INTELLIGENCE COMMUNITY DIRECTIVE

705 Technical Amendment

Sensitive Compartmented Information Facilities

A. PURPOSE

1. Pursuant to Intelligence Community Directive (ICD) 101, Section G.1.b.(3), technical amendments are hereby made to ICD 705, *Sensitive Compartmented Information Facilities*, signed 26 May 2010.

2. This Directive, as amended, reflects the establishment of the National Counterintelligence and Security Center (NCSC) and the designation of the Director of NCSC as responsible for carrying out the counterintelligence and security functions found in DNI memorandum ES 2017-00051, *Establishment of the National Counterintelligence and Security Center*, February 24, 2017.

B. EFFECTIVE DATE: This technical amendment to ICD 705 becomes effective on the date of signature.

Assistant Director
for Policy & Strategy

February 20, 2024
Date

INTELLIGENCE COMMUNITY DIRECTIVE

705

Sensitive Compartmented Information Facilities

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; Executive Order 13526; and other applicable provisions of law.

B. PURPOSE:

1. This Directive establishes that all Intelligence Community (IC) Sensitive Compartmented Information Facilities (SCIF) shall comply with uniform IC physical and technical security requirements (hereinafter "uniform security requirements"). This Directive is designed to ensure the protection of Sensitive Compartmented Information (SCI) and foster efficient, consistent, and reciprocal use of SCIFs in the IC. This Directive applies to all facilities accredited by IC elements where SCI is processed, stored, used, or discussed.

2. This Directive rescinds Director of Central Intelligence Directive (DCID) 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, including the *Manual for Physical Security Standards for Sensitive Compartmented Information Facilities*, and all DCID 6/9 Annexes. This Directive also rescinds IC Policy Memorandum (ICPM) 2005-700-1, *Intelligence Community Update to Director of Central Intelligence (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)*; ICPM 2006-700-7, *Intelligence Community Modifications to DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs);"* and ICPM 2007-700-2, *Intelligence Community Modifications to Annex C of Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)."*

C. APPLICABILITY: This Directive 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 or agency concerned, as an element of the IC.

D. POLICY:

1. All SCI must be processed, stored, used, or discussed in an accredited SCIF.

2. All SCIFs shall comply with uniform security requirements. The Director of the National Counterintelligence and Security Center (D/NCSC) shall, in accordance with Intelligence Community Directive (ICD) 101, *IC Policy System,* and Intelligence Community Policy Guidance (ICPG) 101.2, *Intelligence Community Standards,* issue an IC Standard(s) establishing these requirements no later than 90 days after the effective date of this Directive. The IC Standard(s) shall include, but is not limited to, risk mitigation factors, and specific categories and uses of SCIFs.

3. All SCIFs shall be accredited prior to being used for the processing, storage, use, or discussion of SCI. IC elements may continue to operate SCIFs accredited as of the effective date of this Directive in accordance with physical and technical security requirements applicable at the time of the most recent accreditation or re-accreditation of a given SCIF. IC elements shall ensure that upon re-accreditation a given SCIF is compliant with the current uniform security requirements, unless the IC element head grants a waiver in accordance with section D.5 of this Directive. The D/NCSC shall, in accordance with ICD 101 and ICPG 101.2, issue an IC Standard(s) on SCIF accreditation, re-accreditation, and de-accreditation no later than 90 days after the effective date of this Directive.

4. The IC element head may accredit, re-accredit, and de-accredit SCIFs. This authority may be delegated by the IC element head to a single named official, who shall serve as the Accrediting Official. In accordance with mission need, the Accrediting Official may further delegate decision authority for the accreditation, re-accreditation, and de-accreditation of specific SCIFs while retaining overall responsibility for all such decisions.

5. The IC element head may grant a waiver of the uniform security requirements for a given SCIF, pursuant to a documented mission need. The IC element head may grant a waiver for exceptional circumstances where there is a documented mission need to exceed the uniform security requirements. The IC element head may, in exceptional circumstances, exempt SCIFs from reciprocal use by IC elements, as described in section D.7 of this Directive. The authorities established in this section may be delegated by the IC element head to a single named senior official, who could be the Cognizant Security Authority, and may not be further delegated. In no case may this official be the same person as the Accrediting Official identified pursuant to section D.4 of this Directive.

6. When the Accrediting Official believes that a waiver of the uniform security requirements for a given SCIF is warranted, a written request for a waiver shall be submitted to the IC element head, or the official to whom this role has been delegated per section D.5. The waiver request shall include a detailed statement of the mission need and the specific deviations from the uniform security requirements. All approved waivers shall be reported to the D/NCSC immediately, but no later than 30 days after the IC element head's decision.

7. All SCIFs shall be constructed, operated, and maintained for reciprocal use by IC elements. SCIFs accredited without a waiver of the uniform security requirements shall be available for reciprocal use. When requesting a waiver of the uniform security requirements for a given SCIF, in accordance with section D.6 of this Directive, the Accrediting Official shall include in the request a recommendation on reciprocal use of the SCIF. The D/NCSC shall, in accordance with ICD 101 and ICPG 101.2, issue an IC Standard(s) on the reciprocal use of

SCIFs. The IC Standard(s) shall include, but is not limited to, provisions for exemptions based on mission need.

8. For SCIFs that fall under Chief of Mission authority, IC elements shall comply with Overseas Security Policy Board (OSPB) standards, as defined in Department of State Foreign Affairs Handbook 12 FAH-6. IC elements shall submit all requests for waivers to OSPB standards to the Bureau of Diplomatic Security, Department of State, for approval. Waivers to OSPB standards must be received and approved prior to the commencement of any construction, renovation, or operations in the SCIF. IC elements shall conduct any activities subject to this section consistent with ICD 707, *Counterintelligence and Security Support to U.S. Diplomatic Facilities Abroad.*

9. The D/NCSC shall manage an inventory of information on all SCIFs subject to this Directive, the scope, form, and format of which shall be established in consultation with IC elements. IC elements are responsible for providing to the D/NCSC current information on all SCIFs, as soon as possible but no later than 180 days after the effective date of this Directive, and no later than 30 days thereafter in the case of updated or new information.

E. EFFECTIVE DATE: This guidance becomes effective on the date of signature.

//SIGNED//Dennis Blair	26 May 2010
Director of National Intelligence	Date