US Army Corps of Engineers®

ENGINEERING AND CONSTRUCTION BULLETIN

No. 2015-1 **Issuing Office:** CECW-CE **Issued:** 16 Jan 2015 **Expires:** 17 Jan 2017

Subject: Roles and Responsibilities for Sensitive Compartmented Information Facility (SCIF) Planning and Design

Applicability: Information and Guidance

1. **References:**

a. Unified Facilities Criteria (UFC) 4-010-05, 1 October 2013, Subject: Sensitive Compartmented Information Facilities Planning, Design, and Construction. http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_05.pdf.

b Intelligence Community Directive (ICD) 705, 26 May 2010, Subject: Sensitive Compartmented Information Facilities. http://www.ncsc.gov/publications/policy/docs/ICD_705-Sensitive_Compartmented_Information_Facilities.pdf.

c. Intelligence Community Standard (ICS) 705-1, 17 September 2010, Subject: Physical and Technical Security Standards for Sensitive Compartmented Information Facilities. http://www.ncsc.gov/publications/policy/docs/ICS_705-01_Physical_and_Technical_Security_Standards_for_Sensitive_Compartmented_Information_Facilities.pdf.

d. Intelligence Community Standard (ICS) 705-2, 17 September 2010, Subject: Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information. http://www.ncsc.gov/publications/policy/docs/ICS_705-02_Standards_for_the_Accreditation_and_Reciprocal_Use_of_Sensitive_Compartmented_Information_Facilities.pdf.

e. Intelligence Community Technical Specification for ICD/ICS 705, 23 April 2012, Subject: Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities. http://www.ncsc.gov/publications/policy/docs/Technical_Specifications_for_SCIF_Construction-V1.2.pdf.

2. **Purpose:** To serve as an interim and partial means of clarifying roles and responsibilities for the planning, design, construction, and accreditation of Sensitive Compartmented Information Facilities (SCIFs) in anticipation of formal revisions to UFC 4-010-05 that will address these same concerns in a complete and comprehensive manner. The accompanying spreadsheet will provide a quick reference to the multiple and complex steps to follow in accomplishing a SCIF design.

ECB No. 2015-1
Subject: Roles and Responsibilities for Sensitive Compartmented Information Facility (SCIF) Planning and Design

3. **Background:** With the rescinding of DCID 6/9 and the subsequent release of the Intelligence Community (IC) 705 series Technical Specification on 26 May 2011, the requirements for planning, designing, constructing and accrediting Sensitive Compartmented Information Facilities (SCIFs) became extremely stringent. Early involvement and communication by all stakeholders is crucial to the timely design, construction and accreditation of these facilities. An understanding of these associated roles and responsibilities is necessary to ensure sufficient project funding is programmed and to avoid design and construction delays. In addition, the facility and security documentation must be turned over ready for inspection and approval by the accreditation official. The process to obtain final accreditation is time consuming, costly, and requires a synchronized and concerted team effort between the customer(s), planning agent(s), design agent(s), the construction contractor(s), subject matter expert(s) and Accreditation Official (AO).

4. **Information:**

a. Every project containing a SCIF (stand alone or part of a larger project) must have an identified Site Security Manager (SSM) and a Construction Security Plan (CSP). The SSM will be identified by the using activity or local intelligence (x-2) organization. As soon as a project with a SCIF is authorized for development, the pre-concept SCIF criteria package should be initiated by the SCIF user activity and/or SSM. This process will include preparing a SCIF Concept Request to their higher headquarters Senior Intelligence Officer (SIO), preparation of the SCIF Preconstruction Fixed Facility Checklist (FFC), and a DNI TEMPEST Checklist. The local USACE planning activity and/or installation master planner should assist the SCIF user in documenting all necessary facility design criteria. Once the SIO approves the SCIF criteria package, the SCIF criteria package is sent to the AO for review and issuance of the SCIF ID and the TEMPEST Surveillance Countermeasures (TSCM) requirements. Once the SCIF end-user receives the SCIF ID assignment, the SSM prepares the working CSP, a 'living document' that is adjusted throughout the design and review process.

b. The magnitude of the SCIF project shall determine if the SSM performs these duties on a full time basis, principal basis, or as an additional duty. It is critical that the SCIF criteria package is in place during the project planning stage in order to assure that all associated SCIF facility and manpower costs are captured and adequate funding is programmed into the project. When the garrison or HQDA directs a planning charrette for a project containing a SCIF, the USACE design agent and USACE SCIF subject matter expert(s) (SMEs) at Omaha District's Protective Design Center (PDC) should be invited to participate as a member of the planning charrette team to assure that the SCIF criteria package is in place, the CSP has been initiated, and all costs have been verified.

c. The type of project (renovation of existing spaces, new Military Construction (MILCON), or work for Department of State (DoS)), and location (CONUS/OCONUS), will determine who is responsible for coordinating the CSP and Site Security Manager (SSM) responsibilities:

(1) For renovation projects where a SCIF already exists or is being added based on a higher headquarters validated Military (MI) mission, the user is responsible for developing and obtaining approval of the renovation concept and CSP from the AO.

(2) For projects funded by MILCON, the CSP and SSM efforts may be funded as part of the security cost with MILCON funds. The SCIF end-user and their SIO will provide SCIF SME oversight assistance throughout the project construction, but the security planning and associated construction security administration costs should be included as a part of the MILCON project security requirements.

(3) OCONUS SCIF projects. The creation of new SCIF space at facilities that fall under Chief of Mission (COM) authority is governed by both ICDs and Overseas Policy Board (OSPB) standards, with the more stringent standards applicable. For SCIFs constructed in new facilities, requirements are coordinated with the DoS/Overseas Buildings Operations (OBO). For existing facilities under COM authority, requirements are coordinated with DoS/Bureau of Diplomatic Security (DS), the Regional Security Officer (RSO) and General Services Officer (GSO) for an affected Embassy or Consulate, and the DoS/OBO. Temporary or tactical SCIFs require coordination with the tenant AO, the RSO, and the DoS AO.

(4) The design team must become well versed in the contents of the 'Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities' – IC Tech Spec for ICD/ICS 705. This document describes the required documents, design processes, construction processes, and construction materials required to achieve certification.

(5) The CSP will be a classified document, at least to the FOUO level. Key data including facility name, location, and size, in addition to the name of the SSO, AO and other sensitive information will drive the level of classification. In the event that threat data or SCIF countermeasures are referenced, the classification of the document will be derived from the source documents for the threat data, and may be classified higher. In order for designers or construction contractors to access the CSP document and understand the contract requirements, they must have the proper clearance as individuals and as a company. These clearances are obtained through the DD254 process. The classification of construction plans and all associated documents must follow the requirements as established in the CSP.

(6) The Contracting Officer, Contract Specialist, and PM need to understand the contractor certification requirements so that the proper source selection criteria are included in the RFP.

5. **Recommendations:**

a. Before the final design effort is started, ensure that the SCIF end-user and their higher headquarters SIO is vested and provides an approved SCIF criteria package, appropriate AO approvals including TSCM coordination, a named SSM, and a concept level CSP. If this has not occurred, immediately inform the USACE major subordinate command (MSC) & USACE Headquarters as to allow them to engage with the appropriate stakeholder,

b. Engage the USACE SCIF Subject Matter Experts (SMEs) at Omaha District's Protective Design Center (PDC) prior to starting the planning charrette when a code 0 has been issued. They will advise on processes necessary to achieve a successful project completion. Contact information can be found below.

c. Involve the PDC SMEs and SCIF end-user SMEs in all phases of the project design development and review processes. Involve the PDC, applicable USACE CoS, installation SMEs, and facility end user in the project design development and review process.

6. **Points of Contact (POC):**

a. Omaha District Protective Design Center POCs are as follows:

(1) Daniel G. Kurmel, CENWO-ED-S, (402) 995-2369; daniel.g.kurmel@usace.army.mil.

(2) John Benefiel, CENWO-ED-S, (402) 995-2396; john.l.benefiel@usace.army.mil.

b. The HQ, USACE point of contact for this ECB is Scott C. Wick, CECW-CE, (202) 761-7419; email: scott.c.wick@usace.army.mil.

//S//
Encls JAMES C. DALTON, P.E., SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers