SECURITY EXECUTIVE AGENT DIRECTIVE 8

TEMPORARY ELIGIBILITY

(EFFECTIVE: 18 MAY 2020)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended (50 U.S.C. § 3341); Executive Order (EO) 12968, *Access to Classified Information*, as amended; EO 13526, *Classified National Security Information*; 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*; Title 5, Code of Federal Regulations Part 1400, *Designation of National Security Positions*; and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes policy and requirements for authorizing temporary (often referred to as "interim") eligibility, which includes temporary access to classified information, temporary access to a higher level of classified information, one-time access to classified information, temporary eligibility to hold a sensitive position, and temporary eligibility to hold a higher level sensitive position when determined to be in the national security interest. This Directive rescinds Security Policy Board Issuance 3-97, *Investigative Standards for Temporary Eligibility for Access*.

C. APPLICABILITY: This Directive applies to any executive branch agency, authorized investigative agency, and any authorized adjudicative agency, as defined below, conducting background investigations and adjudications for temporary eligibility.

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, EO, 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, EO, 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. "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 the Vice President;
   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; and
   c. A person working in or for the legislative or judicial branches and the investigation or determination would be conducted by the executive branch; but does not include members of congress; justices of the Supreme Court; and federal judges appointed by the President.
   d. Covered individuals 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.
6. "National security": Those activities which are directly concerned with the foreign relations of the United States (U.S.), or protection of the Nation from internal subversion, foreign aggression, or terrorism.
7. "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. Temporary access to classified information, temporary access to a higher level of classified information, temporary eligibility to hold a sensitive position, and temporary eligibility to hold a higher level sensitive position, as identified below, may be approved by security personnel authorized by the agency head. One-time access to classified information, as identified below, may be approved by the agency head or security personnel authorized by the agency head.

2. Temporary access to classified information and temporary eligibility to hold a sensitive position shall be recorded by the granting agency in either the Intelligence Community (IC) Scattered Castles, the Joint Personnel Adjudication System (JPAS) within the Department of Defense (DoD), or the Central Verification System (CVS) database within the U.S. Office of Personnel Management (OPM), or successor databases and explicitly annotated with the type, level, and date approved, unless authorized by the SecEA to withhold information from the database for national security purposes. This requirement does not apply to one-time access. Recording for one-time access shall be in accordance with paragraph H.4.
3. Agencies shall update the record as required in paragraph E.2 for all adverse adjudicative determinations made related to temporary eligibility. These include any associated exceptions, denials, or revocations.
4. Temporary access to a higher level of classified information and temporary eligibility to hold a higher level sensitive position shall be recorded in a database as identified in paragraph E.2 and explicitly annotated with the type, level, and date approved. Agencies shall update these records in accordance with paragraph E.3.
5. Individuals granted temporary or one-time access to classified information shall be briefed on their responsibilities to protect classified information and sign an approved non-disclosure agreement (e.g., Standard Form [SF] 312, Form 4414) prior to access, and debriefed when access is terminated. Upon termination of temporary access, the database entries as required in paragraph E.2 shall be updated to include the debriefing information.

F. TEMPORARY ACCESS TO CLASSIFIED INFORMATION:

1. Security personnel authorized by the agency head may approve temporary access to classified information for covered individuals before the investigation and adjudication processes are completed during exceptional circumstances when official functions must be performed, to include meeting mission readiness requirements, pursuant to EO 12968, as amended. Concurrently, personnel security background investigations and adjudications shall be expedited.
   a. **Approvals for Temporary Access to CONFIDENTIAL, SECRET, and "L" require:**
      1) Favorable review of a completed SF 86, *Questionnaire for National Security Positions*, by the authorized adjudicative agency;
      2) Citizenship verification;
      3) Initiation of an expedited investigation; and
      4) Completion and favorable review of a Federal Bureau of Investigation (FBI) fingerprint check.
   b. **Approvals for Temporary Access to TOP SECRET and "Q" require:**
      1) Favorable review of a completed SF 86 by the authorized adjudicative agency;

2) Citizenship verification;

3) Initiation of an expedited investigation;

4) Completion and favorable review of the following:

a) FBI fingerprint check;

b) FBI name check; and

c) National Crime Information Center (NCIC) check.

2. Security personnel authorized by the agency head must

a. Include a justification of the temporary eligibility for access; and

b. Notify the covered individual in writing that further access is expressly conditioned on:

1) Favorable completion of an investigation; and

2) Issuance of an access eligibility approval.

3. Security personnel authorized by the agency head shall ensure that covered individuals granted temporary access approvals are limited in exposure to classified information and only to particular identified categories necessary to perform authorized functions.

4. Temporary access to special access program (SAP) and/or controlled access program (CAP) information requires the approval of the establishing authority or the designated program manager. Establishing authorities may implement policies and procedures for temporary access to their SAPs and/or CAPs.

5. Temporary access approvals shall remain valid until the exceptional circumstances have abated, the temporary access is terminated, or final eligibility is granted. Temporary access shall not exceed one year unless approved by security personnel authorized by the agency head. Justification for approved temporary access exceeding one year shall be recorded and maintained by the granting agency.

6. Temporary access shall be valid only with the granting agency and may be terminated at any time if disqualifying information is received. Agencies may accept temporary access approvals from other agencies based on their own risk assessment.

G. TEMPORARY ACCESS TO A HIGHER LEVEL OF CLASSIFIED INFORMATION:

1. Security personnel authorized by the agency head may approve temporary access to a higher level of classified information for a covered individual eligible for access to a lower level when determined necessary to meet operational or contractual exigencies not expected to be of a recurring nature pursuant to EO 12968, as amended.

2. Access approvals shall remain valid until the exigency has abated or the access is terminated. In any case, access shall not exceed 180 days.

3. If access is expected to exceed 180 days, agencies must comply with the requirements in paragraph F above.

4. Access will be limited to specific identifiable information, and information access records shall be maintained. Access to higher level classified information under the control of another agency requires concurrence of the other agency.
5. Temporary access approvals to SAP and/or CAP information must comply with the requirements in paragraph F.4.

H. ONE-TIME ACCESS TO CLASSIFIED INFORMATION:

1. During exceptional circumstances, agency heads or security personnel authorized by the agency head may approve one-time access to classified information when it is determined to be in the national security interest. One-time access shall be limited to individuals whose expertise offers specialized and important benefit and value to the United States Government (USG) or to individuals to whom access to classified information needs to be provided in the interest of national security. One-time access shall be limited to the period needed to accomplish the national security requirement. One-time access shall not exceed one year. Agencies that require an individual to have access in excess of one year shall sponsor the individual for a security clearance.
2. One-time access shall only be granted to individuals who are U.S. citizens with a willingness and ability to abide by regulations governing the use, handling, and protection of classified information.
3. One-time access requires a statement of compelling need that includes
   a. The unique qualifications of the individual(s) and/or the unique circumstances that require divulging classified information;
   b. The expected benefit to the USG and national security;
   c. The expected nature, extent, and level of access to classified information; and
   d. Dates for which access is required.
4. Records documenting one-time access to classified information and the dates for which one-time access was granted shall be maintained by the granting agency.
5. One-time access shall not be active for multiple national security requirements unless specifically authorized by the agency head.
6. The investigative checks and required information identified in the Appendix, at a minimum, shall be obtained and favorably reviewed prior to one-time access. Agencies shall obtain all required SF 86 consent forms.
7. One-time access shall be restricted to specific, identifiable classified information, and shall be limited only to information needed to fulfill the national security requirement. Information access records shall be maintained by the agency.
8. Individuals approved for one-time access shall not be permitted access to classified information technology systems, except under very limited conditions as approved by the agency head or designee. Such conditions shall include restricted access and continuous oversight and monitoring.

9. One-time access to SAP and/or CAP information requires the approval of the establishing authority or the designated program manager. Establishing authorities may implement policies and procedures for one-time access to their SAPs and/or CAPs.
10. Classified information with dissemination control markings that require originator consent for further dissemination (e.g., Dissemination and Extraction of Information Controlled by Originator [ORCON]) may be provided to individuals with a one-time access approval only with prior approval from the originator. Other control markings that restrict access to certain individuals (e.g., Caution-Proprietary Information Involved [PROPIN], ORCON-USGOV, etc.) shall be adhered to.
11. Individuals approved for one-time access shall receive a security briefing and be required to sign an approved non-disclosure agreement prior to receiving classified information. Individuals shall be debriefed immediately when access is no longer required.
12. One-time access approvals shall be valid only within the agency granting such access and may be terminated at any time without appeal. Agencies may accept one-time access approvals from other agencies based on their own risk assessment.
13. One-time access shall not serve as the basis for a subsequent final security clearance and should not be authorized for convenience or to fill positions that would otherwise require a security clearance.

I. TEMPORARY ELIGIBILITY TO HOLD A SENSITIVE POSITION:

1. Security personnel authorized by the agency head may approve temporary eligibility to hold a sensitive position for covered individuals before the investigation and adjudication processes are completed during exceptional circumstances when official functions must be performed, to include meeting mission readiness requirements, pursuant to EO 12968, as amended. Concurrently, personnel security background investigations and adjudications shall be expedited.

   a. **Approvals for Temporary Eligibility for Non-Critical-Sensitive Positions require:**

      1) Favorable review of a completed SF 86 by the authorized adjudicative agency;
      2) Citizenship verification;
      3) Initiation of an expedited investigation; and
      4) Completion and favorable review of a FBI fingerprint check.

   b. **Approvals for Temporary Eligibility for Critical-Sensitive and Special-Sensitive Positions require:**

      1) Favorable review of a completed SF 86 by the authorized adjudicative agency;
      2) Citizenship verification;
      3) Initiation of an expedited investigation; and
      4) Completion and favorable review of the following:

a) FBI fingerprint check;

b) FBI name check (initiation of the check is required prior to approval. Agencies may make a risk-based determination pending completed results); and

c) NCIC check.

2. Security personnel authorized by the agency head must:

   a. Include a justification of the temporary eligibility to hold a sensitive position; and

   b. Notify the covered individual in writing that further eligibility is expressly conditioned on:

      1) Favorable completion of an investigation; and

      2) Issuance of an eligibility approval.

3. Approvals shall remain valid until the exceptional circumstances have abated, the temporary eligibility is terminated, or final eligibility is granted. Temporary eligibility shall not exceed one year unless approved by security personnel authorized by the agency head. Justification for approved temporary eligibility exceeding one year shall be recorded and maintained by the granting agency.

J. TEMPORARY ELIGIBILITY TO HOLD A HIGHER LEVEL SENSITIVE POSITION:

1. Security personnel authorized by the agency head may approve temporary eligibility to hold a higher level sensitive position for a covered individual with eligibility to a lower level when determined necessary to meet operational or contractual exigencies not expected to be of a recurring nature pursuant to EO 12968, as amended.

2. Approvals shall remain valid until the exigency has abated or the eligibility is terminated. In any case, access shall not exceed 180 days.

3. If eligibility is expected to exceed 180 days, agencies must comply with the requirements in paragraph I above.

K. RESPONSIBILITIES:

1. The Director of the National Counterintelligence and Security Center (D/NCSC) shall:

   a. Develop and promulgate guidance and standards to implement this Directive as needed; and

   b. Oversee agency compliance and conduct periodic assessments to verify compliance with this Directive and subsequent guidance and standards.

2. Heads of agencies shall:

   a. Ensure policies and procedures governing the implementation of this Directive are in accordance with all applicable laws and EOs 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);

   b. Actively manage and mitigate all associated risks when balancing the need to grant temporary eligibility to meet mission requirements and the protection of national security;

   c. Record, track, and report temporary eligibility and one-time access based on supplemental reporting guidance issued by the D/NCSC;

   d. Maintain records documenting the:

      1) Nature of the requirement(s) that necessitated temporary eligibility prior to completion of the investigation and adjudication process; and the

      2) Date of expedited background investigation initiation.

   e. Maintain information access records when required;

   f. Act upon and share relevant information of a security, counterintelligence (CI), insider threat, or law enforcement concern with appropriate security, CI, insider threat, or law enforcement officials; and

   g. Terminate temporary eligibility or one-time access if disqualifying information is received at any time during the period of temporary eligibility or one-time access.

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

Richard A. Grenell
Acting Director of National Intelligence
Security Executive Agent

5/18/20
Date

APPENDIX: Requirements for One-time Access

A. CONFIDENTIAL, SECRET, AND "L" ACCESS:

1. The following information, including personally identifiable information (PII), shall be obtained from the individual and corroborated as required in the Federal Investigative Standards (FIS) prior to access authorization:
    a. Full name;
    b. Date and place of birth;
    c. Social security number;
    d. Other names used;
    e. Citizenship to include dual/multiple citizenship;
    f. Current address;
    g. Current employment;
    h. Police record; and
    i. Prior investigations and clearance.
2. The following records checks shall be conducted and favorably adjudicated prior to approving access:
    a. IC Scattered Castles (or successor);
    b. DoD JPAS (or successor);
    c. OPM CVS (or successor); and
    d. NCIC check.

B. TOP SECRET AND "Q" ACCESS:

1. The following information, including PII, shall be obtained from the individual and corroborated as required in the FIS prior to access authorization:
    a. Full name;
    b. Date and place of birth;
    c. Social security number;
    d. Other names used;
    e. Citizenship to include dual/multiple citizenship;
    f. Current address;
    g. Current employment;
    h. Foreign contacts;

i. Police record; and

j. Prior investigations and clearance.

2. The following records checks shall be conducted and favorably adjudicated prior to approving access:

a. IC Scattered Castles (or successor);

b. DoD JPAS (or successor);

c. OPM CVS (or successor);

d. FBI name check;

e. NCIC check; and

f. Intelligence Indices.