

PERSONNEL SECURITY PROGRAM

1. Purpose

This directive establishes Department of Homeland Security (DHS) policy for the Personnel Security Program.

2. Scope

This directive applies to all DHS organizational elements and to any organizational elements that do not have existing procedures and requirements regarding personnel security. Any organizational element that has existing personnel security procedures and requirements may continue them in force until the DHS Office of Security issues a Department-wide policy in this area.

3. Authorities

This directive is governed by numerous Executive Orders and other authorities, such as:

A. Executive Order Number 10450 provides the authority for conducting personnel security investigations. In brief, the order requires:

1. That the appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation;
2. That the scope of the investigation shall be determined according to the degree of adverse effect the occupant or applicant could bring about by virtue of the nature of the position occupied or sought;
3. That any position, the occupant of which could bring about a material adverse effect upon national security, be designated as sensitive; and that any position designated as sensitive shall be occupied only by a person with respect to whom a Single Scope Background Investigation (SSBI) has been conducted.

B. Director of Central Intelligence Directive (DCID) 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Sensitive Compartmented Information," provides the investigative and adjudicative requirements for personnel security investigations of persons requiring access to Sensitive Compartmented

Information (SCI).

- C. E.O. 12968, "Access to Classified Information".
- D. E.O. 12958, "Classified National Security Information".
- E. E.O. 12829, "National Industrial Security Program"

4. Definitions

A. **Single Scope Background Investigation (SSBI)**: The following is a listing of investigative factors that constitute the minimum requirements for an SSBI per OPM guidelines:

1. Personal Subject Interview
2. Employment/Self-employment/Unemployment coverage (7 years)
3. Education (3 years/verification of degree)
4. Residence (3 years)
5. Reference Contacts
6. Law Enforcement Checks (10 years)
7. Former Spouse(s) (10 years)
8. National Agency Checks (NAC)
 - Access to previous federal investigations through:
OPM's Security/Suitability Investigations Index (SII)
Defense Clearance and Investigations Index (DCII)
FBI Check
 - FBI National Criminal History Fingerprint Check
 - Credit Search of National Credit Bureaus (7 years)
 - Military Personnel Record Search (if applicable)
 - Citizen Verification
 - Spouse/Cohabitant NAC Searches

B. **Access National Agency Check and Inquires (ANACI)**: The following is a listing of investigative factors that constitute the minimum requirements for an ANACI per OPM guidelines:

1. Employment/Self-employment/Unemployment coverage (5 years - Inquiry)
2. Education (5 years Highest Degree - Inquiry)
3. Residence (3 years - Inquiry)
4. Reference Contacts (Inquiry)
5. Law Enforcement Checks (5 years Inquiry and/or record)
6. National Agency Checks (NAC)
 - Access to previous federal investigations through:
OPM's Security/Suitability Investigations Index (SII)
Defense Clearance and Investigations Index (DCII)
FBI Check
 - FBI National Criminal History Fingerprint Check
 - Credit Search of National Credit Bureaus (7 years)

-Military Personnel Record Search (if applicable)

C. **Minimum Background Investigation (MBI)**: The following is a listing of investigative factors that constitute the minimum requirements for a MBI per OPM guidelines:

1. Personal Subject Interview
2. Employment/Self-employment/Unemployment coverage (5 years - Inquiry)
3. Education (5 years Highest Degree - Inquiry)
4. Residence (3 years - Inquiry)
5. Reference Contacts (Inquiry)
6. Law Enforcement Checks (5 years - Inquiry)
7. National Agency Checks (NAC)
 - Access to previous federal investigations through:
OPM's Security/Suitability Investigations Index (SII)
Defense Clearance and Investigations Index (DCII)
FBI Check
 - FBI National Criminal History Fingerprint Check
 - Credit Search of National Credit Bureaus (7 years)
 - Military Personnel Record Search (if applicable)

D. **Sensitive Compartmented Information (SCI)**: National security information which by nature of acquisition or source necessitates special safeguarding, handling, and dissemination awareness and procedures. Access to SCI may be granted to employees upon:

1. Satisfactory completion and adjudication of the candidate's SSBI, to include those requirements contained within the DCID 6/4;
2. Acceptability of the candidate based upon adjudication and review of the candidate's personnel security file; and
3. Administration of a comprehensive briefing concerning SCI procedures.

E. **National Agency Check (NAC)**: A check of the following files by the Office of Personnel Management (OPM) or bureau entity with authorized personnel security functions and responsibilities:

1. FBI Identification Files;
2. FBI Investigative Files;
3. Defense Clearance and Investigations Index (DCII); and
4. OPM Investigative Files (including the Security-Investigations Index).

A complete NAC investigation requires submission of the applicant or subject's fingerprints.

F. **National Agency Check Equivalency**: A NAC without the benefit of the applicant or subject's fingerprints. This type of investigation is conducted in all personnel security investigations pending receipt of the full NAC investigation from OPM.

- G. **Applicant:** Any person applying for a civilian position in the Federal Government; OR any person appointed to or occupying a sensitive position prior to completion of an appropriate background investigation.
- H. **Personnel Security Officer:** Any personnel security official with authority to make final suitability and security determinations pursuant to Executive Order Number 10450 and to issue security clearances.
- I. **Sensitive Position:** Any position, the occupant of which could bring about (by virtue of the nature of the position) a material adverse effect on the national security. Sensitive positions are divided into categories of critical-sensitive, noncritical-sensitive, and special-sensitive based on the degree of adverse effect inherent in the position.
- J. **Nonsensitive Position:** Positions in which incumbents have only minimal opportunity to cause damage, realize personal gain, or perform illegal acts. Incumbents of nonsensitive positions may not be granted security clearances for access to national security information classified pursuant to Executive Order Number 12958.
- K. **Security Clearance:** A formal authorization for an employee with a specific "need-to-know" to have access to information that is classified as Confidential, Secret, "L" access authorization, "Q" access authorization, or Top Secret in the interest of national security or the defense of the United States.
- L. **Character:** A trait, or sum of traits, that serves as an index to the essential or distinctive nature of an individual. It is the aggregate of distinctive mental and moral qualities impressed by nature, education, and habit upon the individual.
- M. **Reputation:** The opinion or estimation in which one is generally held. Character is what a person is; reputation is what he or she is reported to be.
- N. **Loyalty:** One's faithful and true allegiance to the United States and its constitutional form of government.
- O. **Suitability:** The character, reputation, and fitness of those under consideration for Government employment.

5. Responsibilities

- A. The **Secretary:** shall designate a DHS Office of Security. The Office of Security will develop (as soon as practicable) appropriate DHS policy and guidelines regarding the minimum requirements of carrying out the responsibilities of this directive.
- B. The **Under Secretary for Management,** through the DHS Office of Security, shall be responsible for all aspects of this directive.
- C. **OPM** shall:

1. conduct NACs, and such related written inquiries as may be specified, for all personnel security investigations involving noncritical-sensitive, special-sensitive, and nonsensitive positions; and
2. conducting NACs for all personnel security investigations involving critical-sensitive positions.

6. Policy & Procedures

- A. Consistent with the interests of national security as prescribed within Executive Order Number 10450, the DHS Personnel Security Program serves as a means of inquiry into the background and activities of an individual, in order to develop information pertinent to the person's loyalty, character, emotional stability, trustworthiness, reliability, and suitability for a position of trust. Information developed is used:
1. to ensure an individual's access, or continued access, to sensitive, proprietary, or classified national security information;
 2. to ensure an individual's access to restricted areas or activities; and
 3. to determine an individual's security eligibility or acceptability for appointment to, or retention in, a sensitive position.
- B. Types of Personnel Security Investigations: The following four terms describe types of personnel security investigations:
1. Single Scope Background Investigation (SSBI) - A personally conducted comprehensive investigation designed to determine the full facts regarding an individual's background and activities so that a determination may be made regarding the individual's employment and the consistency of that employment with the interests of national security. Normally, SSBI's are of a basic 10-year scope, but some investigations may allow an investigative scope of less than 10 years or sometimes more. Investigative referrals of this type will in all instances specify the scope and content of investigations.
- Successful completion and acceptable adjudication of an SSBI may result in the approval and granting of a Top Secret security clearance or "Q" access authorization.
2. Limited Investigation - An investigation limited to certain selected elements, or investigative factors, providing lesser coverage than an SSBI but of sufficient scope to resolve discrepant information, prove or disprove any allegations developed, and obtain facts about an individual's activities that bear upon suitability for certain categories of employment.
- Completion of a limited investigation does not always result in a security clearance

being granted; persons hired on the basis of such investigations MUST NOT be granted access to classified or sensitive information unless a security clearance is granted. Supervisors will be held strictly accountable for violations in this regard.

3. Preliminary Investigation - A preliminary investigation consists of records checks and such other local investigation as may be specified on a case-by-case basis. A preliminary investigation may suffice to temporarily qualify certain applicants for employment pending completion and acceptance of an appropriate background investigation. Appointment of persons hired on the basis of a preliminary investigation will be made contingent upon the successful completion of an appropriate background investigation and the acceptability of that investigation.

4. Periodic Reinvestigation - Security clearance investigations must be updated at least every five years (Top Secret) or ten years (Secret). Normally, these update investigations are designed to cover an employee's activities during the period elapsed since the preceding investigation. However, the scope of these investigations is not necessarily limited to that period and will be appropriately expanded on a case-by-case basis to resolve issues.

- C. Personnel Security Program: The background investigative standard utilized by each DHS bureau or element should be commensurate with the position sensitivity designation and level of clearance necessary for the position. Any organizational element or bureau that transitioned into the DHS and has existing procedures and requirements for their personnel security program, may continue to use their existing procedures until otherwise notified by the DHS Office of Security.
- D. Any questions or concerns regarding this directive should be addressed to the DHS Office of Security.

Appendix A: Contractor Security

1. Purpose

This appendix establishes requirements for access investigations of contractor personnel requiring access to facilities, information systems, security items and products, and/or access Sensitive But Unclassified Information.

2. Scope

This directive applies to all DHS organizational elements and to any organizational elements that do not have existing procedures and requirements regarding personnel security. Any organizational element that has existing personnel security procedures and requirements may continue them in force until the DHS Office of Security issues permanent, Department-wide policy in this area.

3. Authorities

This directive is governed by numerous Public Laws and Executive Orders, such as:

- A. 5 U.S.C. Section 105
- B. E.O. 12968, "Access to Classified Information"
- C. E.O. 12958, "Classified National Security Information"
- D. E.O. 12829, "National Industrial Security Program"

4. Definitions

- A. **Contractors:** Employees of prime contractors, subcontractors, vendors, suppliers, and consultants that provide services to DHS or DHS elements.
- B. **Long-term access:** Recurring unescorted access to DHS or DHS element owned or controlled facilities, information systems, security items and products, and/or DHS Sensitive But Unclassified Information by a contractor employee.
- C. **Sensitive But Unclassified Information:** Information that requires protection due to the risk and magnitude of loss or harm that could result from the inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could reasonably be expected to cause damage to operations of the DHS, elements or its personnel.

5. Responsibilities

- A. The **Secretary**: shall designate a DHS Office of Security that, in conjunction with other appropriate Departmental Offices, will (as soon as practicable) coordinate and issue procedures consistent with this directive.
- B. The **Under Secretary for Management**, through the DHS Office of Security, is responsible for all aspects of this directive.

6. Policy & Procedures

Contractors who require DHS or DHS element facilities access must undergo a contractor access investigation. The purpose of the access investigation is to determine whether or not a contractor employee is a security risk before he or she is admitted to DHS or DHS element facilities.

Any organizational element having existing procedures and requirements for access investigations of contractor personnel requiring access to facilities, information systems, security items and products, and/or access to Sensitive But Unclassified Information may continue to use their existing procedures, until otherwise notified by the DHS Office of Security.

Any questions or concerns regarding this directive should be addressed to the DHS Office of Security.