



**INTELLIGENCE
COMMUNITY
STANDARD**

705-02

Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities

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: This Intelligence Community Standard (ICS) sets forth the criteria that apply to the accreditation of Sensitive Compartmented Information Facilities (SCIF) to enable reciprocal use by all Intelligence Community (IC) elements and to facilitate information sharing to the greatest extent possible.

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

D. ACCREDITATION:

1. Accreditation is the beginning of a life-cycle process of continuous monitoring and evaluation, periodic re-evaluations, and documentation reviews to ensure a SCIF is maintained in an accredited state. To ensure proper implementation of these standards, the National Counterintelligence and Security Center (NCSC) may conduct assessments of SCIFs in coordination with Accrediting Officials (AO) and Cognizant Security Authorities (CSA).

a. A letter of accreditation is a formal statement on behalf of the IC element head indicating that a facility has been designed, constructed, inspected, and certified for the protection of all Sensitive Compartmented Information (SCI) compartments, programs or special activities in accordance with the provisions of ICD 705. Letters of accreditation shall include:

- 1) SCIF Identity (unique identifier and/or location); and
- 2) SCIF Type
 - a) Open or closed storage;
 - b) Acoustic requirements (e.g., discussion or non-discussion, amplified or non-amplified);
 - c) Effective date of accreditation;
 - d) Statement that SCIF meets all physical, TEMPEST, and technical security standards in place; and

22 December 2016

e) Approved waivers, to include details of the standard(s) not met and when they are scheduled to be met, or standard(s) exceeded.

2. Accreditation Process:

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

- 1) Fixed Facility checklists;
- 2) Standard operating procedures;
- 3) Emergency plans;
- 4) Construction Security Plan; and
- 5) Waiver request packages and supporting documentation, if applicable.

b. A TEMPEST review and evaluation may be included in the accreditation documentation if required by the AO. A TEMPEST review and verification of countermeasures by a Certified TEMPEST Technical Authority is a necessary part of the accreditation process.

c. When deemed necessary by the AO, a Technical Surveillance Countermeasures (TSCM) inspection may be required for a new SCIF or a significant SCIF renovation.

3. Evaluations:

a. The CSA shall ensure that regular, periodic re-evaluations are conducted to ensure continued security (to include TEMPEST, physical, technical, etc.) of the SCIF based on the sensitivity of programs, threat, facility modifications, and past security performance, or at least every five years.

4. Re-accreditation:

a. SCIFs that have waivers issued under previous standards shall be re-accredited using the most current standards.

b. All SCIFs shall be re-accredited using current standards when there are major modifications to the SCIF, changes to the sensitivity of programs, or to the threat.

c. SCIFs that have been de-accredited and controlled at the SECRET level (as specified in the *Technical Specification for Construction and Management of Sensitive Compartmented Information Facilities* (hereinafter “*IC Tech Specs*”), Chapter 1, Section B) for less than one year may be re-accredited with the AO’s approval.

d. CSAs shall ensure that the results of all SCIF re-accreditations are reported to the NCSC via the SCIF Repository within 30 days of the evaluation completion.

e. Creation of a Compartmented Area (CA) after accreditation of a SCIF under a previous standard does not require re-accreditation of the parent SCIF to the most current standard. CAs can be established utilizing the current standard even when the parent SCIF remains accredited under a previous standard.

5. De-accreditation:

- a. The de-accreditation of a SCIF is a formal notification to the DNI (via the SCIF Repository) that the facility is no longer accredited.
- b. The AO shall refer to the *IC Tech Specs* for procedures to sanitize facilities and ensure that SCI and observable elements of the mission's operation once contained within the SCIF are properly removed, disposed of, and nothing is left behind.
- c. The *IC Tech Specs* provides a list of the minimally-required actions to be taken when a facility is de-accredited.

E. RECIPROCIITY:

1. Any SCIF that has been accredited by an IC element AO or designee shall be reciprocally accepted for use as accredited by all IC elements when there are no waivers to the requirements established in IC Standard (ICS) 705-01, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, this Standard, and the *IC Tech Specs*.

2. Reciprocity is a condition that occurs when there is a requirement to share an accredited SCIF or portion thereof with a compartment, program or special activity that is sponsored by an IC element or organization other than the current SCIF CSA.

3. Co-use (or co-utilization) and Joint-use (or joint-utilization):

- a. Co-use is considered joint-use when the proposed tenant wants to use the host's information system (IS). Joint-use requires approval of the host IS Authorizing Official.
- b. Reciprocal use requires a co-use (or joint-use) agreement (hereinafter co-use) that identifies the responsibilities of the proposed tenant and host and the purpose of the proposed use (e.g. active operation and processing or storage and/or discussion only). All co-use agreements require completion of the SCIF Co-Use Request and MOA form in the *IC Tech Specs*.
- c. A co-use agreement shall be coordinated between and signed by the proposed tenant's AO or designee and the host AO or designee. Co-use requests must be approved by an authorized government official and routed through the respective IC element's co-use coordinators. A co-use agreement is not required when sharing a SCIF by two or more components under the cognizance of the same IC element. However, a co-use agreement is required for each contracting effort (e.g., contracts, proposals) performed in an accredited contractor SCIF to ensure unique contract security requirements are met.
- d. A co-use agreement shall be coordinated with IS security representatives of both elements when an IS is being introduced to the SCIF by the tenant.
- e. In SCIFs that are under a co-use agreement, a tenant shall accept the host's SCIF accreditation. If modification of the SCIF is required to meet a different type or use (e.g., open storage vs. closed storage or discussion vs. non-discussion), the cost of modifications shall be borne by the tenant that requires the modifications, unless an alternate agreement is reached. In exceptional circumstances where there is a documented mission need to exceed the uniform security requirements established pursuant to ICD 705, an IC element head or designee may grant a waiver, in accordance with ICD 705 and ICS 705-01.
- f. Co-use shall begin on the date the host CSA concurs, unless otherwise stated. Co-use requests for a contractor SCIF must include an end date. This end date will be listed in the

“Expiration Date of Contract” field and shall be considered as the date when the agreement will expire. If the contract (or program) end date is unknown, a best effort will be made to provide an estimated date. If co-use is needed past the expiration date, a new co-use request shall be submitted and approved by the respective IC elements.

g. If a contractor would like to respond to a proposal (e.g., white paper, solicitation) for an agency other than the host CSA, the contractor must obtain an appropriate government sponsor and a co-use request must be approved by both CSAs.

h. The host CSA retains security cognizance of the SCIF unless a transfer of security cognizance is approved by both CSAs in coordination with their AOs.

i. SCIFs may temporarily store SCI on behalf of other organizations for up to seven calendar days for any SCI compartment, sub-compartment or program. Storage requirements exceeding seven days require a formal co-use agreement.

j. The SCIF special security officer may allow conference rooms within a SCIF under their cognizance to be used on an occasional basis by other organizations to hold SCI discussions not related to the CSA without seeking a co-use agreement.

k. When co-use is no longer needed, a cancellation notification (form) will be routed through the tenant and host CSAs.

4. Prevention of unauthorized access to SCI:

a. In circumstances where a SCIF is under a co-use agreement and/or personnel are not briefed into all the respective programs, procedures shall be instituted by the host and tenant CSAs to prevent unauthorized access to that specific compartment, sub-compartment or program information (hereinafter “compartmented information”). Physical, visual, and acoustic access to the compartmented information by unauthorized personnel shall be controlled by the security measures identified in the *IC Tech Specs*, Chapter 2, Section C.

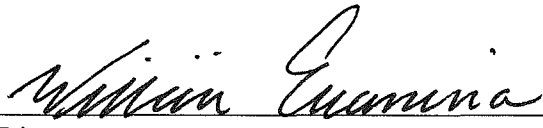
b. Additional security measures (e.g., separate reading room) may be used to further isolate controlled access program (CAP) information if specifically authorized for a CAP in accordance with ICD 906, *Controlled Access Programs*.

c. Physical, TEMPEST, administrative telephone, and TSCM requirements for the parent SCIF shall apply to the CA as well.

5. Special Access Program Facilities (SAPF) Accreditation:

a. When the IC Tech Specs has been applied to construction or renovation and operation of SAPFs, those facilities shall satisfy the standards outlined in ICD 705, ICS 705-01, and this ICS to enable reciprocal use across all IC elements for accreditation by IC elements as a SCIF.

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


 Director
 National Counterintelligence and Security Center

12.22.16
 Date