INTELLIGENCE COMMUNITY POLICY GUIDANCE

704.5

Intelligence Community Personnel Security Database Scattered Castles

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 13526; ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information;* and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community Policy Guidance (ICPG) mandates the recognition and use of the Scattered Castles database, or successor database, as the Intelligence Community's (IC) authoritative personnel security repository for verifying personnel security information for the purposes of, but not limited to, visitor control, clearance reciprocity, and logical access to systems.

2. This Policy Guidance revises ICPG 704.5, *Intelligence Community Personnel Security Database Scattered Castles,* 2 October 2008.

C. APPLICABILITY: This Policy Guidance applies to the IC, as defined by the National Security Act of 1947, as amended, and such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (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 access to Sensitive Compartmented Information (SCI).

D. POLICY

1. Scattered Castles is the program name for the IC security clearance repository for all clearance and access determinations. It serves as the trusted, authoritative personnel security repository for verifying personnel security clearances, access to SCI and other controlled access programs, reciprocity, and documented exceptions to personnel security standards. Scattered Castles is hosted on the Joint Worldwide Intelligence Communication System (JWICS). The Scattered Castles database shall:

a. Consolidate personnel security data records within the IC;

b. Include records of all eligibility-for-access determinations to include approvals, denials, revocations, and suspensions;

c. Include records of all waivers, deviations, or conditions relating to eligibility-for-access determinations;

d. Serve as a National Agency Check data source to avoid duplicative background investigations, adjudications, and where applicable, polygraph examinations;

e. Include records of all personnel holding current access to SCI and other controlled access programs (CAP), if applicable, with the exception of classes of personnel exempted due to specific mission concerns. In sensitive situations, IC organizations may record specific personnel under pseudonym. In these cases, the source IC organization must maintain internal records containing the true information for such personnel;

f. Include records of all collateral clearances and personnel security background investigations and adjudications granted or conducted by an IC element, to include pending and cancelled investigations or adjudications;

g. Include records of all personnel previously granted a clearance or access to SCI and other controlled access programs, and retain records as follows, unless directed otherwise by the DNI or designee:

(1) For personnel whose clearance has been suspended, denied, or revoked, retain records for 50 years from the date of suspension, denial, or revocation;

(2) All other records shall be retained in accordance with the General Records Schedule, Sec. 5.6, Item 181, or successor records retention guidance.

h. Serve as the primary source for verifying and accepting visit certifications without additional hard copy or electronic documentation from the visitor's parent organization. Where Scattered Castles is not available, hard copy or electronic visit certifications shall continue to be accepted by the organization to be visited.

2. In order to promote IC integration, personnel security clearance reciprocity, and uninterrupted access to the IC Information Environment, IC elements shall ensure all relevant and required information is entered into the Scattered Castles database in a timely manner. In addition, IC elements accepting Second Party Integrees shall refer to DNI policy memorandum ES 2016-00816, *Second Party Integree Access to the Intelligence Community Information Environment*.

3. The Scattered Castles database shall serve as the primary source for security clearance and access verifications. In order to facilitate hiring actions and personnel mobility across the IC, IC elements may grant human resources professionals or other personnel, as appropriate, access to Scattered Castles.

4. The Scattered Castles Executive Steering Group (SCESG), comprised of representatives from each IC element, shall be responsible for determining database requirements and access management to include identifying required data fields.

E. ROLES AND RESPONSIBILITIES

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

a. Collaborate with the Department of Defense (DoD) and the Office of Personnel Management (OPM) to ensure personnel security information contained in the *Joint Personnel Adjudication System* (JPAS) within DoD and the *Central Verification System* (CVS) within OPM, or successor databases, is also entered into the Scattered Castles database.

b. Oversee, operate, and maintain the Scattered Castles database in collaboration with the SCESG;

c. Chair the SCESG; and

d. Collaborate with the ODNI Special Programs Division to ensure timely and updated inventory of IC CAPs and ensure agencies provide Scattered Castles CAP information in accordance with ICD 704.

2. The Assistant DNI for Information and Data shall provide NCSC with the *Access Value List* with the most recent SCI and other IC CAP inventory to be recorded in Scattered Castles, consistent with ICD 906, *Controlled Access Programs.*

3. Heads of IC elements shall:

a. Designate representatives with the appropriate levels of personnel security expertise to the SCESG;

b. Identify security points-of-contact, access managers, technical representatives, and data load points-of-contact;

c. Ensure all Scattered Castles data is accurate, valid, appropriately classified, and submitted weekly to the Scattered Castles database, at a minimum, to include briefings, debriefings, and temporary (interim) clearances;

d. Record all clearance denials, revocations, suspensions, and reciprocity inquiries within 24 hours of the decision;

e. Populate the Scattered Castles database and retain relevant and comprehensive personnel security information in compliance with record retention requirements identified in this ICPG; and

f. Update the Scattered Castles database regarding granted crossover clearances and access approvals.

g. Grant access to the Scattered Castles database, as appropriate.

F. EFFECTIVE DATE: This Policy Guidance becomes effective on the date of signature.

Acting Director of National Intelligence

Date 2/25/20