INTELLIGENCE COMMUNITY DIRECTIVE 704

Technical Amendment

Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information

A. PURPOSE

1. Pursuant to Intelligence Community Directive (ICD) 101, Section G.1.b.(3), a technical amendment is hereby made to Intelligence Community Directive 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, October 2008.

2. This Directive, as amended, conforms to the *Federal Investigative Standards*, December 2012, and Security Executive Agent Directive 4, *National Security Adjudicative Guidelines*, June 2017.

3. This amendment rescinds Intelligence Community Policy Guidance 704.2, *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*.

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

Assistant Director of National Intelligence for Policy and Strategy

June 20, 2018
Date

INTELLIGENCE COMMUNITY DIRECTIVE 704

Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002, as amended; Executive Order (EO) 12333, as amended; EO 12968, as amended; EO 13467, as amended; EO 13526; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Directive (ICD) establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI). This Directive also documents the responsibility of the DNI for overseeing the program producing these eligibility determinations. It directs application of uniform personnel security standards and procedures to facilitate effective initial vetting, continuing personnel security evaluation, and reciprocity throughout the Intelligence Community (IC). This Directive rescinds Director of Central Intelligence Directive 6/4, 02 July 1998, as amended; Intelligence Community Policy Memorandum (ICPM) 2006-700-3, 12 July 2006; ICPM 2006-700-4, 12 July 2006; ICPM 2006-700-5, 12 July 2006; and ICPM 2006-700-6, 12 July 2006.

C. APPLICABILITY: This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such other elements of any department or agency as may be designated by the President, or designated jointly by the DNI and the head of the department or agency concerned, as an element of the IC, or those government entities designated to determine eligibility for SCI access.

D. POLICY

1. The DNI establishes eligibility standards for access to SCI. The DNI delegates, to heads of IC elements, the authority to grant access to such information in accordance with this Directive. Heads of IC elements may further delegate determination approval authority to the Cognizant Security Authority (CSA). Notwithstanding this delegation, the DNI retains the authority in any case to make a determination granting or denying access to such information. All such determinations are discretionary and based on IC mission requirements, and do not create any rights, substantive or procedural.

2. In all access determinations, national security must be protected. Exceptions to the personnel security standards in this Directive shall be based on a finding that the risk to national security is manageable and acceptable. Nothing in this Directive, or its accompanying procedural guidelines, shall preclude the DNI, or Principal Deputy DNI, in consultation with the relevant head of an IC element, from taking actions regarding a subject's access to SCI.

3. IC elements using polygraph programs for personnel security purposes may require polygraph examinations when the head of an IC

element deems it to be in the interest of national security. These polygraph programs shall include standardized training and certification of operators to ensure consistent and fair processes.

4. Heads of IC elements or designees may determine that it is in the national interest to authorize temporary access to SCI, subject to the following requirements – temporary access approvals shall be granted only during national emergencies, hostilities involving United States personnel, or in exceptional circumstances when official functions must be performed, pursuant to EO 12968, as amended. Temporary access approvals shall remain valid until the emergencies, hostilities, or exceptional circumstances have abated or the access is rescinded. In any case, temporary access shall not exceed one year.

5. When eligibility for access is first adjudicated, CSAs are required to use sound risk management. Continuous personnel security and counterintelligence (CI) evaluation will be required of all personnel granted access to SCI.

6. Subjects who have immediate family members or other persons who are not United States citizens to whom the subject is bound by affection or obligation may be eligible for access to SCI as the result of a condition, deviation, or waiver from personnel security standards.

7. This ICD and its associated Intelligence Community Policy Guidance (ICPG) promulgate the personnel security policy of the DNI. These associated ICPGs are described below:

a. The evolving critical threat environment requires that innovative security, CI, and risk management measures be continually developed and implemented to support intelligence production, information sharing, reciprocity, and personnel mobility. Eligibility for access to SCI shall be contingent on meeting DNI personnel security standards as measured by investigative activities prescribed in ICPG 704.1, *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* and the application of specific adjudicative guidelines contained in Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines.*

b. Denial of initial access to SCI, revocation of continued access eligibility, and the appeals process for such actions, is addressed in ICPG 704.3, *Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes.*

c. All IC security elements shall accept in-scope personnel security investigations and access eligibility determinations that are void of conditions, deviations, or waivers. Specific guidelines are contained in ICPG 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations.*

d. The IC Scattered Castles repository, or successor database, shall be the authoritative source for personnel security access approval verifications regarding SCI, visit certifications, and documented exceptions to personnel security standards. Heads of IC elements shall ensure that accurate, comprehensive, relevant, and timely data are delivered to this repository. Specific guidelines are contained in ICPG 704.5, *Intelligence Community Personnel Security Database Scattered Castles.*

E. PERSONNEL SECURITY STANDARDS: Threshold criteria for access to SCI are as follows:

1. The subject requiring access to SCI must be a U.S. citizen.

2. The subject must be stable, trustworthy, reliable, discreet, of excellent character, and sound judgment; and must be unquestionably loyal to the United States.

3. Members of the subject's immediate family and any other person(s) to whom the subject is bound by affection or obligation shall not be subject to physical, mental, or other forms of duress by either a foreign power or by persons who may be or have been engaged in criminal activity, or who advocate either the use of force or violence to overthrow the U.S. Government, or alteration of the form of the U.S. Government by unconstitutional means.

F. EXCEPTIONS TO PERSONNEL SECURITY STANDARDS

1. A head of an IC element may grant access based on an exception to the above standards based on all available information that the specific risk to national security is manageable and acceptable. In such cases, additional personnel security and/or CI evaluation may be required. All risk assessments shall become a part of an individual's security file and the results of the risk assessment shall be annotated as an exception in the record.

2. The DNI, or designee, is the exclusive authority for granting an exception to the requirement that the subject be a U.S. citizen. Exceptions to this requirement shall require a letter of compelling need that is based upon specific national security considerations.

3. When an exception to these personnel security standards is warranted and a subject is granted access to SCI, the approving organization shall document its findings in the subject's security record and the Scattered Castles or successor database. In accordance with SEAD 4, the findings shall be characterized as a waiver, condition, deviation, or out-of-scope.

G. ROLES AND RESPONSIBILITIES

1. The Director, National Counterintelligence and Security Center shall:

   a. Carry out the responsibilities of the DNI with respect to security;

   b. Oversee the IC security programs and develop IC security standards; and

   c. Provide IC security services in the form of research, training, and security databases.

2. Heads of IC elements and those government entities designated to determine eligibility for SCI access shall uniformly and consistently implement DNI security policies governing access to classified national intelligence information.

3. The CSA, as the senior security authority designated by a head of an IC element, shall:

   a. Oversee all aspects of security program management within an IC element; and

   b. As needed, formally delegate responsibility for certain security matters to specific offices within their agencies.

H. EFFECTIVE DATE: This ICD is effective on the date of signature.

//SIGNED// J.M. McConnell
Director of National Intelligence

1 OCT 08
Date