DHS INSTRUCTION HANDBOOK 121-01-007
THE DEPARTMENT OF HOMELAND SECURITY PERSONNEL SUITABILITY AND SECURITY PROGRAM

APPROVAL DATE: JUNE 2009

DEPARTMENT OF HOMELAND SECURITY

OFFICE OF THE CHIEF SECURITY OFFICER

Jerry Williams
Chief Security Officer

6/18/09
Date

TABLE OF CONTENTS

CHAPTER 1, GENERAL

I. Purpose

This Instruction establishes procedures, program responsibilities, minimum standards, and reporting protocols for the Department of Homeland Security (DHS) Personnel Suitability and Security Program. It does not prohibit any DHS Component from exceeding the requirements. This Instruction implements the authority of the Chief Security Officer (CSO) under DHS Directive 121-01.

The Office of the Chief Security Officer (OCSO) is actively involved in the multiple U.S. Government Executive Branch initiatives to revise and consolidate the Personnel Suitability and Security programs. Accordingly, this Instruction will be revised as new Executive Orders and implementing guidance are issued.

II. Scope

This Instruction applies throughout DHS (except where exempt by statute), to DHS covered individuals (e.g., federal employees, applicants, excepted service federal employees, and contractor employees) providing support to DHS and who require unescorted access to DHS-owned facilities, DHS-controlled facilities, or commercial facilities operating on behalf of DHS; access to DHS information technology (IT) systems and the systems' data; or access to national security information. This Instruction defines the minimum standards for the DHS Personnel Suitability and Security Program, but does not prohibit any Component from exceeding these requirements based on mission or potential for adverse impact on National Security. Requests to lower any of the minimum standards set forth in this Instruction must be approved by the DHS CSO.

DHS Management Directive 11048, Suspension, Denial, and Revocation of Access to Classified Information and Management Directive 11050.2 , Personnel Security and Suitability Program are hereby canceled.

(Note: This Instruction does not address procedures for implementing Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors. Procedures for HSPD -12 will be the subject of a separate Instruction.)

III. Authorities

A. Title 5, United States Code, Section 552(a), "Records maintained on individuals" [The Privacy Act of 1974, as amended]

B. Title 5, United States Code (U.S.C.), Section 7532, "Suspension and

removal”

C. Executive Order 10450, as amended, “Security Requirements for Government Employment,” April 27, 1953

D. Executive Order 10577, as amended, “Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service,” November 22, 1954

E. Executive Order 12829, as amended, “National Industrial Security Program”, January 6, 1993

F. Executive Order 12958, as amended, “Classified National Security Information,” April 17, 1995

G. Executive Order 12968, as amended, “Access to Classified Information,” August 2, 1995

H. Executive Order 13311, as amended, “Homeland Security Information Sharing,” July 29, 2003

I. Executive Order 13467, as amended, “Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,” June 30, 2008

J. Executive Order 13488, “Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust,” January 16, 2009

K. Title 5, Code of Federal Regulations, Part 731, “Suitability”

L. Title 5, Code of Federal Regulations, Part 732, “National Security Positions”

M. Title 5, Code of Federal Regulations, Part 736, “Personnel Investigations”

N. Title 5, Code of Federal Regulations, Part 5, “Regulations, Investigation and Enforcement (Rule V)”

O. Title 5, Code of Federal Regulations, Part 752, “Adverse Actions”

P. Title 6, Code of Federal Regulations, Section 7.10, “Authority of the Chief Security Officer, Office of Security”

Q. Title 32, Code of Federal Regulations, Part 147, “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information”

R. Federal Acquisition Regulation (FAR), Part 4.4, “Safeguarding Classified Information within Industry”

S. Homeland Security Acquisition Regulation (HSAR), Part 3004.470, Security requirements for access to unclassified facilities, Information Technology resources and sensitive information”

T. National Security Affairs memorandum, “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,” December 29, 2005

U. Delegation of Authorities from the Assistant Deputy Director of National Intelligence for Security to Chief Security Officer, Department of Homeland Security, March 13, 2006

V. DHS Delegation 0102, “Delegation to Deputy Secretary – Procedures for Access to Classified Information”

W. DHS-Delegation 8001, “Delegation to the Chief, Office of Security, for Security Clearances of DHS Personnel”

X. DHS Sensitive Systems Handbook 4300A, Version 5.5, September 30, 2007

Y. DHS Sensitive Systems Policy Directive 4300A, September 20, 2007

IV. Definitions

Personnel security terms and definitions pertaining to this Instruction are located in Appendix B.

V. Responsibilities

A. ***The Chief, Personnel Security Division, Office of Security***, is responsible for:

1. Issuing Department-wide policy for the management and operation of the Personnel Suitability and Security Program.

2. Evaluating and reporting effectiveness of the DHS Personnel Security Program to the Chief Security Officer (CSO) and the Office of Management and Budget (OMB).

3. Chairing a DHS Personnel Security Working Group (PSWG) consisting of senior-level personnel security representatives from each DHS Component with a personnel security office.

4. Representing DHS interests in government-wide personnel suitability and security working groups.

5. Establishing and maintaining a departmental personnel security adjudicator training program.

6. Establishing and maintaining a departmental database for the tracking of personnel security cases.

7. Conducting compliance reviews of DHS Component personnel security programs.

8. Determining an employee's suitability and eligibility for access to classified information.

9. Communicating his or her findings regarding both suitability and eligibility for access to classified information to the Office of the Chief Human Capital Officer in order to ensure all applicants and employees are timely informed of the decision and how it may affect their prospective or current employment.

B. ***The Chief, Counterintelligence and Investigative Division, Office of Security***, is responsible for conducting investigations, on an as needed basis, in support of personnel security adjudications.

C. ***The Chief, Physical Security Division, Office of Security***, coordinates with the Office of Security, Personnel Security Division in the areas of fingerprint checks, issuance of employee and contractor access control passes and DHS identification media, and the implementation of Homeland Security Presidential Directive #12 (HSPD-12).

D. ***DHS Component Heads*** having a personnel suitability and security program are responsible for implementing and complying with the minimum standards required by this Instruction. This Instruction does not prohibit any Component from exceeding the requirements based on mission needs or the potential for an adverse impact on National Security. However, no Component may reduce the standards/requirements without prior approval of the DHS CSO.

E. ***DHS Chief Human Capital Officer (CHCO)*** coordinates with Office of Security, Personnel Security Division to establish acceptable position risk levels.

F. ***Under Secretary for Intelligence and Analysis*** is responsible for validating the "need to know" of the State and local personnel requesting a TOP SECRET clearance and/or SCI access against the specific mission requirements and compelling-need criteria outlined in this Instruction for all DHS Components

except for the U.S. Coast Guard and the Office of Security.

G. ***Chief Procurement Officer*** is responsible for ensuring that contracting officials and program officials consider whether personnel security or clearance requirements are applicable and insert appropriate agency or federal security program requirements in DHS solicitations, contracts, agreements, or other transactions.

DHS Contracting Officer's Technical Representatives (COTR) are authorized representatives of the contracting officer who are designated to perform certain contract administration functions or activities to include notifying contracting entities of the results of the fitness screening for individual contractor employees, and for notifying personnel security if a contractor employee's status changes in any way.

VI. Procedures

A. All covered individuals with unescorted access to DHS information or facilities undergo a suitability/fitness investigation and determination. Suitability/fitness is an assessment of an individual's character or conduct that may have an impact on promoting the efficiency and the integrity of the Federal service.

B. All DHS covered individuals are investigated commensurate with the position sensitivity as described in the OPM Position Sensitivity Designation Guidance. Investigations may be completed post-appointment/employment subject to the requirements outlined in the Chapters herein.

C. DHS affords fair, impartial, and equitable treatment to all contractor employees through the consistent application of fitness standards, criteria, and procedures as specified in applicable laws, regulations, and orders. DHS reserves the right to restrict access to DHS facilities, sensitive information, or resources, for any contractor employee. The decision of DHS does not intend to imply that the contractor employee's fitness for employment elsewhere is affected.

D. Determinations concerning access to classified information, and the denial or revocation of access to classified information, is based on the National Security Affairs memorandum, "Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," dated December 29, 2005 and Executive Order 12968, "Access to Classified Information," dated August 2, 1995, as amended. Pursuant to the Adjudicative Guidelines, "any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security."

E. Eligibility determinations conducted in accordance with Executive Order 12968 will be accepted by DHS without re-adjudication, unless there is substantial

information indicating an employee may not satisfy the Executive Order 12968 standards or exceptions outlined in OMB implementing guidance.

F. DHS is committed to sharing information with State and local personnel and may grant SECRET level clearances to State, local, private sector, and tribal personnel. On a case-by-case basis, the Chief Security Officer may grant or accept TOP SECRET clearances and/or access to SCI for State and local personnel.

G. A suspension of access to classified information is an administrative action and does not require the review procedures set forth in Executive Order 12968, Section 5.2. Denial or revocation of access to classified information is based on the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, Title 32, Code of Federal Regulations, Part 147 and those set out in Executive Order 12968, Section 5.2.

H. DHS is a member of the National Industrial Security Program (NISP), and as such reciprocally accepts security clearances granted to contractors by the Department of Defense Industrial Security Clearance Office (DISCO).

VII. No Private Right

This Instruction is an internal DHS document. It is not intended to, and does not create any rights, privileges or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, or its officers, employees or any other person.

VIII. Questions

Address all questions or concerns regarding this Instruction to the Office of Security, Personnel Security Division.

CHAPTER 2, FEDERAL EMPLOYEE/APPLICANT SUITABILITY REQUIREMENTS

Scope: This chapter defines the suitability requirements for federal employees, applicants, and excepted service positions where the incumbent can be noncompetitively converted to the competitive service and career appointments into a position in the Senior Executive Service, as defined in 5 C.F.R. §731.101(b) (effective June 16, 2008).

Pursuant to the authority delegated by the President of the United States under 5 U.S.C. sections 1104 and 3301, Executive Order 10577, and 5 C.F.R. § 731, individuals seeking admission to the civil service must undergo an investigation to establish their suitability for employment. Suitability adjudication, denial, and due process procedures are conducted in accordance with 5 C.F.R. § 731.

The suitability process determines an individual's suitability for employment based upon an assessment of their character or conduct that may have an impact on the integrity or efficiency of the Federal service. This differs from the issue of whether a person is "qualified" to do the job. Qualification determinations are based on an individual's experience, education, knowledge, skills, and abilities rather than on character traits and conduct.

Security clearances (e.g., Confidential, Secret, Top-Secret) on the other hand, are granted to individuals with a specific requirement for access to classified material and require a separate investigation, adjudication, and determination (see Chapter 4).

1. Suitability Risk Assessment:

   A. Federal Employees/applicants requiring access to DHS facilities, IT systems, or Sensitive Information receive an appropriate investigation based on the risk level of their positions.

   B. In accordance with 5 C.F.R. Part 731, the following criteria are used to determine the risk levels for each position occupied by a federal employee:

      (1) High Risk: High Risk positions have the potential for exceptionally serious impact on the integrity and efficiency of Federal service. These positions involve duties that are especially critical to the agency or the program mission with a broad scope of responsibility and authority.

(2) Moderate Risk: Moderate Risk positions have the potential for moderate to serious impact on the integrity and efficiency of Federal service. These positions involve duties that are considerably important to the agency or program mission with significant program responsibility or delivery of service.

(3) Low Risk: Low Risk positions have the potential for limited impact on the integrity and efficiency of Federal service. These positions involve duties and responsibilities of limited relation to the agency or program mission.

C. Appendix A outlines the security forms, background investigations, and preliminary checks required for DHS federal employees/applicants at each risk level.

2. Suitability Investigative Requirements:

A. The minimum investigative standard for a Low Risk position is a National Agency Check with Inquiries (NACI).

B. The minimum investigative standard for a Moderate Risk Public Trust Position is a Minimum Background Investigation (MBI).

C. The minimum investigative standard for a High Risk Public Trust Position is a Background Investigation (BI).

3. Suitability Adjudicative Criteria:

A. Entry on Duty Determinations (EOD). Subject to the below requirements, DHS Component Security Offices may implement procedures for making EOD determinations. A favorable EOD determination is a risk management decision that allows the federal employee/applicant to commence work before the required background investigation is completed. The investigation should be initiated before appointment, but no later than 14 calendar days after placement in the position. The EOD determination does not substitute for the required background investigation. In addition, if a federal employee/applicant is entering a High Risk IT position (for example, system administrator, programmer, hardware technician, or firewall manager) and receives a favorable EOD determination, the federal employee/applicant may only perform duties equivalent to Moderate Risk positions until the required background investigation is completed.

B. Suitability is a consideration for every position covered by this Instruction. Suitability determinations are made in accordance with 5 C.F.R. § 731.202. When making a determination, the following may be considered as a basis for finding a federal employee/applicant unsuitable:

(1) Misconduct or negligence in employment;
(2) Criminal or dishonest conduct;
(3) Material, intentional false statement or deception or fraud in examination or appointment;
(4) Refusal to furnish testimony as required by 5 C.F.R. § 5.4;
(5) Alcohol abuse, without evidence of substantial rehabilitation, or a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;
(6) Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;
(7) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force;
(8) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

C. In making a suitability determination, DHS Component Security Offices consider the following additional considerations to the extent they deem these considerations pertinent to the individual case:

(1) The nature of the position for which the person is applying or in which the person is employed;
(2) The nature and seriousness of the conduct;
(3) The circumstances surrounding the conduct;
(4) The recency of the conduct;
(5) The age of the person involved at the time of the conduct;
(6) Contributing societal conditions; and
(7) The absence or presence of rehabilitation or efforts toward rehabilitation.

D. When a Federal employee/applicant is found unsuitable for Federal employment, the following actions may be taken: cancellation of eligibility, denial of appointment, removal, cancellation of reinstatement eligibility, or debarment.

E. Reinvestigations. Federal employees in High Risk positions are reinvestigated every five years, or more frequently as circumstances warrant. Federal employees in Moderate or Low Risk positions are reinvestigated every ten years, or more frequently as circumstances warrant. See Appendix A.

F. Fingerprinting:

(1) Fingerprints are required for all initial investigations. Fingerprints can be taken by DHS security personnel; or Federal, State, or local law enforcement personnel.

(2) Unless electronic fingerprinting devices are available, the Federal Fingerprint Card (SF-87) is used and requires the signature of the person fingerprinted and the signature of the person who took the fingerprints. DHS Component security office personnel review all fingerprints to ensure that this requirement is met and that the signature on the fingerprint card of the person being fingerprinted appears to match the signature on the submitted forms.

G. Standards for Using Previous Investigations. Some federal employees/applicants may have already been investigated by another Federal agency. DHS Components use these investigations whenever practicable to reduce the number of investigation requests, associated costs, and unnecessary delays. The following standards for use of these investigations apply:

(1) New forms are obtained and pre-employment checks completed.

(2) Any investigation conducted by, or for, another Federal agency on a federal employee/applicant that is of the same or higher risk and scope as the one required, is sufficient to meet the investigative requirements if it was conducted within the past five years. If that investigation is unavailable, a new, appropriate investigation is completed. The investigation is obtained and reviewed in conjunction with pre-employment checks to make a suitability decision for employment in accordance with the Adjudicative Criteria paragraph above.

(3) Any investigation conducted by, or for, another Federal agency on a federal employee/applicant the scope of which is less than that required for DHS employment is upgraded to meet the investigative requirements of the position if the investigation was conducted within the past five years, or a new investigation is initiated.

H. Derogatory Information:

(1) When adverse information is developed in the course of an investigation, the scope of the inquiry is normally expanded to the extent necessary to obtain such additional information as may be required to determine whether the federal employee/applicant is granted unescorted access to DHS facilities and sensitive information.

(2) A Federal employee/applicant on whom unfavorable or derogatory information is developed is notified of the information in writing via a Notice of Proposed Action (NOPA), to include copies of all records and reports relied upon, and offered an opportunity to refute, explain, clarify, or mitigate the information in question. The Federal employee/applicant answers the charges in writing and furnishes documentation and/or affidavits in support of the response within 30 calendar days after the date of the NOPA. If an unfavorable determination is made the servicing Human Capital Office is formally notified and informed of the reason(s).

I. Citizenship Requirements:

(1) As outlined in DHS MD 3120.2, Employment of Non-Citizens, the Federal Government gives strong priority to hiring United States citizens and nationals, but non-citizens may be hired in certain circumstances. Components considering non-citizens for Federal employment in the competitive service follow usual selection procedures and ensure compliance with all three of the following: applicable immigration laws; any applicable appropriations act ban on paying certain non-citizens; and any executive order restriction on appointing non-citizens in the competitive service. Components considering non-citizens for Federal employment in the excepted service and Senior Executive Service ensure compliance with immigration laws and any applicable appropriations act ban. In addition, Components are responsible for applying any citizenship requirements that may appear in their individual Component authorization and appropriations laws.

(2) Only U.S. citizens are eligible for federal employment positions requiring access to DHS IT systems that are involved in the development, operation, management, or maintenance of DHS IT systems, unless a waiver is granted in accordance with the Waiver Section K of this chapter.

J. Investigation Residency Requirements:

For a federal employee/applicant who has resided outside of the United States for more than two of the last five years preceding DHS employment, there must be U.S. citizen sources who can verify his/her reportable activities (e.g., places of residence, educational institutions attended, etc.) outside the United States within this five-year period. Sufficient verifiable information is required for such an investigation, using the same standard as would be required if the individual resided within the United States. Otherwise, the individual is ineligible to work in that position. These residency requirements do not apply to those

individuals who work or worked for the United States Government in foreign countries in Federal or military capacities or were or are dependents of Federal or military employees serving in foreign countries.

K. Waivers:

(1) A waiver of the U.S. citizenship requirement noted in paragraph 3.I.(2) above may only be granted by the head of the Component or designee, with the concurrence of both the DHS CSO and CIO or their designees. Components receiving personnel security services directly from the OCSO may only be granted a waiver with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted, all of the following are required:

(a) The individual is either a Lawful Permanent Resident of the United States or a citizen of the Republic of Ireland, Israel, or any nation on the Allied Nations List maintained by the Department of State;

(b) All required security forms specified by DHS and any necessary background check are satisfactorily completed;

(c) There is a compelling reason for using this individual as opposed to a U.S. citizen; and

(d) The waiver is in the interest of DHS.

(2) Requests for waivers of any other requirement set forth herein, to include surge support and resource issues, are submitted in writing to the DHS Chief Security Officer. Waiver requests include a justification, and are considered on a case-by-case basis.

CHAPTER 3, EXCEPTED SERVICE FEDERAL EMPLOYEE AND CONTRACTOR EMPLOYEE FITNESS REQUIREMENTS

Scope: This chapter defines the fitness requirements for excepted service federal employees in positions that do not noncompetitively convert to competitive service positions and contractor employees (at any tier) requiring unescorted access to DHS-owned facilities, DHS-controlled facilities, or commercial facilities operating on behalf of DHS; access to DHS information technology (IT) systems and the systems' data; or access to Sensitive Information (as defined herein). This Instruction defines the minimum standards, but does not prohibit any DHS Component from exceeding the requirements.

1. Fitness Risk Assessment:

A. Excepted service federal employees and contractor employees having access to DHS facilities, IT systems, or Sensitive Information receive an appropriate fitness screening, based on the risk level of their positions.

B. The DHS program official or Chief Human Capital official, and the security office within each DHS Component with sufficient authority, responsibility, and knowledge of the acquisition is responsible for determining the risk level for each excepted service or contractor employee position. [Note: The DHS program official coordinates with the DHS Contracting Officer to ensure that solicitations and contracts include appropriate requirements for contractor personnel.] The risk level is based on an overall assessment of the damage that an untrustworthy individual could cause to the efficiency or the integrity of DHS operations. When determining risk levels, program officials may compare the individual's duties, responsibilities, and access with those of DHS federal employees in similar positions.

C. Risk levels for each position occupied by an excepted service Federal employee or contractor employee are determined using the following criteria:

(1) High Risk: High Risk positions have the potential for exceptionally serious impact on the integrity and efficiency of Federal service. These positions involve duties that are especially critical to the agency or the program mission with a broad scope of responsibility and authority.

(2) Moderate Risk: Moderate Risk positions have the potential for moderate to serious impact on the integrity and efficiency of Federal service. These positions involve duties that are considerably important to the agency or program mission with significant program responsibility or delivery of service.

(3) Low Risk: Low Risk positions have the potential for limited impact on the integrity and efficiency of Federal service. These positions involve duties and responsibilities of limited relation to the agency or program mission.

D. Appendix A outlines the security forms, background investigations, and preliminary checks required for DHS excepted service federal employees and contractor employees at each risk level.

2. Fitness Investigative Requirements:

A. The minimum investigative standard for a Low Risk position is a National Agency Check with Inquiries (NACI).

B. The minimum investigative standard for a Moderate Risk Public Trust Position is a Minimum Background Investigation (MBI).

C. The minimum investigative standard for a High Risk Public Trust Position is a Background Investigation (BI).

3. Fitness Adjudicative Criteria:

A. Entry on Duty Determinations (EOD). Subject to the below requirements, DHS Component Security Offices may implement procedures for making EOD determinations. A favorable EOD determination is a risk management decision that allows the excepted service federal employee or contractor employee to commence work before the required background investigation is completed. The investigation should be initiated before appointment, but no later than 14 calendar days after placement in the position. The EOD determination does not substitute for the required background investigation. In addition, if an individual entering a High Risk IT position (for example, system administrator, programmer, hardware technician, or firewall manager) receives a favorable EOD determination, the individual may only perform duties equivalent to Moderate Risk positions until the required background investigation is completed.

B. When making a fitness determination, the following may be considered as a basis for finding an excepted service federal employee or contractor employee unfit:

(1) Misconduct or negligence in employment;
(2) Criminal or dishonest conduct;
(3) Material, intentional false statement or deception or fraud in examination or appointment;
(4) Refusal to furnish testimony;

(5) Alcohol abuse, without evidence of substantial rehabilitation, or a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;
(6) Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;
(7) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force;
(8) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

C. In making a fitness determination, DHS Component Security Offices consider the following additional considerations to the extent they deem these considerations pertinent to the individual case:

(1) The nature of the position for which the person is applying or in which the person is employed;
(2) The nature and seriousness of the conduct;
(3) The circumstances surrounding the conduct;
(4) The recency of the conduct;
(5) The age of the person involved at the time of the conduct;
(6) Contributing societal conditions;
(7) The absence or presence of rehabilitation or efforts toward rehabilitation.

D. An excepted service federal employee or contractor employee's eligibility to perform work, for, or on behalf of the Department may be cancelled, or an individual may be removed when the fitness determination finds that the individual is not fit for the reason(s) cited above.

E. Reinvestigations. Excepted service federal employees and contractor employees in High Risk positions are reinvestigated every five years or more frequently as circumstances warrant. Individuals in Moderate or Low Risk positions are reinvestigated every 10 years or more frequently as circumstances warrant. See Appendix A.

F. Fingerprinting:

(1) Fingerprints are required for all investigations. Fingerprints can be taken by DHS security personnel, or Federal, State, or local law enforcement personnel.

(2) Unless electronic fingerprinting devices are available, the Fingerprint Card (FD-258) is used and requires the signature of the person fingerprinted and the signature of the person who took the

fingerprints. Component security office personnel review all FD-258s to ensure that this requirement is met and that the signature on the FD-258 of the person being fingerprinted appears to match the signature on the submitted forms.

G. Standards for Using Previous Investigations. Some excepted service federal employees or contractor employees may have already been investigated by another Federal agency. Components use these investigations whenever practicable to reduce the number of investigation requests, associated costs, and unnecessary delays. The following standards for use of these investigations apply:

(1) New forms are obtained and pre-employment checks completed.

(2) Any investigation conducted by, or for, another Federal agency on an excepted service federal employee or a contractor employee that is of the same or higher type and scope as the one required is sufficient to meet the investigative requirements if it was conducted within the past five years. The investigation is obtained and reviewed in conjunction with pre-employment checks to make a fitness decision for employment in accordance with the Adjudicative Criteria paragraph above. If that investigation is unavailable, a new, appropriate investigation is completed.

(3) Any investigation conducted by, or for, another Federal agency on an excepted service federal employee or contractor employee, the scope of which is less than that required for DHS work, is upgraded to meet the investigative requirements of the position if the investigation was conducted within the past five years, or a new investigation is initiated.

H. Derogatory Information:

(1) When adverse information is developed in the course of an investigation, the scope of the inquiry is normally expanded to the extent necessary to obtain such additional information as required to determine whether the excepted service federal employee or contractor employee is granted unescorted access to DHS facilities and sensitive information.

(2) An excepted service federal employee or contractor employee on whom unfavorable or derogatory information is developed is notified of the information in writing via a Notice of Proposed Action (NOPA) to include copies of all records and reports relied upon, and offered an opportunity to refute, explain, clarify, or mitigate the information in question. The individual answers the charges in writing and furnishes documentation and/or affidavits in support of the response within 30

calendar days after the date of the NOPA.

(3) Derogatory information is not disclosed to the contractor's employer. When a final determination is made, the DHS Program Office and/or the Contracting Officer is informed simultaneously with notification to the affected individual that the contractor employee is ineligible to render services or otherwise perform under the DHS contract. The decision of DHS is not intended to imply that the contractor employee's fitness for employment elsewhere is affected.

I. Citizenship Requirements:

(1) Only U.S. citizens (not Lawful Permanent Residents) are eligible for employment on contracts requiring access to DHS IT systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver is granted in accordance with Section K below.

(2) Only U.S. citizens and Lawful Permanent Residents are eligible for employment on contracts requiring access to sensitive information unless a waiver is granted in accordance with Section K below.

J. Investigation Residency Requirements:

For excepted service federal employees or contractor employees who have resided outside of the United States for more than two of the last five years preceding DHS employment, there must be U.S. citizen sources who can verify their reportable activities (e.g., places of residence, educational institutions attended, etc.) outside the United States within this five-year period. Sufficient verifiable information is required for such investigations, using the same standard as would be required if the individuals resided within the United States. Otherwise, the individuals are ineligible to work in those positions. These residency requirements do not apply to those individuals who work or worked for the United States Government in foreign countries in Federal or military capacities or were or are dependents of Federal or military employees serving in foreign countries.

K. Waivers:

(1) The waivers of the U.S. citizen requirement noted in paragraph 3.I.(2) above may only be granted by the head of the Component or designee, with the concurrence of both the DHS CSO and CIO or their designees. Components receiving personnel security services directly from the OCSO may only be granted a waiver with the approval of both the CSO and the CIO or their designees. In order for a waiver to be

granted, all of the following are required:

(a) The individual is a Lawful Permanent Resident of the United States;

(b) All required security forms specified by DHS and any necessary background check are satisfactorily completed;

(c) There is a compelling reason for using this individual as opposed to a U.S. citizen; and,

(d) The waiver is in the interest of DHS.

(2) Requests for waivers of any other requirement set forth herein, to include surge support and resource issues, are submitted in writing to the DHS Chief Security Officer. Waiver requests include justification and are considered on a case-by-case basis.

CHAPTER 4, SECURITY CLEARANCE REQUIREMENTS

Scope: This chapter defines the national security clearance requirements for federal employees, applicants, excepted service federal employees and contractor employees who require SCI access.

Access to classified information is limited to persons whose official duties require knowledge or possession of the information. No one has a right to have access to classified information solely by virtue of office, rank, or position. Access to classified information is based upon: (1) granting of a security clearance following the completion and favorable adjudication of an investigation commensurate with the level of access required for the position; (2) completing an initial National Security Information indoctrination briefing; (3) executing an SF-312, "Classified Information Nondisclosure Agreement" form; and (4) verifying an official "need to know."

A Security Clearance is a determination that a person is able and willing to safeguard classified national security information. This determination is a separate process from that of an employment suitability determination. If an individual is found suitable, and the position is designated at a national security sensitivity level, the security clearance criteria is applied to determine if the individual meets the standards for access to classified information. Interim access to SECRET classified information may be granted when there is an intention to grant a final security clearance once the pending background investigation is completed and favorably adjudicated.

As a basis for granting access authorization, DHS will accept verification that a covered individual currently has a security clearance and/or SCI access approval granted by another Federal agency, provided the investigative basis for the previous security clearance/SCI access approval meets the scope of the investigation required for DHS access authorization and that the investigation is in scope.

1. Position Sensitivity Designation:

   A. All positions within DHS are designated using the OPM Position Sensitivity Designation Guidance.

   B. All DHS federal employees/applicants (competitive and excepted service) are investigated commensurate with the position sensitivity as described in the OPM Position Sensitivity Designation Guidance.

   C. The supervising official with sufficient knowledge of duty assignments is responsible for assigning position sensitivity designations. Designations are subject to final approval by the Component's respective Personnel Security Office. The DHS Office of Security retains the position sensitivity designation authority for:

(1) All Presidential appointees in the Department requiring confirmation by the Senate, to the extent of the Department's authority with respect to these officials;

(2) Under Secretaries and their primary deputies; and

(3) Component personnel security officers and any official with delegated authority to grant security clearances.

D. Positions may be designated either as public trust positions or national security positions.

E. DHS federal employees (competitive and excepted service) who are reassigned or promoted to higher position/job descriptions may need a higher level of investigation.

2. Investigative Requirements:

A. The minimum investigative standard for a non-critical sensitive position with a SECRET clearance requirement is a Minimum Background Investigation (MBI).

B. The minimum investigative standard for a critical or special sensitive position with a TOP SECRET or TS/SCI clearance requirement is a Single Scope Background Investigation (SSBI).

C. DHS does not grant or accept interim TOP SECRET clearances.

D. All federal employees/applicants requiring access to classified information are required to complete the Standard Form (SF) 86 "Questionnaire for National Security Positions", if the prior investigation does not meet the standards for the position.

E. National Security adjudications and due process are in accordance with E.O. 12968, "Information Security Oversight Office (ISOO) Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," December 29, 2005, and, if necessary, the Director of Central Intelligence Directive (DCID) 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," July 2, 1998.

F. Investigations should be initiated **before** appointment or, if necessary, not later than 14 calendar days after placement in the position as outlined in 5 C.F.R. 736.201(c).

G. For those positions designated as National Security Positions, post-appointment/employment investigations are initiated, provided that following requirements are met:

(1) For positions designated Non-Critical Sensitive, investigations are initiated post appointment following favorable review of the Standard Form (SF) 86 and pre-employment checks.

(2) For positions designated Critical Sensitive, investigations are completed pre-appointment/employment or post appointment with a waiver provided that:

(a)The SF 86 is completed and the required investigation has been initiated (if applicable) within 14 days of appointment.

(b) Checks of the Security/Suitability Investigations Index (SII) at OPM and the Defense Clearance and Investigations Index (DCII), PIPS/CVS, have been completed (if applicable). If a recent investigation exists (within the previous five years) the employing agency obtains and reviews before entry on duty approval is granted.

(c) Fingerprint check results and for those Components with law enforcement authority, NCIC results have been received.

(d) Credit check results have been received.

(e) CIS system checks of the for foreign born relatives or connections have been completed, if needed.

(f) All of the above checks are favorable. If any derogatory information exists the investigation is completed and favorably adjudicated prior to entry on duty.

H. The pre-appointment investigative requirement may not be waived for appointment to positions designated as Special Sensitive under 5 C.F.R. Part 732.

I. Break in Service. If a federal employee/applicant who requires access to classified information has been retired or separated from U.S. Government

employment for less than two years and is the subject of an investigation that is otherwise current (within the past five years), the agency may grant access following, at a minimum, a review of an updated SF 86 and applicable records. A reinvestigation is not required unless the review indicates that the individual may no longer satisfy the standards of Executive Order 12968.

J. Reinvestigations. An SSBI-PR is conducted every five years for TOP SECRET and SCI eligibility. An ANACI is conducted every 10 years for SECRET. See Appendix A.

K. Reciprocity. Eligibility determinations conducted in accordance with Executive Order 12968 are accepted by DHS without re-adjudication, unless there is substantial information indicating that an individual covered by this Chapter may not satisfy the Executive Order 12968 standards. Further investigation is only conducted to meet required reinvestigation or security clearance revalidation requirements, or if derogatory information exists. DHS follows the standards in accordance with E.O. 12968, the Intelligence Reform and Terrorism Prevention Act of 2004, and OMB Memorandum "Reciprocal Recognition of Existing Personnel Security Clearances," dated December 12, 2005.

3. Access to Classified Information:

A. Eligibility for access to classified information is granted in accordance with Executive Order 12968, as amended. Access is not granted unless the individual covered by this Chapter has:

(1) Demonstrated a "need-to-know" the information in order to do his/her job.

(2) Undergone the requisite background investigation required for the level of access;

(3) Been adjudicated under the National Security Affairs memorandum, "Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," dated December 29, 2005 and Adjudicative Standards set forth in 32 C.F.R. § 147, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," to determine their eligibility for access to classified information

(4) Been adjudicated under the Adjudicative Standards set forth in DCID 6/4, Annex C for individuals covered under this Chapter who are eligible for SCI access.

(5) Signed a Classified Information Non-Disclosure Agreement (SF

312); and,

(6) Been briefed regarding the responsibilities associated with access to classified information.

These Guidelines apply to all individuals covered by this Chapter being considered for initial or continued eligibility for access to classified information and are used in all security clearance determinations. In the event an individual fails or ceases to meet the standards for a security clearance, he/she is provided with the appropriate due process in accordance with the applicable law, rule, and/or regulation.

B. Temporary Access. In accordance with Section 2.1(b) (3) of Executive Order 12968, temporary eligibility for access to classified information may be granted when there is a temporary need, such as one-time participation in a classified project, provided the investigative standards under Executive Order 12968 have been satisfied. In such cases, the expiration of this temporary access is identified by a fixed date or event, and access to classified information is limited to that related to the particular project or assignment.

C. Interim Access:

(1) Interim access to SECRET classified information may be granted when there is an intention to grant a final security clearance once the pending background investigation is completed and favorably adjudicated. At a minimum, eligibility requires completion of the SF 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, NCIC check, credit check, and fingerprint submission.

(2) DHS does not grant or accept interim TOP SECRET clearances.

D. Waiver Requests. Any request for exemptions to the above requirements are submitted, in writing, to the Office of Security, Chief Security Officer. Waiver requests should include a justification, and are considered on a case-by-case basis.

CHAPTER 5, STATE, LOCAL, AND PRIVATE SECTOR PROGRAM REQUIREMENTS

Scope: This chapter defines the national security clearance requirements for State, Local, Private Sector, Territorial and Tribal entities.

1. Eligibility for State, Local, Private Sector, Territorial and Tribal:

   A. Most State, local, private sector, territorial, and tribal clearances are granted at the SECRET level.

   B. When possible, the majority of information that DHS shares with State and local government officials is communicated at the unclassified level.

   C. State and Territorial Governors and their respective Homeland Security Advisor (HSA) are authorized to receive TOP SECRET clearances. Other positions may be granted TOP SECRET clearances based on a "need-to-know" and as approved by the sponsoring DHS Component.

   D. Interim SECRET clearances may be granted when official actions need to be performed before completion of investigative and adjudicative processes associated with security clearance procedures.

   E. DHS does not grant or accept interim TOP SECRET clearances.

2. Eligibility for State and Local Personnel to Gain SECRET/TOP SECRET Clearances and/or Access to SCI:

   A. DHS policy is to grant access to State, local, private sector, territorial, and tribal personnel at the SECRET level. On a case-by-case basis, according to the compelling-need criteria outlined in Section 3 below, the DHS Chief Security Officer may grant or accept TOP SECRET clearances and/or access to SCI.

   B. The granting of TOP SECRET clearances and/or access to SCI is in accordance with Executive Order 12968, as amended, "Access to Classified Information" and DCID 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to SCI," and/or subsequent guidance issued by the Director of National Intelligence (DNI).

C. State and local personnel who do not have a current, within scope Single Scope Background Investigation (SSBI) or TOP SECRET security clearance and/or SCI eligibility, granted by either DHS or another authorized Federal agency, are processed for an updated (periodic review) or first-time investigation provided they are eligible per the criteria below. The sponsoring DHS Component is responsible for the cost of the investigation and any required re-investigation; the Office of Security is responsible for the costs associated with administering the clearance.

D. In accordance with executive order and statute, reciprocity provisions apply to the investigations and adjudications for security clearances granted to State and local personnel; however, unless approved by the DHS Chief Security Officer pursuant to the compelling-need criteria below, access is limited to the SECRET level.

E. All Federal and DHS policies and requirements to safeguard classified information apply to State and local personnel granted TOP SECRET clearances and/or who are eligible for access to SCI.

3. Specific Criteria for Granting Top Secret Clearances and/or Access to SCI:

A. Prior to DHS granting a TOP SECRET clearance and/or access to SCI, the sponsoring Component requires a formal written agreement that individuals assigned by a State or local agency will serve as integrated detailees to DHS for a minimum of 12 months over a 36-month period from the date the clearance and/or access is granted.[1] The DHS Office of Security may waive the 12-month requirement on a case-by-case basis.

B. The granting of TOP SECRET clearances and/or the granting of eligibility for access to SCI is limited to:

(1) Personnel identified by the DHS Chief Intelligence Officer. These personnel will represent a cross-section of States and Urban Area Security Initiative cities and will perform the following functions:

(a) Enhance the intelligence analysis process by identifying intelligence information of interest to State and local authorities.

(b) Assist in the dissemination of sanitized intelligence products to the appropriate State and local customers.

[1] The 12-month requirement does not apply to individuals with an in scope SSBI or current Top Secret and/or SCI access granted by another authorized Federal agency.

(2) Law enforcement officers identified by the Director, Office of Operations Coordination or the Director, National Operations Center (NOC) who will perform the following regionally oriented functions at the NOC:

(a) Assess U.S. focused reporting with a potential nexus to terrorism and provide significant insights regarding tactics, techniques, and procedures potentially employed by terrorists.

(b) Enhance the operational process by identifying the capability of State and local law enforcement to respond and apply countermeasures to identified tactics, techniques, and procedures.

4. Extended Absences:

The sponsoring Component ensures that the DHS Office of Security is promptly notified of any absence exceeding 30 days. Personnel absent longer than 30 days are debriefed in accordance with the DHS SCI Administrative Handbook. For absences longer than 60 days, the individual is debriefed from all SCI access until his/her return. The debriefing is documented but no re-justification (Request for Access) is necessary if the individual returns to the same duty position. Furthermore, the individual may retain his/her DHS Office of Security issued access control card during the absence.

5. Denial or Revocation of a Security Clearance:

Final determinations concerning access to classified information, and the denial or revocation of access to classified information, is conclusive and not subject to review or appeal.

6. Reinvestigations:

A periodic reinvestigation is conducted every five years for TOP SECRET and SCI eligibility. An ANACI is conducted every 10 years for SECRET. See Appendix A.

CHAPTER 6, SUSPENSION, DENIAL, AND REVOCATION OF ACCESS TO CLASSIFIED INFORMATION

Scope: The procedures in this chapter apply to all DHS Federal employees (both competitive and excepted service) and contractor employees with SCI access. It does not apply to non-SCI contractor personnel, State and local government personnel, or private-sector individuals. It also does not apply to decisions to suspend access to DHS facilities, sensitive information, and information technology systems. This chapter creates no procedural or substantive rights.

1. Denial or Revocation of Security Clearance:

Determinations concerning access to classified information, and the denial or revocation of access to classified information, is based on the National Security Affairs memorandum, “Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,” dated December 29, 2005 (hereinafter Adjudicative Guidelines). Pursuant to the Adjudicative Guidelines, "any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security."

2. Deciding Authority:

DHS review officials for personnel security determinations regarding suspension, revocation, denial, granting, or reinstatement include:

- ***First-Level Deciding Authority***: The person with responsibility for the implementation and management of the Personnel Security Program within the DHS Component Security Office. For the Office of the Secretary and those Components without security offices, the First-Level Deciding Authority is the Chief of the Personnel Security Division, DHS Office of Security.

- ***Second-Level Deciding Authority***: A supervisor of the First-Level Deciding Authority within the DHS Component Security Office. For the Office of the Secretary and those Components without security offices, the Second-Level Deciding Authority is the DHS Chief Security Officer or his or her designee.

- ***Third-Level Deciding Authority***: The Security Appeals Board. For each denial or revocation matter, the Board is comprised of three high-level officials appointed by the Secretary or his or her designee. Two of these members are selected from outside the security field, in accordance with Executive Order 12968.

The following procedural requirements apply when a DHS Federal employee, excepted service Federal employee, or contractor employee with SCI access has been denied access to classified information or has had their access to classified information revoked:

3. Notice of Determination:

A. The First-Level Deciding Authority provides a written Notice of Determination that:

(1) Informs the individual that his or her access to classified information has been denied or revoked.

(2) Includes a written explanation for the determination to the extent permitted by law, as required by Executive Order 12968.

(3) States the name and office address of the Second-Level Deciding Authority to whom the individual should direct any reply, request, or filing.

(4) Informs the individual of his or her right to be represented by counsel or other representative at his or her own expense.

(5) Advises the individual that they may request documents, records, and reports upon which the denial or revocation was based; and/or request a copy of the entire investigative file, as permitted by the applicable laws and regulations, including Executive Order 12968.

(a) These documents, records, and reports must be requested no later than 15 calendar days following the receipt of the Notice of Determination.

(b) If requested, the documents, records, and reports are made available to the extent they would be available if requested under the Freedom of Information Act, Title 5, United States Code, Section 552, or the Privacy Act of 1974, Title 5, United States Code, Section 552a, and as permitted by national security and other applicable laws.

(6) Advises the individual that he/she may reply in writing and may request a review of the determination.

(a) If the individual requests documents, records, or reports, the written reply must be submitted within 30 calendar days of the date of final notification that all documents relied upon have been provided.

(b) If the individual does not request documents, records, or reports, the written reply must be submitted within 30 calendar days of the date of the Notice of Determination.

(7) Advises the individual that they may request to appear personally, or via telephone or teleconference, before the Second-Level Deciding Authority and to present relevant documents, materials, and information at that time. A request to appear personally must be made within 30 calendar days following the date of the Notice of Determination, or 30 calendar days from the date of final notification that all documents relied upon have been provided if the individual requested documents, reports, or records.

(a) Travel expenses and any associated costs are incurred by the individual.

(b) The individual and his or her representative, the Second-Level Deciding Authority, counsel advising the Component, and administrative support personnel requested by the Second-Level Deciding Authority are permitted to attend the personal appearance. A court reporter may be present in order to produce a written summary or recording of the proceeding.

(c) A written summary or recording of such appearance is made part of the individual's security file.

(d) The personal appearance does not require that statements be made under oath. The proceeding need not allow for the testimony or cross-examination of witnesses.

(8) Advises the individual that if no response is provided to the Notice of Determination within the specified time periods, the Notice of Determination becomes final without further notice.

B. In the case of an employee, the First-Level Deciding Authority notifies the individual's supervisor(s) of the denial or revocation and advises the supervisor of his or her responsibility for ensuring that the individual not have access to classified information during the denial or revocation process.

4. Notice of Review:

A. The Second-Level Deciding Authority reviews the record in the case including the Notice of Determination, any documentation on which the Notice of Determination is based, the written reply, the personal appearance (if any), and any documentation provided with the written reply or at the time of the personal appearance.

B. Upon completion of the review, the Second-Level Deciding Authority provides a written decision to the individual and/or his or her representative, in accordance with Executive Order 12968. The Notice of Review advises the individual of the decision to reverse or to uphold the Notice of Determination:

(1) If the decision is to reverse the Notice of Determination, the Notice of Review states, to the extent permitted by the national security and applicable law, the basis for the action.

(2) If the decision is to uphold the Notice of Determination, the Notice of Review informs the individual that he or she has 15 days from the date of the Notice of Review to file an appeal in writing with the Security Appeals Board. The Notice of Review, except in cases involving the USSS, also informs the individual to address the written appeal to:

Department of Homeland Security
Attn: Chief, Personnel Security Division
Anacostia Naval Annex
245 Murray Drive S.W., Building 410
Washington, DC 20528

The individual sends a copy to the Second-Level Deciding Authority.

(3) Extensions of time to appeal the Notice of Review are not granted by the Security Appeals Board absent compelling circumstances.

C. When a notice of appeal is submitted, the Second-Level Deciding Authority forwards materials pertinent to the underlying denial or revocation matter to the Security Appeals Board through the DHS Office of Security.

D. Security Appeals Board:

(1) Appeals are decided by the Security Appeals Board. Members of the Security Appeals Board selected to review a matter cannot have a current supervisory relationship with the employee or applicant.

(2) The individual may provide the Board with supplemental written documents, materials, and information. These documents, materials, and information must be provided within 30 calendar days of the date of the Notice of Review.

(3) The Chair of the Security Appeals Board may request through the DHS Office of Security additional documents, materials, and information from the Component where the case originated.

(4) The majority decision of the Security Appeals Board is controlling. The decision of the Security Appeals Board is final.

(5) The decision of the Security Appeals Board to either grant or deny access to classified information is made in writing, as required by Executive Order 12968. The decision by the Security Appeals Board is drafted by the DHS Office of Security. A copy of the decision is provided to the affected individual and/or their representative, along with a copy to the employing Component.

(6) All cases are considered by the Security Appeals Board on a case-by-case basis employing the Adjudicative Guidelines. Prior final decisions of the Security Appeals Board are persuasive, but are not controlling precedent.

5. Suspension of Access to Classified Information:

A. A suspension of access to classified information is an administrative action that does not require the same review procedures as those associated with a denial or revocation of access to classified information or those set out in Executive Order 12968, Section 5.2. The following procedures apply when an individual's access to classified information is suspended:

(1) Access to classified information may be suspended immediately by the First-Level Deciding Authority. Suspension of access to classified information is appropriate where there is reason to believe that the individual's continued access to classified information is not in the interests of national security.

(2) A written Notice of Access Suspension is issued to the individual including a brief statement of the reason(s) for the suspension action consistent with the interests of national security. If notification will likely compromise an ongoing investigation, the individual need not be notified at the time of the suspension, but must be notified as soon thereafter as practical.

(3) The First-Level Deciding Authority notifies the individual's supervisor(s) of the suspension and advises the supervisor of his or her responsibility for ensuring that the individual not have access to classified information during the time of the suspension.

(4) The Notice of Access Suspension states that the suspension remains in effect for either a specified period of time or until an event or set of events have occurred. Where access to classified information is suspended, attempts to resolve the matter as expeditiously as circumstances permit should be made.

B. Authority of the Secretary:

(1) Nothing in this Chapter prohibits the Secretary from personally exercising the appeal authority, in accordance with Executive Order 12968. In such case, the decision of the Secretary is final.

(2) When the Secretary or Deputy Secretary personally certifies that the procedures set forth in this chapter cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, in accordance with Executive Order 12968, the procedures set forth in this Chapter will not be made available. This certification is conclusive.

(3) In accordance with Executive Order 12968, this chapter is not deemed to limit or affect the responsibility and power of the Secretary to deny or terminate access to classified information in the interests of national security. The power and responsibility to deny or terminate access to classified information may be exercised only where the Secretary determines that the procedures in this chapter cannot be invoked in a manner that is consistent with national security. This determination is conclusive.

CHAPTER 7, GENERAL PERSONNEL SECURITY PROGRAM REQUIREMENTS

General Personnel Security Program Requirements:

A. Personnel Security Records. All DHS Personnel Security Offices store personnel security case files and background investigations in a combination-locked cabinet or safe or equally secure area. Any disclosures of information from background investigation files are made in accordance with appropriate laws, regulations, and the DHS Privacy Act system of records notice.

B. Record Retention. At a minimum, DHS Personnel Security Records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a and 22c, approved by the National Archives and Records Administration. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable, except in instances of ongoing litigation. Indexes to personnel security case files are destroyed with the related case.

C. Transfer of Personnel Security Files. Unclassified personnel security files are sent by First Class mail or by other means approved for the transmittal of this information. This applies to active or inactive files and the mailing of one or more investigative reports to the investigative service providers or DHS Components. Memoranda or other transmittal forms are used to ensure that records of the locations of personnel security files and reports are maintained.

D. Personally Identifying Information. Two primary laws (The Privacy Act of 1974, (5 USC 552a) and the E-Government Act of 2002) give federal agencies responsibilities for protecting and securing personal information. These laws regulate the collection, maintenance, use, and dissemination of personal information in government records when that information is retrieved by the name or other personal identifier of the subject of record. DHS handles personally identifiable information (PII) in accordance with the provisions of the Privacy Act of 1974 and E-Government Act of 2002. All DHS users of this information provide appropriate protection of information contained in, or extracted from, paper files or automated systems.

E. Procurement Actions. DHS Personnel Security Offices work with DHS procurement offices to ensure contractor employee requirements for fitness screening, as required by this Instruction, are included in solicitations and contracts, and that potential bidders, and contractors are aware of all fitness screening requirements at the earliest stages of the acquisition. Security considerations for procurement actions are completed in accordance with the Homeland Security Acquisition Manual, Part 3007, Appendix A – Acquisition

Planning Guide. This guide states that all DHS acquisitions or combination of acquisitions supporting a program that meet the threshold requirements in HSAM 3007.103(d)(2)(i) require a formal written approved Acquisition Plan (AP) before initiating any contractual action.

F. Use of Technology. Information technologies implemented to support personnel security processes utilize the proper technical safeguards, user training, assessments (e.g., privacy, certification and accreditation) to ensure adequate protection of personnel security related information.

G. HSPD-12. HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" requires agencies to develop and implement mandatory government-wide standards for secure and reliable forms of identification for covered individuals.

H. Freedom of Information Act (FOIA). An individual may request, under the provisions of the Privacy Act and/or FOIA, copies of their personnel security file. The individual may be provided excerpts, summaries, or an analytical extract of the information contained in the file. The individual may request the investigation report directly from the investigative agency (i.e., DHS or OPM). Requests for documentation contained in a personnel security file which was relied upon in a notice of charges or a notice of determination (and to the extent the documentation is being requested to prepare a response to a notice of charges or notice of determination) need not be submitted as a FOIA request. However, these documents are made available to the extent the documents would be available under the FOIA, including all applicable exemptions and redactions.

I. Customer Service. DHS Personnel Security Offices generate and deliver personnel security related information to potential applicants and the DHS community. Information is disseminated using newsletters, instructional brochures, web sites, and/or customer service telephone or service desks, etc. All customers are extended professional and courteous service.

.

INVESTIGATION MATRIX

Suitability

Risk Level	Security Forms Required	Type of Investigation Required	Preliminary Checks Required for Pre-Appointment Determination
High	-SF 85P -Fingerprint Card -Credit Release Form -SF 85P-S[2]	Background Investigation (BI)	• Favorable Review of Forms • Favorable Fingerprint & Credit • Scheduling of the BI • Component Specific Checks
Moderate		Minimum Background Investigation (MBI)	• Favorable Review of Forms • Favorable Fingerprint & Credit • Scheduling of the MBI • Component Specific Checks
Low	-SF 85 -Fingerprint Card	National Agency Check with Inquiry (NACI)[3]	• Favorable Review of Forms • Favorable Fingerprint & Credit • Scheduling of the NACI • Component Specific Checks

[2] Only Weapons-Carrying Contract Guards complete the SF 85P-S in addition to SF 85P.
[3] Requirement of HSPD-12.

Security Clearance

Security/Risk Level	Security Forms Required	Type of Investigation Required	Preliminary Checks Required for Interim Clearance
SCI/SAP – Special Sensitive	-SF 86 -Fingerprint Card -Credit Release Form	Single Scope Background Investigation (SSBI)	N/A
Top Secret – Critical Sensitive		Single Scope Background Investigation (SSBI)	
Secret – Non-Critical Sensitive		Minimum Background Investigation (MBI)	• Favorable Review of Forms • Favorable Fingerprint & Credit • Scheduling of the MBI • Component Specific Checks

Periodic Reinvestigations (PR)

Position/Risk Designation	Personnel Reinvestigation	Frequency of Reinvestigation
High	PRI	Every 5 years
Moderate	ANACI	Every 10 years
Low Risk	NACI	Every 10 years
Special Sensitive – Top Secret/SCI	SSBI-PR	Every 5 years
Critical Sensitive – Top Secret	SSBI-PR	Every 5 years
Non Critical Sensitive – Secret	ANACI	Every 10 years
Non-Sensitive	NACI	Every 10 years

DEFINITIONS

1. ***Access to Classified Information (Access)***: The ability and opportunity to obtain knowledge of classified information. Note: "Access" is implicitly authorized access. When conveying the notion that a person was able to obtain classified information improperly, qualifiers such as "unauthorized" or "improper" or "illicit" usually are used. [EO 12968 (definition only)].

2. ***Access National Agency Check and Inquiry (ANACI)***: Consists of a National Agency Check (NAC), employment checks, education checks, residence checks, reference checks, and law enforcement agency checks.

3. ***Security Access Adjudication (Adjudication)***: Final decision based on evaluation of data and evidence. Includes pertinent data contained in a background investigation, and/or any other available relevant reports, to determine whether an individual is eligible for access to classified information and for Federal employment.

4. ***Appeal***: A formal request, submitted by an applicant, employee, or contractor with SCI access for review of a decision.

5. ***Applicant***: A person, other than a DHS employee, who has received an authorized conditional offer of employment.

6. ***Background Investigation (BI)***: Consists of a National Agency Check (NAC), personal interviews with the individual and other sources, credit checks, law enforcement agency checks, residences checks, and employment checks.

7. ***Classified Information***: Information that has been determined to require protection against unauthorized disclosure, pursuant to Executive Order 12958, as amended, or a predecessor order. Such information is marked to indicate its classified status when in documentary form.

8. ***Component Security Office***: The security office of the following Components have the authority to make suitability and security clearance determinations:

   A. Citizenship and Immigration Services, United States (USCIS)

   B. Coast Guard, United States (USCG)

   C. Customs and Border Protection, United States (CBP)

   D. Federal Emergency Management Agency (FEMA)

   E. Federal Law Enforcement Training Center (FLETC)

F. Immigration and Customs Enforcement, United States (ICE)

G. Secret Service, United States (USSS)

H. Transportation Security Administration (TSA)

9. ***CONFIDENTIAL Information***: Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security of the United States.

10. ***Contract***: A contract is a mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them, as defined in the Federal Acquisition Regulations (FAR). It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. § 6301, *et seq*.

11. ***Contractor Employee***: An individual who performs work for or on behalf of any agency under a contract and who, in order to perform the work specified under the contract, requires access to space, information, information technology systems, staff, and /or other assets of the Federal Government. Such contracts, include, but are not limited to: (i) personal services contracts; (ii) contracts between any non-Federal entity and any agency; and (iii) sub-contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the agency.

12. ***Covered Individual***: 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: (1) the President or (except to the extent otherwise directed by the President) employees of the President under section 105 or 107 of title 3, United States Code; or (2) the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under section 106 of title 3 or annual legislative branch appropriations acts.

13. ***Personnel Security Deciding Authorities (Deciding Authorities)***: DHS review officials for personnel security determinations regarding suspension, revocation, denial, granting, or reinstatement of an individual's access eligibility.

A. ***First-Level Deciding Authority***: The person with responsibility for the implementation and management of the Personnel Security Program within the DHS Component Security Office. For the Office of the Secretary and those

Components without security offices, the First-Level Deciding Authority is the Chief of the Personnel Security Division, DHS Office of Security.

B. ***Second-Level Deciding Authority***: A supervisor of the First-Level Deciding Authority within the DHS Component Security Office. For the Office of the Secretary and those Components without security offices, the Second-Level Deciding Authority is the DHS Chief Security Officer or his or her designee.

C. ***Third-Level Deciding Authority***: The Security Appeals Board. For each denial or revocation matter, the Board is comprised of three high-level officials appointed by the Secretary or his or her designee. Two of these members on the Security Appeals Board are selected from outside the security field, in accordance with Executive Order 12968.

14. ***Denial of Security Clearance***: An adjudicative decision that a covered individual whose duties require access to national security information, or a contractor employee whose duties require access to SCI, is not eligible for access to classified information.

15. ***Derogatory Information***: Information which potentially justifies unfavorable suitability or security adjudication; such information may prompt a request for additional investigation or clarification for resolution of an issue.

16. ***DHS Facility***: DHS-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of the Department. It includes DHS-controlled commercial space shared with non-government tenants; DHS-owned contractor-operated facilities; and facilities under a management and operating contract such as for the operation, maintenance, or support of a Government-owned or-controlled research, development, special production, or testing establishment.

17. ***Employment Position Sensitivity Categories***: Defined by the Office of Personnel Management.

A. ***Non-Sensitive/Low Risk***: Positions that have the potential for limited impact on the integrity and efficiency of the Federal service. These positions involve duties and responsibilities of limited relation to an agency or program mission.

B. ***Moderate Risk***: Positions that have the potential for moderate to serious impact on the integrity and efficiency of the Federal service. These positions involve duties that considerably important to the agency or program mission with significant program responsibility or delivery of service.

C. ***High Risk***: Positions that have the potential for exceptionally serious impact on the integrity and efficiency of the Federal service. These positions involve duties that are especially critical to the agency or program mission with a broad scope of responsibility and authority.

D. ***Non-Critical Sensitive***: Positions that have the potential for serious damage to the national security. These positions involve either access to SECRET or CONFIDENTIAL national security information materials, or duties that may adversely affect, directly or indirectly, the national security operations of the Department.

E. ***Critical Sensitive***: Positions that have the potential for exceptionally grave damage to the national security. These positions may include access up to, and including, TOP SECRET national security information or materials; or other positions related to national security, regardless of duties, that require the same degree of trust.

F. ***Special Sensitive***: Any position designated at a level higher than Critical Sensitive by a document that complements E.O. 10450 and E.O. 12968 (such as Director of Central Intelligence Directive 6/4 that sets investigative requirements and access to Sensitive Compartmented Information and other intelligence-related Special Sensitive information).

18. ***Excepted Service***: As defined in Section 2103 of Title 5, United States Code, the "excepted service" consists of those civil positions which are not in the competitive service or the Senior Executive Service.

19. ***Federal Employee***: A person other than the President and Vice President, employed by, detailed to, or assigned to, a DHS Component or the Office of the Secretary, or another Federal agency, including members of the Armed Forces.

20. ***Fitness***: "Fitness" is the level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee.

21. ***Fitness Determination***: A decision by an agency that a person has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee.

22. ***Information Technology (IT)***: Equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by DHS. This definition applies if the equipment is used by DHS directly or is used by a

contractor under a contract with DHS that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. The definition includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. The definition does not include any equipment acquired by a federal contractor incidental to a federal contract.

23. ***INFOSEC:*** The ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or component in a classified automated information system.

24. ***IT Systems***: Information technology systems that are (1) owned, leased, or operated by a Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, State, or local government agency on behalf of DHS.

25. ***Lawful Permanent Resident***: A person who has immigrated legally but is not an American citizen; this person has been admitted to the U.S. as an immigrant and has a Permanent Resident Card, Form I-551 also known as a green card. Also known as "Permanent Resident Alien," "Resident Alien Permit Holder," or "Green Card Holder."

26. ***Limited Background Investigation (LBI)***: Consists of a National Agency Check (NAC), personal interview with the individual, education checks, credit checks, law enforcement agency checks, residence checks and employment checks consisting of personal interviews and/or records reviews.

27. ***Minimum Background Investigation (MBI)***: Consists of a National Agency Check (NAC), personal interview with the individual, reference checks, credit checks, law enforcement agency checks, residence checks, and employment checks. Other than the personal interview, there are no source interviews conducted during this investigation.

28. ***National Agency Check (NAC)***: Consists of records searches in the Office of Personnel Management (OPM) Security/Suitability Investigations Index; FBI Identification Division/Headquarters investigation files; FBI National Criminal History Fingerprint File; Defense Clearance and Investigations Index; and other sources, as necessary, to cover specific areas of a subject's background.

29. ***National Agency Check with Inquiries (NACI)***: Consists of a NAC, employment checks, education checks, law enforcement agency checks, and personal reference checks. Pursuant to the requirements of Homeland Security

Presidential Directive 12, a NACI is initiated and a favorable fingerprint check completed prior to the issuance of a DHS Personal Identity Verification (PIV) Card.

30. ***National Agency Check and Credit (NACC Check)***: Consists of a National Agency Check and credit checks.

31. ***National Crime Information Center (NCIC) Check***: Consists of a check of the computerized index of criminal justice information (e.g., criminal record history information, fugitives, stolen properties, missing persons).

32. ***National Security Positions***: Positions that involve activities of the U.S. Government concerned with the protection of the nation from foreign aggression or espionage, as defined under Executive Orders 10450 and 12968. These include positions involved with developing defense plans or policies; intelligence or counterintelligence activities; foreign relations, and related activities concerned with preserving the military strength of the United States; and positions that require regular use of, or access to, classified information.

33. ***Need-to-Know***: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

34. ***Private Sector***: Individuals and entities, including for-profit and non-profit, which are not part of any government. This includes individuals, sole proprietorships, partnerships, associations, and corporations, private voluntary organizations and non-public educational institutions, as well as all other nonprofit institutions.

35. ***Public Trust Positions***: Positions that may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; positions involving access to, or operation of, or control of financial records, with a significant risk for causing damage or realizing personal gain, as defined under 5 C.F.R. 731.

36. ***Revocation of Security Clearance***: An adjudicative determination that a person who had access to classified information is no longer eligible to have such access to classified information.

37. ***SECRET Information***: Information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security of the United States.

38. ***Sensitive Compartmented Information (SCI)***: Classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the Director of Central Intelligence.

39. ***Sensitive Information***: Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy. This definition includes one of the following categories of information:

A. Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 211- 224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual; or

B. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or

C. Sensitive but Unclassified Information (SBU) – For Official Use Only -, which consists of any other information which:

(1) If provided by the government to the contractor, is marked in such a way to place a reasonable person on notice of its sensitive nature;

(2) Is designated “sensitive” in accordance with subsequently adopted homeland security information handling requirements.

40. ***Single Scope Background Investigation (SSBI)***: Consists of a National Agency Check (NAC), a spouse or cohabitant NAC, a personal Subject Interview, and citizenship, education, employment, residence, law enforcement, and record searches covering the most recent 10 years of an individual’s life, or since his or her 18th birthday, whichever is shorter.

41. ***Suitability***: A determination based on an individual's character or conduct that may have an impact on the integrity or efficiency of the Federal service. During a suitability determination, the Department may consider identifiable character traits and past conduct which are sufficient to determine whether or not a given individual is likely to carry out the duties of a job with appropriate integrity. Suitability-screening standards and determinations are distinct from security clearance standards and determinations, which address whether an individual is eligible for access to classified information.

42. ***Suspension of Security Clearance***: A decision that a person who had access to classified information is temporarily ineligible to continue such access.

43. ***TOP SECRET Information***: Information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security of the United States.