ARMAG Review of Recent ICD 705; Version 1.5 Primary Updates

On March 13, 2020, the Director of National Intelligence (DNI) and the Physical and Technical Security Expert Working Group (PTSEWG) released the latest iteration of the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (IC "Tech Specs" for short) Version 1.5. The Tech Specs are essentially an integrated "best practices" guide for use in conjunction with the capstone document Intelligence Community Directive (ICD) 705; Intelligence Community Standard (ICS) 705-1; and ICS 705-2.

Updates	Version	Date	Pages	Section	Changes	Approver
1	1.5	11/13/19	3-4	Chapter 2.A.3.a	Added clarification language	PTSEWG
2	1.5	11/13/19	5-6	Chapter 2.C.2	Defined CA Types	PTSEWG
3	1.5	11/13/19	8	Chapter 3	Added Pre-Construction Checklist language	PTSEWG
4	1.5	11/13/19	13-15	Chapter 3.E	Expanded SCIF Door Criteria	PTSEWG
5	1.5	11/13/19	30	Chapter 4.E.2	Added reference to Inspectable	PTSEWG

					Materials Checklist	
6	1.5	11/13/19	35	Chapter 5.A	Added language in Applicability	PTSEWG
7	1.5	11/13/19	46	Chapter 6.A.1.a	Added exception language	PTSEWG
8	1.5	11/13/19	74-77	Chapter 10	Changed "CSA" to "AO" where appropriate	PTSEWG
9	1.5	11/13/19	90	Chapter 12.G.8	Added TSCM language to Inspections/Reviews	PTSEWG
10	1.5	11/13/19	95-97	Chapter 12.N/O/P	Added CUA instructions	PTSEWG
11	1.5	11/13/19	98	Chapter 13	Updated FFC and added CUA Guide and Cancellation Forms, Inspectable Materials Checklist, Pre-Construction Checklist	PTSEWG

The following is a clarification of the updates issued under ICD 705; Ver. (1.5):

1.) The primary change is the addition of the line: "or established on a permanent or temporary basis within or on U.S. diplomatic facilities/compounds." This section is a clarification of the language regarding "Threat, Vulnerability, Probability and Consequence Analysis," guidance for Chief of Mission (COM) and/or U.S. Diplomatic facility compounds and specific guidance documents (classified) for ascertaining specific threat information, such as for TEMPEST determinations by a Certified TEMPEST Technical Authority (CTTA).

2.) Many of the same requirements for Compartmented Areas (CA's) remain the same, but now CA's are further defined into three specific categories as follows:

*Category I: Intended for workstation environments that can be "Open Bays" or "Open Spaces" but the need exists to view classified compartmented information. While no physical walls may exist, this category outlines specific measures necessary to protect the viewed information. No storage or discussion is authorized, logical and/or physical.

*Category II: These are areas where discussions of compartmented information may take place and if so equipped and approved, compartmented information may also be viewed and processed. STC requirements apply (45/50) and amplified sound (example: VTC) is also authorized, however, there is still no storage of compartmented information allowed.

Category III: The highest level of Compartmented space, this category defines the strict requirements for allowing the greatest permissibility in viewing, processing, storage, discussing, handling, etc. of Compartmented Information. All personnel residing within or who have unfettered access to a Type III CA must be formally briefed into all compartments that reside within the Type III CA.

3.) New to the Tech Specs manual is a "SCIF Pre-Construction Checklist." Language was added identifying this document and its location.

4.) Historically, Accrediting Officials (AO's) have had little issue in accrediting a secondary SCIF door where there is a justified need "operationally" and in fact, earlier Tech Spec volumes have acknowledged this. This change more clearly defines specific criteria for what constitutes a Secondary Entrance Door as follows:

(a) Be equipped with a GSA-approved pedestrian door egress device with deadbolt meeting the most current version of Federal Specification FF-L-2890 for secondary door use. An AO-approved alternate device with similar functionality may be authorized. Additional standalone and flush-mounted deadbolts are prohibited.

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

While there was a persistent belief that the PTSEWG was likely going to eliminate the FF-L-2890 requirement given the issue in Version 1.4 concerning the policy conflict between the GSA spec language and the 705 requirement for no external hardware on the door, this did not occur. Several devices were located on the open market that could meet both requirements, one of which is the Lockmasters **FF-L-2890C**. In the highlighted section above, it appears there is a recognition for utilizing those devices with AO approval. They are also saying you cannot bypass the "deadlocking deadbolt" requirement with a standalone flush mounted device.

5.) Inspectable Materials Checklist was added as a "pointer" to Chapter 13 where this document is located along with other related checklists and forms

6.) Changes to the Applicability Section start with the addition of the word "SCIF" to **Section 4** dealing with existing facilities. **Section 5** under Applicability is a new section that states that an upgrade in the SETL (Security Environment Threat Listing) Technical Threat rating for a facility under COM authority, along with the RSO, shall conduct a survey for OSPB (Overseas Security Policy Board) compliance to the new technical threat requirements, and document any compliance issues accordingly. Finally, in **Section 6** under Applicability, the outdated terminology "Tactical" is removed and the requirement is added for advance coordination

between the AO and DoS AO.

7.) Clarification added to section with the line, “This chapter does not apply to temporary SCIFs established or operated within or on U.S. diplomatic facilities/compounds; see Chapter 5 for applicable guidance.”

8.) This update to the PED (Personal Electronic Device) policy recognizes that the AO, not the CSA (Cognizant Security Authority…AO’s act on behalf of the CSA) is the primary decision maker on appropriate mitigations and documentation for each agency.

9.) Section 12; G, which speaks to Inspection criteria had the following **Section 8** added: “Technical Surveillance Countermeasures (TSCM) activities in SCIFs will only be conducted by USG TSCM teams established or sponsored by a USG element. USG TSCM teams consist of USG military or civilian personnel or USG contractors who have successfully completed approved TSCM training.” Given the large number of commercially available contractors conducting TSCM testing, this new section establishes that only “USG established or sponsored” elements can be permitted to do this level of testing on both domestic or overseas SCIF facilities.

10.) This change creates sections “N,” “O,” and “P” that are new to the Tech Specs and speaks to the need and requirements for Co-Use Agreements, or “CUA’s.” The first section establishes the parameters of the CUA, the next section addresses completing the form and the final section establishes the correct procedures for terminating the CUA agreement

11.) As stated in the matrix, this acknowledges the updates of the FFC and CSP, including the addition of the CUA Guide and Cancellation Forms, Inspectable Materials Checklist, Pre-Construction Checklist