INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 704

PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION AND OTHER CONTROLLED ACCESS PROGRAM INFORMATION

(EFFECTIVE: 01 OCTOBER 2008)

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 12958, as amended; EO 12968, EO 13467, 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) and information protected within other controlled access programs. 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 other departments or agencies that 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 and other controlled access program information. 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 and other controlled access information.

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 and other controlled access program information, 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. Temporary access approvals shall remain valid until the emergency(ies), 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 and other controlled access program information.

6. Subjects who have immediate family members or other persons who are non-United States citizens to whom the subject is bound by affection or obligation may be eligible for access to SCI and other controlled access program information 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 and other controlled access program information shall be contingent on meeting DNI personnel security standards as measured by investigative activities prescribed in ICPG 704.1 and the application of specific adjudicative guidelines contained in ICPG 704.2.

b. Guidance pertaining to denial of initial access to SCI and other controlled access programs or revocation of continued access eligibility, and the appeals process for such actions is contained in ICPG 704.3.

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.

d. The IC Scattered Castles repository, or successor database, shall be the authoritative source for personnel security access approval verifications regarding SCI and other controlled access programs, 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.

e. Additional ICPGs, and amendments to the ICPGs listed above, may be promulgated by the Deputy Director of National Intelligence for Policy, Plans, and Requirements (DDNI/PPR) following formal IC coordination.

E. PERSONNEL SECURITY STANDARDS

Threshold criteria for eligibility 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 a condition, deviation, or waiver 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 and other controlled access program information, the approving organization shall document its findings in the subject's security record and the Scattered Castles or successor database. The findings shall be characterized as a waiver, condition, or deviation.

G. RESPONSIBILITIES

1. **Deputy Director of National Intelligence for Policy, Plans, and Requirements** is responsible for enforcing the authorities and carrying out the responsibilities of the DNI with respect to security.

2. **Assistant Deputy Director of National Intelligence for Security** is responsible for overseeing IC security programs.

3. **Director of the DNI Special Security Center** is responsible for developing, coordinating, and implementing DNI security policies throughout the IC and providing IC security services in the form of research, training, and security databases.

4. **Heads of IC Elements** are responsible for uniformly and consistently implementing DNI security policies governing access to classified national intelligence.

5. **Cognizant Security Authority** is responsible, as the senior security authority designated by a Head of an IC Element, for overseeing all aspects of security program management within an organization. The CSAs may formally delegate responsibility for certain security matters to specific elements within their agencies.

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

J M McConnell

Director of National Intelligence

1 OCT 08

Date

APPENDIX A – ACRONYMS

ICD 704 -- PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION AND OTHER CONTROLLED ACCESS PROGRAM INFORMATION

CI	counterintelligence
CSA	Cognizant Security Authority
DNI	Director of National Intelligence
EO	Executive Order
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
ICPM	Intelligence Community Policy Memorandum
SCI	Sensitive Compartmented Information
US	United States