INTELLIGENCE COMMUNITY POLICY GUIDANCE
NUMBER 704.5

INTELLIGENCE COMMUNITY PERSONNEL SECURITY DATABASE SCATTERED CASTLES

(EFFECTIVE: 02 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 13355; EO 12958, as amended; EO 12968, and other applicable provisions of law.

B. APPLICABILITY: This directive applies to the Intelligence Community (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 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 Sensitive Compartmented Information (SCI) access.

C. SCOPE: This Intelligence Community Policy Guidance (ICPG) mandates the recognition and use of the Scattered Castles (SC) database, or successor database, as the IC's authoritative personnel security repository for verifying personnel security access approvals regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards.

D. KEY ELEMENTS

The SC database shall:

1. Consolidate personnel security data records within the IC;

2. Record all eligibility-for-access determinations to include approvals, denials, revocations and suspensions;

3. Record waivers, deviations, or conditions relating to eligibility-for-access determinations;

4. Provide a National Agency Check data source to avoid duplicative background investigations and, where applicable, polygraph examinations;

5. Record all individuals holding current access to SCI and other controlled access programs, with the exception of classes of individuals 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 these individuals;

6. Include records of subjects previously holding SCI and other controlled access program access;

7. For subjects with active clearances, retain data records indefinitely; for subjects who have been debriefed or terminated, retain records for two years; for subjects whose clearances have been revoked or denied, retain records for seven years; and for subjects whose clearances have been suspended and are pending revocation, retain records indefinitely; and

8. 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 database access constraints prevent entry of personnel security data into the SC database, hard copy or electronic visit certifications shall continue to be accepted by the organization to be visited.

E. RESPONSIBILITIES

1. The DNI Special Security Center shall:

a. Collaborate with the Department of Defense and the Office of Personnel Management (OPM) to ensure Senior Officials of the Intelligence Community -approved personnel security information contained in the SC database is accessible and the data is correlated with OPM's Clearance Verification System database at the appropriate level of classification to protect agency-specific classified information;

b. Oversee, operate, and maintain the SC database in collaboration with the Scattered Castles Executive Steering Group (SCESG).

2. The SCESG, comprised of representatives from each IC element, shall be responsible for database functionality and access management of the database.

3. Senior Officials of the Intelligence Community shall:

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

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

c. Populate the SC database with relevant and comprehensive personnel security information; and

d. Be responsible for updating the SC database regarding subjects granted crossover clearances or special access approvals;

e. Ensure all SC data is accurate and submitted in a timely manner; conduct a total records refresh at least once every thirty-one (31) days; update records, to include briefings and debriefings, at least weekly; and record all clearance denials, revocations and suspensions within twenty-four (24) hours of the decision.

F. EFFECTIVE DATE: This ICPG is effective on the date of signature.

David R. Shedd
Deputy Director of National Intelligence
for Policy, Plans and Requirements

October 2, 2008
Date

APPENDIX A – ACRONYMS

ICPG 704.5 -- INTELLIGENCE COMMUNITY PERSONNEL SECURITY DATABASE SCATTERED CASTLES

DNI	Director of National Intelligence
EO	Executive Order
IC	Intelligence Community
ICPG	Intelligence Community Policy Guidance
SC	Scattered Castles
SCESG	Scattered Castles Executive Steering Group
SCI	Sensitive Compartmented Information