. Consider SID on U.S. Government or U.S. Government sponsored contractor facilities to substitute for standards herein. SID shall be documented in the CSP and the Fixed Facility Checklist.

5. SSMs shall:

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

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

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

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

e. Ensure procedures to control site access are implemented.

6. CTTAs shall:

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

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

7. CSTs shall:

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

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

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

K. EFFECTIVE DATE: This Standard becomes effective on the date of signature.

David R. Shedd
Assistant Director of National Intelligence for
Policy, Plans, and Requirements

September 17, 2010
Date