



SECURITY EXECUTIVE AGENT DIRECTIVE 6

CONTINUOUS EVALUATION

(EFFECTIVE: 12 JANUARY 2018)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Security Clearance Information Act, as amended; Executive Order (EO) 12968, *Access to Classified Information*, as amended; EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, as amended; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*, and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes policy and requirements for the continuous evaluation (CE) of covered individuals who require continued eligibility for access to classified information or eligibility to hold a sensitive position.

C. APPLICABILITY: This Directive applies to any executive branch agency, authorized adjudicative agency, authorized investigative agency, and covered individuals as defined below.

D. DEFINITIONS: As used in this Directive, the following terms have the meanings set forth below:

1. “Agency”: Any “executive agency” as defined in Section 105 of Title 5, United States Code (U.S.C.), including the “military departments,” as defined in Section 102 of Title 5, U.S.C., and any other entity within the executive branch that comes into possession of classified information or has positions designated as sensitive.

2. “Authorized adjudicative agency”: An agency authorized by law, executive order, or designation by the SecEA to determine eligibility for access to classified information in accordance with EO 12968, as amended, or eligibility to hold a sensitive position.

3. “Authorized investigative agency”: An agency authorized by law, executive order, or designation by the SecEA to conduct a background investigation of individuals who are proposed for access to classified information or eligibility to hold a sensitive position or to ascertain whether such individuals continue to satisfy the criteria for retaining access to such information or eligibility to hold such positions.

4. “Classified national security information” or “classified information”: Information that has been determined, pursuant to EO 13526, any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

5. “Continuous Evaluation”: A personnel security investigative process to review the background of a covered individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated records checks and business rules, to assist in the ongoing assessment of an individual’s continued eligibility. It supplements—but does not replace—the established personnel security program for scheduled periodic reinvestigations of individuals for continuing eligibility.

6. “Covered individual”:

a. A person who performs work for or on behalf of the executive branch or who seeks to perform work for or on behalf of the executive branch, but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. §§ 105 or 107, the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. § 106 or annual legislative branch appropriations acts;

b. A person who performs work for or on behalf of a state, local, tribal or private sector entity, as defined in EO 13549, but does not include duly elected or appointed Governors of a state or territory, or an official who has succeeded to that office under applicable law;

c. A person working in or for the legislative or judicial branches with eligibility for access to classified information and the investigation or determination was conducted by the executive branch; but does not include Members of Congress; Justices of the Supreme Court; and Federal judges appointed by the President; and

d. Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who require eligibility for access to classified information or eligibility to hold a sensitive position, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.

7. “National Security Eligibility”: Eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

8. “Reasonably exhaustive efforts”: The appropriate level of effort to resolve issues or corroborate discrepant information. They may include multiple attempts or techniques to satisfy the issue, attempts to corroborate the activity through references from the background investigation, and/or attempts to obtain and pursue additional leads through other aspects of the investigation.

9. “Sensitive position”: Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security regardless of whether the occupant has access to classified information, and regardless of whether the occupant is an employee, military service member, or contractor.

E. POLICY:

1. CE shall be conducted on covered individuals with national security eligibility by the head, or designee, of the agency sponsoring the covered individual.

2. Automated records checks shall be conducted to identify adjudicatively relevant information to assist in assessing the continued eligibility of a covered individual at any time during the period of eligibility. The automated records checks will include checks of commercial databases, U.S. Government (USG) databases, and other information lawfully available to security officials at any time during the period of eligibility.

3. Technical and security safeguards shall be implemented to ensure CE is conducted only on covered individuals to protect the privacy, civil liberties, and personally identifiable information of covered individuals and any other individual whose information is inadvertently collected as part of the CE process. Absent a national security concern, criminal reporting requirement, or other legal requirement, information pertaining to individuals other than the covered individual will not be retained unless that information is relevant to a security determination of the covered individual.

4. Information gathered by CE shall be forwarded to the sponsoring agency for analysis of adjudicative relevance and a determination if the information meets thresholds for further investigation and/or adjudication.

5. Authorized investigative agencies shall make reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to the covered individual.

6. Agencies shall ensure further investigation is conducted when required, consistent with the Federal Investigative Standards. Any potentially disqualifying issue(s) shall be adjudicated using the National Security Adjudicative Guidelines. No unfavorable personnel security actions shall be taken solely on uncorroborated or unverified discrepant information collected pursuant to this Directive. When an adjudicative determination is made to deny or revoke national security eligibility, review proceedings, to the extent they are made available in EO 12968, as amended, Part 5, shall be afforded covered individuals at a minimum.

7. Agencies shall update either Scattered Castles, the Joint Personnel Adjudication System within the Department of Defense, or the Central Verification System database within the U.S. Office of Personnel Management or successor databases, unless authorized by the SecEA to withhold information from the database for national security purposes, to inform on a covered individual's national security eligibility for reciprocity purposes.

8. Authorized investigative agencies may develop and implement a full or partial CE capability for their agency and may provide this capability to other agencies. Agencies may choose to obtain required CE checks from the Office of the Director of National Intelligence, National Counterintelligence and Security Center (NCSC), or another authorized investigative agency.

9. All CE capabilities shall be subject to verification of compliance with this Directive and subsequent CE guidance, standards, and requirements.

F. RESPONSIBILITIES:

1. The Director, NCSC (D/NCSC) shall:
 - a. Develop and promulgate CE guidance and standards, to include identification of data sources and periodicity;
 - b. Issue implementation and business process guidelines;
 - c. Develop, implement, and operate a CE capability that will be available to agencies;
 - d. Conduct periodic assessments of agencies' CE capabilities to verify compliance with this Directive and subsequent CE guidance and standards; and
 - e. Conduct research and development to ensure that existing CE standards, data sources, periodicity, and capabilities remain efficient and effective, and comply with legal, privacy, and civil liberties requirements.
2. Heads of agencies shall:
 - a. Determine if their agency shall use the capability provided by D/NCSC, develop their own full or partial capability, or utilize another authorized investigative agency's capability to conduct CE records checks;
 - b. Ensure policies and procedures governing the administration of CE data (e.g., collection, use, disclosure, and retention of information obtained from CE) are in accordance with all applicable laws and executive orders, and include appropriate protections for privacy and civil liberties (e.g., System of Records Notices required by the Privacy Act, or Privacy Impact Assessments where required by the E-Government Act);
 - c. Ensure agency CE capabilities comply with SecEA guidance and standards;
 - d. Conduct CE on covered individuals, consistent with SecEA guidance and standards, who require continued national security eligibility when the agency holds the covered individual's eligibility;
 - e. Ensure covered individuals are aware of CE as an element of the Personnel Security Program and their continuing security and counterintelligence (CI) reporting obligations. CE shall be included in initial and annual security awareness training.
 - f. Implement policies and procedures to respond to information (to include new information) identified during CE records checks in accordance with CE implementation guidance;
 - g. Make reasonably exhaustive efforts to ensure information obtained from CE that meets thresholds for further investigation and/or adjudication is resolved. Agencies should use standard personnel security processes to resolve potential issue information received on a covered individual;
 - h. Act upon and share relevant information of a security, CI, or law enforcement concern with appropriate security, CI, insider threat, or law enforcement officials;

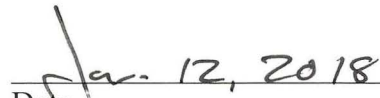
i. Share relevant information that may result in an adverse determination of the covered individual's continued national security eligibility with security officials of other agencies that have a direct interest in the covered individual. Direct interest is defined as the individual being on joint duty, detail or otherwise working for the other agency; or the other agency has granted access or additional access to the individual; and

j. Cease conduct of CE on individuals who no longer meet the definition of covered individual (e.g., termination of employment, no longer affiliated with the USG).

G. EFFECTIVE DATE: This Directive becomes effective on the date of signature.



Daniel R. Coats
Security Executive Agent



Date