DHS INSTRUCTION 121-01-007-01, REVISION 01, THE DEPARTMENT OF HOMELAND SECURITY PERSONNEL SECURITY, SUITABILITY AND FITNESS PROGRAM

APPROVAL DATE: 08/8/2016

DEPARTMENT OF HOMELAND SECURITY

OFFICE OF THE CHIEF SECURITY OFFICER

Rich McComb
Chief Security Officer

8 Aug 16
Date

June 14, 2017 UPDATE: This document was updated to move the Security Appeals Board to Headquarters on Pages 40-41.

14 June 17

Instruction# 121-01-007-01
Revision# 01

TABLE OF CONTENTS

DHS INSTRUCTION 121-01-007-01

CHAPTER 1, General

1. Purpose

This Instruction establishes procedures, program responsibilities, standards and reporting protocols for the Department of Homeland Security (DHS) personnel security and suitability program. This Instruction implements the authority of the Office of the Chief Security Officer (OCSO) under DHS Directive 121-01 and DHS Delegation 12000.

The OCSO is actively involved in the U.S. Government Executive Branch initiatives to revise and align the personnel security and suitability programs. This Instruction may be revised as necessary when new Executive Orders (E.O.), regulations and implementing guidance are issued.

2. Scope

This Instruction applies throughout DHS, to DHS covered individuals (i.e., DHS employees, Coast Guard Officers and members, applicants for DHS employment, state, local, tribal and private sector entities and officials, contractor employees, interns, consultants, volunteers and temporary employees) requesting or 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 or their data; access to sensitive information and/or access to national security information. This Instruction defines the standards for the DHS personnel security and suitability program.

3. Authorities and References

A. Executive Order (E.O.) 10450, as amended, "Security Requirements for Government Employment," April 27, 1953
B. E.O. 10577, as amended, "Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service," November 22, 1954
C. E.O. 10865, as amended, "Safeguarding Classified Information within Industry," February 20, 1960
D. E.O. 12333, as amended, "United States Intelligence Activities," December 4, 1981
E. E.O. 12829, as amended, "National Industrial Security Program", January 6, 1993
F. E.O. 12968, as amended, "Access to Classified Information," August 2, 1995
G. E.O. 13311, as amended, "Homeland Security Information Sharing," July 29, 2003
H. E.O. 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

I. E.O. 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009
J. E.O. 13526, "Classified National Security Information," December 29, 2009
K. E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," August 18, 2010
L. E.O. 13556, "Controlled Unclassified Information," November 4, 2010
M. E.O. 13587, "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
N. Presidential Policy Directive/PPD-19, "Protecting Whistleblowers with Access to Classified Information," October 10, 2012
O. Implementation of the Revised Federal Investigative Standards, Performance Accountability Council memorandum, April 30, 2014
P. Approval of the Revised Federal Investigative Standards memorandum, December 2012
Q. Security Executive Agent Directive 1, March 13, 2012
R. Title 5, Code of Federal Regulations (CFR), Part 5, "Regulations, Investigation and Enforcement (Rule V)"
S. Title 5, CFR, Part 5.2, "Investigations and Evaluations"
T. Title 5, CFR, Part 302, "Employment in the Excepted Service"
U. Title 5, CFR, Part 731, "Suitability"
V. Title 5, CFR, Part 732, "National Security Positions", as amended in subsequent iterations
W. Title 5, CFR, Part 736, "Personnel Investigations"
X. Title 5, CFR, Part 752, "Adverse Actions"
Y. Title 6, CFR, Section 7.10, "Authority of the Chief Security Officer, Office of Security"
Z. Title 8, CFR Part 274a, "Control of Employment of Aliens"
AA. Title 6 CFR 29, "Protected Critical Infrastructure Information"
BB. Title 9 CFR Part 1520, "Protection of Sensitive Security Information"
CC. Title 5, United States Code (U.S.C.), Section 552(a), "Records maintained on individuals" [The Privacy Act of 1974, as amended]
DD. Title 5, U.S.C., Section 7532, "Suspension and removal"
EE. Title 5, U.S.C. App., "Inspector General Act of 1978"
FF. Title 18, U.S.C., Section 922, "Unlawful Acts" (The Lautenberg Amendment)
GG. Title 50, U.S.C. 403-31h, "National Security Act of 1947"
HH. Title 50, U.S.C. 403q, "Central Intelligence Agency Act of 1949"
II. 6 U.S.C. section 211- 224, "Critical Infrastructure Information Act of 2002"
JJ. Public Law 110-181, Section 3002 (The Bond Amendment)
KK. Intelligence Community Directive Number 704 (ICD 704), "Personnel Security Standards and Procedures Governing Eligibility For Access To

Sensitive Compartmented Information And Other Controlled Access Program Information," October 1, 2008

LL. Intelligence Community Policy Guidance Number 704.3 (ICPG 704.3), "Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes," October 2, 2008

MM. "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," as amended

NN. General Records Schedule (GRS) 18, Security and Protective Services Records

OO. U.S. Office of Personnel Management (OPM)/Central-9, Personnel Investigations Records

PP. Department of Homeland Security/ALL--023, Personnel Security Management System of Records, February 23, 2010

QQ. Homeland Security Presidential Directive-12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004

RR. Federal Information Processing Standards Publication (FIPS) PUB 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013

SS. Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12 (OPM Memorandum, July 31, 2008

TT. Federal Acquisition Regulation (FAR), Part 4.4, "Safeguarding Classified Information within Industry"

UU. Department of Defense (DoD) 5220.22-M, "National Industry Security Program Manual" (NISPOM), as amended

VV. Office of Management and Budget (OMB) Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 12, 2005

WW. Homeland Security Acquisition Regulation (HSAR), Part 3004.470, Security requirements for access to unclassified facilities, Information Technology Resources and Sensitive Information

XX. Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive, February 2012

YY. DHS Designations Chart, September 26, 2012

ZZ. DHS Delegation 12000, Delegation for Security Operations within the Department of Homeland Security, June 5, 2012

AAA. DHS Policy Directive 121-04, Security Clearance Reciprocity, February 5, 2015

BBB. DHS Directive 121-01, Chief Security Officer, June 30, 2008

CCC. DHS Sensitive Systems Policy Directive 4300A, April 30, 2014

DDD. ISS-5200 "SCI Access and SCIF Accreditation Process," December 3, 2012

EEE. DHS Instruction 121-01-011, The Department of Homeland Security Administrative Security Program, April 25, 2011

FFF. Department of Homeland Security MD 4900, Individual Use and Operation

of DHS Information Systems/Computers
GGG. Department of Homeland Security DHS Directives System Directive 140-04, Special Access Program Management, August 12, 2009
HHH. Department of Homeland Security DHS Directives System MD 140-01, Information Technology Systems Security, July 31, 2007
III. Department of Homeland Security Management Directive System MD 11052, Internal Security Program, October 12, 2004
JJJ. Department of Homeland Security Management Directive System MD 3120.2, Employment of Non-Citizens, March 22, 2004
KKK. Department of Homeland Security Protected Critical Infrastructure Information Program Procedures Manual, April 2009
LLL. Homeland Security Acquisition Manual (HSAM), Part 3007.103(d)(2)(i) and Appendix H– Acquisition Planning Guide

4. Definitions

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

5. Responsibilities

A. **Office of the Chief Security Officer - DHS Chief Security Officer (CSO)** has been designated by the Secretary, DHS, as the Senior Agency Official pursuant to Section 5.4.(d) of E.O. 13526. The CSO has also been designated as the DHS Cognizant Security Authority (CSA) by the Secretary. In accordance with DHS Delegation 12000, the CSO has Department-wide responsibility for the supervision, oversight and direction of the Department's Security Programs for personnel, information technology and communications systems, facilities, property, equipment, information and other material resources. The CSO establishes unified policies and business practices across the Department to ensure the efficient and effective use of resources in performing the actions needed to achieve functional excellence in the Security Program. The DHS OCSO retains the position sensitivity designation authority for all Presidential appointees in the Department requiring confirmation by the Senate.

(1) The **Personnel Security Division (PSD)** is responsible for evaluating and reporting effectiveness of the DHS Personnel Security Program to OCSO and the security and suitability Executive Agents; chairing the DHS Personnel Security Subcommittee consisting of senior-level personnel security representatives from each DHS Component authorized in DHS Delegation 12000 to perform personnel security activities; representing DHS interests in government-wide personnel security and suitability working groups; establishing and maintaining a departmental database for the tracking of personnel security cases; conducting compliance reviews of DHS Component personnel security programs; determining covered individuals' suitability, fitness, eligibility to occupy a national security position or eligibility for access

to classified information; and notifying the appropriate program office of the suitability, fitness, or eligibility adjudicative decision.

(2) **Security Systems Division (SSD)** is responsible for program management, operations and maintenance of the Integrated Security Management System (ISMS), and integrating ISMS, the Identity Management System (IDMS) and Physical Access System (PACS). SSD supports the automated lifecycle of DHS personnel security and suitability cases to include the capture of information related to background checks, investigations, and final determinations. See Chapter 8 for more information.

(3) **State, Local, Tribal, and Private Sector (SLTPS)/Security Management Division (SMD)** is responsible for processing state, local, tribal and private sector (SLTPS) security clearances. See Chapter 7 for more information.

(4) **Special Access Program Central Office Division (SAPCO)** is designated by the CSO as the Cognizant Security Authority for DHS Special Access Programs (SAPs) and oversight authority for DHS' participation in non-DHS SAPs. Establishes, develops, coordinates and implements SAP policies and procedures for oversight, execution, management, administration, security and information assurance. SAPs are governed by DHS Directives System Directive 140-04, Special Access Program Management and DHS MD 140-01, Information Technology Systems Security.

(5) **Administrative Security Division (ASD)** is responsible for processing and providing recommendations to the CSO when information is subject to a classification challenge or mandatory review appeal; approving or disapproving of classification and declassification guides before signature by an original classification authority; providing oversight of non-criminal security inquiries and investigations involving the potential mishandling of classified information; providing policy and oversight for information designated/information considered to be sensitive but unclassified; providing security training policy and procedural guidance to all Components; directing and administering the Department's Security Compliance Review Program; and preparing and processing "Contract Security Classification Specification" (DD Form 254) for classified contracts.

(6) **Physical Security Division (PHYSD)** coordinates with the OCSO/PSD in the areas of issuance of employee and contractor employee access control passes and DHS identification media.

(7) **Identity Management Division (IMD)** ensures a unified identity authentication and authorization environment for the Department with authoritative sources to help provide accurate and timely identification of people, resources and associated attributes and privileges, by assuring the

security, resiliency and reliability of the Department's identity management and governance process.

B. **Operational Component Heads** are responsible for implementing and complying with the personnel security standards and requirements established by this Instruction. The DHS CSO provides prior written approval for any/all adjustments to the standards/requirements.

C. **Chief Human Capital Officer (CHCO)** is responsible for Department-wide human capital policy and program development. The Office of the Chief Human Capital Officer (OCHCO) also serves as the human capital line of business chief for DHS Components. In this role, the OCHCO works collaboratively with Component offices and leverages other standing organizations (e.g., Office of Personnel Management's CHCO Council and Sub Councils) to ensure the best approach for the Department's human capital initiatives. As a part of hiring responsibilities, OCHCO is responsible for overseeing and providing guidance to the Components regarding establishing position risk/sensitivity levels (except for Presidential appointees). For DHS HQ employees, OCHCO Human Resources Management Services creates and classifies position descriptions, including designating the position risk/sensitivity levels (except for Presidential appointees), and provides that information to OCSO/PSD.

D. **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.

E. **DHS and Component Freedom of Information Act Officers and Privacy Officers** are responsible for ensuring that documents requested by individuals are made available to them to the extent they would be available if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C. 552a), as applicable.

F. **DHS Office of the General Counsel and Component Legal Programs** are responsible for providing legal services related to this Instruction.

G. **DHS Office of the Inspector General (OIG)** is responsible for initiating, conducting, supervising and coordinating investigations, audits, inspections and other reviews relating to the programs and operations of the Department.

H. **Under Secretary for Intelligence and Analysis** is responsible for validating the "need to know" for state and local personnel requesting a security clearance and/or Sensitive Compartmented Information (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 (USCG).

I. **DHS Contracting Officer's Representatives (CORs)** are appointed by the Contracting Officer (CO) in writing to perform specific functions in managing a contract. The COR provides technical directions to the contractor employee within the confines of the agreement. The CO and the COR work together to ensure the contract requirements are clearly communicated to the contractor employee.

J. **Chief Intelligence Officer (CINT)** exercises final Departmental authority to approve new SCI access requests for "communities" of personnel not previously approved for such access in accordance with ISS-5200 "SCI Access and SCIF Accreditation Process."

6. Requirements

A. All covered individuals with unescorted access to DHS information or facilities are subject to an investigation and a favorable determination.

B. All DHS covered individuals are investigated commensurate with the position risk/sensitivity and are set in accordance within the U.S. Office of Personnel Management (OPM) position risk/sensitivity designation guidance. Certain investigations may be completed post-appointment/employment, subject to the requirements outlined in this Instruction.

C. Suitability/fitness is an assessment of an individual's character or conduct to decide whether the individual's employment or continued employment would or would not protect the integrity and promote the efficiency of the federal service.

D. DHS affords fair, impartial and equitable treatment to all applicants for federal employment and current federal employees through the consistent application of suitability standards, criteria and procedures as specified in applicable laws, regulations and Executive Orders. DHS reserves the right to restrict access to DHS facilities, sensitive information, or resources, for federal employees.

E. 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 Executive Orders. DHS reserves the right to restrict access to DHS facilities, sensitive information, or resources, for contractor employees. Any decision of DHS regarding a contractor employee's fitness is not considered an employment action.

F. Determinations concerning access to classified information, and the denial or revocation of access to classified information, are based on the "current applicable Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," (Adjudicative Guidelines), or successor guidelines, and E.O. 12968, "Access to Classified Information." 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.” A suspension of access to classified information is a temporary administrative action and does not require the review procedures set forth in E.O. 12968, Section 5.2.

G. Determinations concerning eligibility for access to SCI, and information protected within other Controlled Access programs, are based on the current applicable Intelligence Community Policy Guidance (ICPG). Denial or revocation of access to SCI, other Controlled Access Program Information and Appeal Processes is governed by ICPG 704.3.

H. DHS utilizes reciprocity, including those by other agencies, in accordance with federal regulations and Executive Orders, unless there is information indicating an employee may not satisfy the E.O. standards.

I. DHS utilizes reciprocal recognition of fitness determinations for contractor employees and excepted service employees in accordance with E.O. 13488.

J. DHS is committed to sharing information and may grant Secret level clearances to state, local, tribal and private sector personnel. On a case by case basis, Top Secret Clearances and/or SCI access may be granted consistent with E.O. 13549 and its implementing directive and ISS-5200 “SCI Access and SCIF Accreditation Process”.

K. DHS is a member of the National Industrial Security Program (NISP) and therefore reciprocally accepts security clearances granted to contractor employees by the Department of Defense (DoD). DHS does not have the authority to grant clearances to contractor employees and therefore has no role in the processing or granting of security clearances for contractor employees. DHS does have the authority to determine eligibility for access to SCI for contractor employees.

L. Personnel security offices coordinate investigations impacting an employee’s ability to maintain a security clearance, employee malfeasance or criminal activity with the appropriate DHS investigative element.

7. 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.

8. Questions

Address all questions or concerns regarding this Instruction to the OCSO/PSD.

CHAPTER 2, Personnel Security Program Standards

1. Scope

The standards delineated in this chapter cover general personnel security program requirements.

2. Adjudicator Standards and Investigative Requirements

A. Adjudicators are to meet Performance Accountability Council (PAC) approved training requirements as promulgated by the Security and Suitability Executive Agents.

B. In accordance with OPM's Suitability Processing Handbook, each suitability adjudicator is subject to a favorable determination based on the results of at least a high risk investigation.

C. National security adjudicators are to meet the personnel security investigative and adjudicative standards for assignment to a critical sensitive position.

3. Training and Certification Minimum Requirements for Background Investigators

A. Investigators conducting investigations for agencies under OPM delegation are required to meet the personnel security investigative and adjudicative standards for assignment to a critical sensitive position.

B. Investigators are required to meet PAC approved training requirements as promulgated by the Security and Suitability Executive Agents.

C. All investigative personnel new to the program are required to attend and successfully complete a DHS-approved or OPM-sponsored Background Investigator Training Program.

4. Personally Identifiable Information (PII)

A. Two primary laws [The Privacy Act of 1974, (5 USC § 552a) and the E-Government Act of 2002], as amended, set forth requirements for federal agencies regarding protecting and securing personal information.

B. 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.

C. All DHS users of PII are to provide appropriate protection of information

contained in, or extracted from, paper files or automated systems.

5. Personnel Security Record Requirements

A. ISMS is the primary electronic storage medium for personnel security records maintained by DHS. Refer to Chapter 8 for more information.

B. Original signatures are not required; electronic or facsimile copies are acceptable for personnel security release forms, such as the standard form (SF) releases, unless required by Executive Order or OPM guidance.

C. Hard copy personnel security case files and background investigations are stored in a secure area and stored in accordance with PII and classified document regulations. Any disclosures of information outside of DHS from background investigation files are made in accordance with appropriate laws, regulations, or the DHS Privacy Act System of Records Notice (SORN) and recorded on DHS Form 11000-8.

6. Record Retention

A. Pursuant to the current records schedule, DHS personnel security records are retained and destroyed in accordance with General Records Schedule (GRS) 18, item 22a and 22c, approved by the National Archives and Records Administration (NARA), the OPM Central-9 records as recorded in the Federal Register and the DHS ALL--023 System of Records. 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.

7. Transfer of Personnel Security Files

A. Unclassified personnel security files are sent electronically (preferred method) whenever possible through secure messaging. If this method is not available, then files may be sent by first class/certified 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.

8. Fingerprints

A. Fingerprints are required for all initial investigations and some reinvestigations. Fingerprints can be taken by DHS personnel or federal, state, or local law enforcement personnel, or other approved entities.

B. Electronic fingerprinting methods are preferred for automation and reporting purposes.

C. Fingerprint capture establishes a biometric chain of trust by using the prints as part of the background investigation for Personal Identity Verification (PIV) credentialing and system/facility access.

9. Freedom of Information Act (FOIA) and/or Privacy Act

A. An individual may request, under the provisions of the Privacy Act and/or FOIA, copies of their personnel security file. Such requests are handled by the appropriate FOIA or Privacy Act office as the subject matter experts.

10. Use of Technology

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

11. Homeland Security Presidential Directive-12 (HSPD-12)

A. The “HSPD 12 policy for the 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. In order to obtain a PIV card/credential, an individual is required to undergo the appropriate investigation and receive a favorable adjudication.

12. Residency Requirements

A. To ensure adequate investigative coverage, individuals applying for any DHS position are required to have resided within the United States for three or more years out of the last five years. This is assessed based on the signature date of the standard form questionnaire submitted for the position. If the individual does not meet the investigative coverage or one of the exemptions below, he/she is ineligible to work for or on behalf of DHS, unless otherwise noted herein.

(1) For investigative coverage, U.S. citizen sources are necessary to verify their reportable activities (e.g., places of residence, educational institutions attended, etc.) outside the U.S. 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 U.S.

(2) The following are exempt from the residency requirements and may be considered for Entry on Duty (EOD) prior to completion of the background

investigation, on a case-by-case basis:

a. Those who work or worked for the U.S. Government in foreign countries in federal civilian or military capacities;

b. Those who were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location(s);

c. Those who worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation;

d. Those who studied abroad at a U.S. affiliated college or university; or

e. Those who have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

13. Citizenship Requirements

A. 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. 5 CFR 7 and 5 CFR 338 Citizenship Requirements for Federal Requirements, Title 8 of the U.S.C. 1324, OPM Federal Investigative Notice (FIN) 03-01 and DHS MD 3120.2 were used to create and establish DHS policy regarding employment of non-citizens.

B. Components considering non-citizens for federal employment in the competitive service follow usual selection procedures and meet the requirements of the following: immigration laws, any applicable appropriations act ban on paying certain non-citizens and Executive Order restrictions on appointing non-citizens in the competitive service.

C. Components considering non-citizens for federal employment in the excepted service need to ensure compliance with immigration laws and any applicable appropriations act ban.

D. Components are responsible for applying any citizenship requirements that may appear in their individual authorization and appropriations laws.

E. Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted in accordance with the exceptions section below.

F. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for federal employment positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted in accordance with the exceptions section below.

14. Exceptions

A. For non-U.S. citizens that are eligible for access to DHS IT systems or positions that are involved in the development, operation, management or maintenance of DHS IT systems, Component heads, with the concurrence of both the DHS CSO and CIO, or their designees, may grant an exception of the U.S. Citizenship requirement. Components receiving personnel security services directly from the OCSO require approval of both the DHS CSO and the CIO or their designees to obtain an exception. The following steps are necessary for a review of an exception request for a non-U.S. citizen:

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

(2) The exception is in the interest of DHS; and

(3) Adherence to the procedures outlined in DHS 4300A Sensitive Systems Handbook and MD 11052, as amended, for exception to the requirement that persons accessing DHS systems be U.S. citizens.

B. In order for an exception to be granted for competitive service positions, all of the following are required:

(1) There are no U.S. citizens who are basically qualified and available to fill the specific competitive service position;

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

(3) All requirements of 8 CFR Part 274a, or successor, are met.

C. Requests for exceptions of any other requirement set forth herein, such as residency requirements, surge support and/or resource issues are to be submitted in writing directly to the DHS CSO.

D. Exception requests need to receive appropriate vetting as necessary and include a justification. Such requests are considered on a case-by-case basis.

15. Quality Assurance

A. OCSO/PSD and Operational Components that have delegated investigative authority are required to institute internal review procedures that constitute part of a quality assurance program, to ensure that DHS investigations meet federal investigative standards, including monitoring investigative staff for the purpose of ensuring professionalism and integrity of their investigative products.

B. Processes that should be tracked in a quality assurance program consist of all metrics in the investigations process which can be used to ensure quality, accurate and timely products in compliance with federal investigative standards. This includes tracking specific metrics and implementing specific quality review processes in anticipation of government-wide investigations performance standards as set by the Security and Suitability Executive Agents.

16. Counterintelligence (CI) Referrals

A. When CI concerns develop, the OCSO/PSD coordinates the information with the Office of Intelligence and Analysis (I&A) for action.

B. Operational Components that do not have their own counterintelligence program need to contact OCSO/PSD for a referral to I&A.

C. Security offices in Components that have counterintelligence programs, excluding USCG Counterintelligence Service with their authority under E.O. 12333, need to coordinate information in conjunction with I&A when it involves personnel security issues.

17. Polygraph Programs

A. Some Components utilize polygraph programs for the hiring process.

B. For those Components that fall under the OPM-delegated polygraph authority, OPM approves and annually renews the use of the polygraph for competitive service employment screening and personnel investigations under the authority of E.O.s 10450 and 10577. Renewal requires DHS to recertify that it meets and continues to meet OPM's standards.

C. For screening applicants in national security positions, the Security Executive Agent directives and standards are followed. The polygraph program complies with the criteria set by the National Center for Credibility Assessment (NCCA) whose primary responsibility is polygraph training, polygraph examiner certification, program quality assurance and polygraph research for the Executive Branch.

18. National Security Timelines

A. Refer to minimum requirements in Appendix C.

B. 90% of initial national security adjudications are required to be completed in accordance with Office of the Director of National Intelligence (ODNI) mandates and Intelligence Reform and Terrorism Prevention Act (IRTPA) standards.

C. Reinvestigations and Continuous Evaluation programs are set by guidance issued by ODNI as the Security Executive Agent.

CHAPTER 3, Federal Suitability, Excepted Service and Contractor Employee Fitness Requirements

1. Scope

This chapter defines the suitability requirements for competitive service federal applicants, appointees and excepted service positions where the incumbent can be non-competitively converted to the competitive service and career appointments into a position in the Senior Executive Service, as defined in 5 CFR Part 731.101(b). This chapter also defines the fitness requirements for excepted service federal applicants and appointees in positions that do not non-competitively convert to competitive service positions and contractor employees 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.

A. Pursuant to the authority delegated by the President of the United States under 5 U.S.C. Sections 1104 and 3301, E.O. 10577 and 5 CFR Part 731, individuals seeking appointment to the competitive service are required to undergo an investigation to establish their suitability for employment. Suitability adjudication, denial and due process procedures are conducted in accordance with 5 CFR Part 731. Under E.O. 10577, the President delegated to OPM authority to investigate the qualifications and suitability of applicants for the competitive service.

B. The suitability process allows for the determination of 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.

C. Security clearances (i.e., Confidential, Secret, and Top Secret) are granted to individuals with a specific requirement for access to classified material, and may require an additional investigation and an adjudicative determination (refer to Chapter 4).

2. Suitability and Fitness Risk Assessments

A. Federal applicants and appointees requiring access to DHS facilities, IT systems, or sensitive information undergo the requisite investigation for the risk level of their positions.

B. Excepted service federal applicants or appointees requiring access to DHS facilities, IT systems, or sensitive information receive an appropriate fitness screening, based on the risk level of their positions as determined by OCHCO and the appropriate security office within each DHS Operational Component with

sufficient authority and/or responsibility.

C. Contractor employees requiring access to DHS facilities, IT systems, or Sensitive Information receive an appropriate fitness screening, based on the risk level of their positions. The DHS program official and the security office within each DHS Operational Component with sufficient authority and/or responsibility, and knowledge of the acquisition, is responsible for determining the risk level for each contractor employee position. The DHS program official coordinates with the DHS contracting officer to ensure that solicitations and contracts include appropriate requirements for contractor employees.

3. Position Risk/Sensitivity Levels and Investigative Requirements

A. The position risk/sensitivity level is based on an overall assessment of the impact that an individual could cause to the efficiency or the integrity of DHS operations.

B. Position designation is required to determine the appropriate level of investigation; therefore, all positions within DHS are to be designated. OPM sets forth guidance on position risk/sensitivity levels and the OPM Position Designation System and Automated Tool (PDT) is provided to simplify and automate the process.

C. The following criteria are used to determine the risk levels for each position occupied:

(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 background investigation requirements and the security forms necessary for each position risk/sensitivity level.

E. Investigations should be initiated before appointment, but no later than 14 calendar days after placement in the position, as outlined in 5 CFR 736.201(c).

4. Suitability/Fitness Reciprocity

A. Reciprocity applies to the fullest extent possible; see definition of Reciprocity in Appendix D.

B. Investigations and adjudications conducted by other federal agencies should be used whenever practicable to reduce the number of investigation requests, associated costs and unnecessary delays. The following standards for use of these investigations apply:

(1) After validating need through the appropriate systems, an investigation conducted with a favorable adjudication within the past five years and no more than a two year break in service by or for another federal agency on a federal applicant/appointee/contractor employee that is of the same or higher risk and scope as the one required, is sufficient to meet the investigative requirements. If that investigation is unavailable or not made available within a reasonable amount of time, a new appropriate investigation is required to be initiated.

(2) New security forms may be obtained and pre-employment checks completed for:

a. Applicants for law enforcement positions;

b. Applicants for positions subject to a polygraph screening requirement; and/or

c. When new derogatory information has been developed.

5. Suitability Adjudicative Criteria

A. Suitability is a consideration for every position covered by 5 CFR § 731.101. Suitability determinations are made in accordance with 5 CFR § 731.202. When making a determination, the following may be considered as a basis for finding a competitive service 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 CFR § 5.4 (i.e., a refusal to provide testimony to the Merit Systems Protection Board, OPM, or the Office of Special Counsel);

(5) Alcohol abuse, without evidence of substantial rehabilitation, of 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; and/or

(8) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

B. Subject to the above requirements, DHS OCSO and Operational Components may implement procedures for making EOD determinations. A favorable EOD determination is a preliminary risk management decision that allows the federal applicant/appointee to commence work before the required background investigation is completed. The investigation should be initiated before appointment, but no later than 14 calendar days of placement in the position. The EOD determination does not take the place of the required adjudicative decision for the background investigation and it does not represent a final suitability determination. Special Sensitive positions do not qualify for EOD determinations.

6. Fitness Adjudicative Criteria

A. When making a fitness determination for positions in the excepted service that cannot non-competitively convert to the competitive service, the non-exclusive disqualifying factors listed in 5 CFR § 302.203 or the below factors listed under B can be used.

B. For contractor employee positions, the following factors may be considered, as a basis for finding an excepted service federal applicant, appointee or contractor employee unfit. The qualification standards established provide that certain reasons may disqualify an applicant for appointment. The following factors, among others, may be included as disqualifying reasons:

(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 CFR § 5.4 (i.e., a

refusal to provide testimony to the Merit Systems Protection Board or the Office of Special Counsel);

(5) Alcohol abuse, without evidence of substantial rehabilitation, of 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 (for Excepted Service employees); and

(9) Any other nondiscriminatory reason that an individual's employment (or work on a contract) would not protect the integrity or promote the efficiency of the service.

C. Subject to the above requirements, DHS Operational Component security offices may implement procedures for making EOD determinations. A favorable EOD determination is a preliminary risk management decision that allows the excepted service federal employee applicant or appointee or contractor employee to commence work before the required background investigation is completed. The investigation should be submitted within 14 calendar days of placement in the position. The EOD determination does not substitute for the required background investigation and it does not represent a final fitness determination.

7. Suitability and Fitness Considerations

A. In making a suitability or fitness determination, the adjudicator needs to consider any of the following additional considerations to the extent they deem these 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/or

(7) The absence or presence of rehabilitation or efforts toward rehabilitation.

8. Supplemental Information

A. When issues are developed during the course of an investigation the scope of the inquiry is expanded as necessary to obtain additional information as may be required to assist in the determination of whether the federal applicant/appointee is suitable for employment, or to determine whether the excepted service federal applicant/appointee or contractor employee is fit and granted unescorted access to DHS facilities and sensitive information.

B. When applicable, if further information from the individual is needed, correspondence may be sent that affords him/her the ability to refute, explain, clarify, or mitigate the developed information.

9. Suitability or Fitness Notifications

A. For a competitive service federal applicant or appointee, when a suitability determination is made (favorable or unfavorable), the servicing Human Capital Office is formally notified.

B. For an excepted service applicant/appointee, when a fitness determination is made (favorable or unfavorable), the servicing Human Capital Office is formally notified.

C. For contractor employees, when a fitness determination is made (fit or unfit), the DHS/Component Program Office and/or the Contracting Officer and Contracting Officer's Representative (COR) are informed simultaneously.

10. Suitability and Fitness Determinations

A. When an applicant is found unsuitable for federal employment or a federal appointee/applicant is found unsuitable for another position, DHS may deny the individual appointment to the position without taking any of the additional steps under 5 CFR 731.203(a). A non-selection, or cancellation of eligibility for a specific position based on an objection to an eligible or pass over of a preference eligible under 5 CFR 332.406, is not a suitability action even it is based on reasons set forth in 731.202.

B. An excepted service federal applicant or appointee may be denied employment when the fitness determination finds that the individual is not fit.

C. If a contractor employee is found unfit, a notification is made to the contractor employee that they are ineligible to render services or otherwise perform under the DHS contract. Unfavorable information is not disclosed to the contractor employee's company.

11. Suitability Actions

A. The following are suitability actions under 5 CFR 731.203, which may be appealed to the Merit Systems Protection Board (MSPB) that may also be considered: cancellation of eligibility, removal, cancellation of reinstatement eligibility, and debarment.

B. DHS may elect to take a suitability action for an applicant or an appointee under 5 CFR 731 subpart D. When a suitability action is proposed, the individual is sent a written letter and is afforded 30 days from the date of the Notice of Proposed Action (NOPA) to refute, explain, clarify, or mitigate the unfavorable information. The individual is allowed the opportunity to answer the charges in writing and may furnish documentation and/or affidavits in support of the response. The NOPA also advises the individual that they may request a copy of the material relied upon in the proposal action. All decisions are based on legitimate non-discriminatory reasons.

C. All suitability actions are reported to the servicing Human Capital Office and OPM.

12. Reporting Determinations

A. All suitability and fitness determinations are reported to OPM.

B. Fitness determinations made where no investigation is initiated are not required to be reported to OPM.

13. Procurement Actions

A. 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 contractor employees are aware of all fitness screening requirements at the earliest stages of the acquisition.

B. Security considerations for procurement actions are completed in accordance with the Homeland Security Acquisition Manual, Part 3007, Appendix H– Acquisition Planning Guide. This guide states that all DHS acquisitions or combination of acquisitions supporting a program that meet the threshold requirements in Homeland Security Acquisition Manual (HSAM) 3007.103(d)(2)(i)

require a formal written approved Acquisition Plan (AP) before initiating any contractual action.

14. Reinvestigations

A. See Appendix A for reinvestigation requirements.

CHAPTER 4, Requirements for National Security Positions, Eligibility and Access to Classified Information and/or Sensitive Compartmented Information (SCI)

1. Scope

This chapter defines national security eligibility requirements for national security positions, which includes sensitive positions with no access, eligibility for access, and SCI eligibility for all federal employees and applicants. This chapter also covers contractor employees who require eligibility for SCI.

A. If an individual is determined suitable for employment and the position is designated as a national security sensitive position, the national security guidelines are applied to determine if the individual meets the standards to encumber a national security position or for eligibility to access classified information.

B. Access to classified information is limited to those individuals 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; and (4) verifying an official "need to know."

2. Position Risk/Sensitivity Levels and Investigative Requirements

A. The position risk/sensitivity level is based on an overall assessment of impact that an individual could cause to national security.

B. Position designation is required to determine the appropriate level of investigation; therefore, all positions within DHS are to be designated. OPM sets forth guidance on position risk/sensitivity levels and the OPM Position Designation System and Automated Tool is provided to simplify and automate the process.

C. An investigation is considered in scope within 5 years and not to exceed 7 years upon full implementation of the federal investigative standards.

D. In accordance with 5 CFR Part 732 or superseding guidance, the following criteria are used to determine the risk/sensitivity levels for each position occupied:

(1) Non-Critical Sensitive (NCS): Positions that have the potential to cause damage to the national security, up to and including damage at the significant or serious level and may require eligibility for access to classified material at the Secret or Confidential level.

(2) Critical Sensitive (CS): Positions that have the potential to cause exceptionally grave damage to the national security. These positions may require eligibility for access up to Top Secret national security information or materials; or other positions related to national security, regardless of duties, that require the same degree of trust.

(3) Special Sensitive (SS): Any position designated at a level higher than Critical Sensitive. These positions have duties with the potential to cause inestimable damage to the national security. These positions may require eligibility for access up to, and including, Top Secret, SCI, or Special Access Program (SAP) levels.

E. Appendix A outlines the background investigation requirements and the security forms necessary for each position risk/sensitivity level.

F. Those occupying a national security position are required to complete the SF 86 "Questionnaire for National Security Positions." National security investigations are conducted in accordance with federal investigative standards.

G. For positions designated as national security positions, post-appointment/employment investigations may be conducted with a waiver provided that the following standards from 5 CFR 732 or superseding guidance are met:

(1) For positions designated non-critical sensitive (NCS), investigations can be completed post appointment contingent upon a favorable review of the Standard Form (SF) 86 and pre-employment checks and an expedited submission of the request for an investigation.

(2) For positions designated critical sensitive (CS), investigations are completed pre-appointment/employment, or post-appointment with an exception provided that the following standards from 5 CFR 732 or superseding guidance are met:

a. An exception of the pre-appointment investigative requirement contained in section 3(b) of E.O. 10450 for employment in a sensitive national security position may be made only for a limited period:

1. In case of emergency if the head of the department or agency concerned finds that such action is necessary in the national interest; and

2. When such finding is made a part of the records of the department or agency.

(3) For positions designated special sensitive (SS), the pre-appointment investigative requirement may not be waived.

(4) Investigations should be initiated before appointment, but no later than 14 calendar days after placement in the position, as outlined in 5 CFR 736.201(c).

3. Security Clearance Reciprocity

A. Reciprocity applies to the fullest extent possible, as outlined in DHS Policy Directive 121-04, Security Clearance Reciprocity; see definition of reciprocity in Appendix D.

B. DHS follows the standards in accordance with E.O. 12968, the Intelligence Reform and Terrorism Prevention Act of 2004 and Office of Management and Budget (OMB) Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," as amended.

C. Eligibility determinations conducted in accordance with E.O. 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 E.O. 12968 standards. Further investigation is only conducted to meet required reinvestigation or security clearance revalidation requirements, or if derogatory information exists.

D. In accordance with ICD 704, eligibility determinations for SCI are accepted by DHS without re-adjudication, unless there is substantial information indicating that an individual covered by this chapter may not satisfy the ICD 704 standards. Further investigation is only conducted to meet required reinvestigation or security clearance revalidation requirements, or if derogatory information exists.

4. Eligibility for Access to Classified Information and SCI Access

A. Eligibility for access to classified information is granted in accordance with E.O. 12968, as amended; access to SCI and other controlled access program information governed by ICD 704 and the underlying policy guidance. 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 favorably adjudicated under the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," as amended;

(4) Been favorably adjudicated under the ICD 704 criteria for individuals covered under this chapter who are eligible for SCI access or Special Access Programs;

(5) Signed a Classified Information Non-Disclosure Agreement (SF 312); and

(6) Signed a Sensitive Compartmented Information Nondisclosure Agreement, Form 4414, if applicable.

B. Been briefed regarding the responsibilities associated with access to classified information and/or indoctrinated into SCI programs by an authorized Security Manager and/or Special Security Officer (SSO).

C. The eligibility requirements apply to all individuals covered by this Instruction who are being considered for initial or continued eligibility for access to classified information and access to SCI and Controlled Access Program Information. In the event an individual fails to meet or ceases to maintain the eligibility requirements for a security clearance or SCI access, he/she is provided with the appropriate due process in accordance with this Instruction.

5. Exceptions to SCI Standards

A. ICD 704 eligibility for access determinations are accepted by DHS and are not to be re-adjudicated unless: new information has surfaced since the last investigation that indicates the subject may not satisfy the adjudicative requirements contained therein or the original adjudication was recorded with an exception since the last adjudication; or the original adjudication was recorded with an exception, i.e., a waiver, condition or deviation annotated to the case.

B. Exceptions, such as waivers, deviations and conditions may require a second review.

C. DHS may accept or reject access eligibility approvals carrying exceptions based on its own risk assessment in accordance with ICD 704.

D. For a full discussion on the ICD 704 exception process, refer to Appendix B.

6. National Security Adjudicative Guidelines

A. National security positions are adjudicated using the national security adjudicative guidelines.

B. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for national security positions is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) The nature, extent and seriousness of the conduct;

(2) The circumstances surrounding the conduct, to include knowledgeable participation;

(3) The frequency and recency of the conduct;

(4) The individual's age and maturity at the time of the conduct;

(5) The extent to which participation is voluntary;

(6) The presence or absence of rehabilitation and other permanent behavioral changes;

(7) The motivation for the conduct;

(8) The potential for blackmail, pressure, coercion, exploitation, or duress; and

(9) The likelihood of continuation or recurrence.

C. Each case is judged on its own merits and final determination remains the responsibility of DHS. Any doubt concerning personnel being considered for access to classified information is resolved in favor of national security.

D. The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security and is an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person:

(1) GUIDELINE A: Allegiance to the United States;

(2) GUIDELINE B: Foreign Influence;

(3) GUIDELINE C: Foreign Preference;

(4) GUIDELINE D: Sexual Behavior;

(5) GUIDELINE E: Personal Conduct;

(6) GUIDELINE F: Financial Considerations;

(7) GUIDELINE G: Alcohol Consumption;

(8) GUIDELINE H: Drug Involvement;

(9) GUIDELINE I: Psychological Conditions;

(10) GUIDELINE J: Criminal Conduct;

(11) GUIDELINE K: Handling Protected Information;

(12) GUIDELINE L: Outside Activities;

(13) GUIDELINE M: Use of Information Technology Systems

E. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, or adverse information.

F. When information of a security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) voluntarily reported the information;

(2) was truthful and complete in responding to questions;

(3) sought assistance and followed professional guidance, where appropriate;

(4) resolved or appears likely to favorably resolve the security concern;

(5) has demonstrated positive changes in behavior and employment; and/or

(6) should have his/her access temporarily suspended pending final adjudication of the information.

G. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of denial or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

7. Temporary Access

A. In accordance with Section 2.1(b)(3) of E.O. 12968, eligibility for access to classified information may be granted temporarily when there is a need, such as one-time participation in a classified project, provided the investigative requirements under E.O. 12968 have been satisfied.

B. In such cases, temporary access is limited to an expiration date or passing of an identified event, and access to classified information is limited to that needed for the particular project or assignment.

C. An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

a. Is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

b. Is not to exceed 180 days; and

c. Is limited to specific, identifiable information that is made the subject of a written access record.

D. Where the access granted under Subsection (a) of Section 2.3 of E.O. 12968 involves another agency's classified information, that agency needs to concur before access to its information is granted.

8. Interim Access

A. 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, required checks and fingerprint submission.

B. Per Section 3.3 of E.O. 12968, in exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

C. Except for military personnel in the U.S. Coast Guard, DHS does not grant or accept interim Top Secret clearances.

D. Requests for exceptions to the above requirements are submitted in writing to the DHS CSO. Exception requests should include a justification and are considered on a case-by-case basis.

9. Contractor Employee Clearance Requirements

A. The Department of Defense (DoD) grants all clearances for contractor employees. Requests for clearances are submitted to DoD through the designated Facility Security Officer (FSO) at the cleared contract company.

B. For contractor employees obtaining authorization to access classified information, the following criteria is used:

(1) The contractor employee has a need to perform on a DHS or Component contract which has requirements for classified access. An executed Contract Security Classification Specification form (DD Form 254) is required be on file for the contract.

(2) The firm or business under contract with DHS or Component that requires access to classified information is required to have a facility clearance granted by the DoD Defense Security Service (DSS) commensurate with the level of access required to perform on the contract. Facility clearances granted at an interim Top Secret level are eligible only for access to DHS classified information at the Secret level.

(3) Contract personnel are required to have a clearance granted by the DoD commensurate with the level of access required for performance under the contract. Clearances granted at an interim Top Secret level are eligible only for access to DHS classified information at the Secret level.

(4) The FSO needs to submit a visit authorization request for the contract employee in accordance with the National Industrial Security Program Operating Manual (NISPOM), Chapter 6. Per DHS Instruction 121-01-011,

The Department of Homeland Security Administrative Security Program, letters are only accepted in writing. The visit authorization letter may be submitted either by email, mail, facsimile, or teletype, in sufficient time to allow for approval or disapproval of the requested visit.

10. Denial, Suspension or Revocation of a Security Clearance

A. Follow the guidelines in Chapter 5 of this Instruction.

11. Reinvestigations

A. See Appendix A for reinvestigation requirements.

CHAPTER 5, Suspension, Denial and Revocation of Access/Eligibility for Classified Information

1. Scope

The procedures in this chapter apply to all DHS federal employees; applicants; and state and local government, tribal, or private sector individuals, unless otherwise noted. The procedures do not apply to contractor employees or to decisions to administratively withdraw access to DHS facilities, sensitive information and/or information technology systems.

2. Responsibilities of Officials in the Security Clearance/Eligibility Adjudication and Appeal Process

A. DHS officials for personnel security determinations regarding denial, revocation or reinstatement include:

(1) The Deciding Official has the responsibility for the implementation and management of the Personnel Security Program within the DHS Operational Component security office. For the Office of the Secretary and those Components without personnel security delegation, the Deciding Official is the Chief of the PSD, DHS OCSO. For the other Components, it is the Chief or Director of the Personnel Security Program. The Deciding Official determines whether to deny or revoke eligibility to access classified information. Where necessary or appropriate, adjudication may be completed by the DHS OCSO or another Operational Component security office. The Deciding Official makes appropriate notifications of the denial or revocation.

(2) The Reviewing Official is a supervisor of the Deciding Official within the DHS Component security office. For the Office of the Secretary and those Components without personnel security delegation, the Reviewing Official is the DHS Chief Security Officer or designee. The Reviewing Official determines whether to uphold the Deciding Official's decision to deny or revoke eligibility to access classified information. In cases where necessary or appropriate, the review may be completed by a Reviewing Official such as the DHS CSO or another Operational Component Chief Security Officer.

(3) The DHS Security Appeals Board (hereafter the Board) determines whether to uphold or reverse a decision to deny or revoke eligibility to access classified information. If the Reviewing Official upholds the decision of the Deciding Official, the Board may review that decision, upon request of the individual. For each denial or revocation appeal, the Board is comprised of three high-level officials (GS-15 or above) appointed by the Secretary that will serve on a rotational basis. Two of these members are selected from outside the security

field, in accordance with E.O. 12968. To avoid any appearance of impropriety, no member of the Board may review a security clearance determination when there would be a conflict of interest or regarding an individual who is above him/her in the supervisory chain of command; in such instances, either a new member without a conflict is appointed to the Board, which can be from any Component as deemed appropriate, or the matter is to be decided directly by the DHS Secretary as provided for in section 10 below. The Board members need to have been investigated and adjudicated at a level commensurate with the case(s) they review.

3. Procedural Requirements

A. The subsequent procedural requirements apply to DHS applicants and/or federal employees who have been denied access to classified information or have had their eligibility/access to classified information revoked.

B. Security offices may issue letters of intent/proposals to deny or revoke a security clearance prior to rendering a final determination.

4. Suspension

A. A suspension of access to classified information is a temporary 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 forth in E.O. 12968, Section 5.2.

B. 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 Deciding Official or designee when there is reason to believe that the individual's continued access to classified information is not clearly in the interests of national security.

(2) The Deciding Official may delegate authority to suspend access to an alternate security official.

(3) The employee’s direct supervisor is notified of the clearance suspension.

(4) Other offices are notified as appropriate.

(5) All security systems are updated as required.

C. A written Notice of Access Suspension is issued to the individual and includes a brief statement of the reason(s) for the suspension action consistent with the interests of national security. If notification is likely to compromise an ongoing

investigation, the individual specifics are not disclosed at the time of the suspension, but thereafter as soon as practicable.

D. The Deciding Official notifies the individual's supervisor(s) of the suspension and advises the supervisor of his or her responsibility for ensuring that the individual does not have access to classified information during the time of the suspension.

E. 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.

F. The security office allows an employee to respond to the information within 10 days after being notified of a suspension of access.

G. A suspension of a security clearance is not considered a final action or an adverse action.

5. Denial or Revocation of a Security Clearance/Eligibility

A. Determinations concerning access to classified information, and the denial or revocation of access/eligibility to classified information, are based on the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," as amended (hereafter Adjudicative Guidelines).

B. The DHS Office of the General Counsel and Component Legal Offices may provide legal review and ensure legal compliance when the security office acts to deny or revoke a security clearance/eligibility.

6. Notice of Determination

A. The Deciding Official provides a written Notice of Determination (NOD) to the individual that includes the following:

(1) Notifies that the individual's eligibility for access to classified information has been denied or revoked.

(2) A written explanation for the determination to the extent permitted by law, as required by E.O. 12968.

(3) The name and office address of the Reviewing Official 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. The individual is responsible for providing a signed written designation of a representative; this ensures

the individual's consent to such representation. DHS directs its written communications to the individual; the individual is then responsible for sharing this information with their identified representative.

(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 (if such investigation was relied upon by the agency in rendering its decision), as permitted by the applicable laws and regulations, including E.O. 12968. Advises the individual that if no response is provided to the Notice of Determination within the specified time periods, the Notice of Determination is both final and not subject to further challenge.

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

(7) 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 (FOIA), 5 USC § 552, or the Privacy Act of 1974, 5 USC § 552a. The individual may be required to submit a formal request to the agency's FOIA or Privacy Act office.

(8) Advises the individual that he/she may reply in writing and may request to make a personal appearance with the Reviewing Official.

(9) If the individual requests documents, records, or reports, their written reply is required to be submitted within 30 calendar days of the date of notification that all documents relied upon have been provided.

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

(11) Advises the individual that they may request to appear personally, via telephone, videoconference, or other media as available, before the Reviewing Official and to present relevant documents, materials and information at that time. A personal appearance needs to be requested 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. DHS or its Components are not required to reimburse an individual's travel expenses or any associated costs; such costs may be reimbursed in accordance applicable travel regulations at the sole discretion of the agency. Travel for an individual's representative cannot be reimbursed.

b. The individual and his or her representative, the Reviewing Official, legal counsel advising the Component and administrative support personnel requested by the Reviewing Official are permitted to attend the personal appearance.

c. A court reporter, transcriber, or note-taker is also present in order to produce a written summary or recording of the proceeding. A written summary or recording of such appearance is made part of the individual's security file, and if requested, a copy may be provided to the individual.

d. The purpose of a personal appearance is for the individual to present information and evidence regarding the security determination. It is non-adversarial and the individual does not have the right to call or cross-examine witnesses.

7. Notice of Review

A. The Reviewing Official reviews the record in the case, including the Notice of Determination, the documentation on which the Notice of Determination is based, the written reply, the record or transcript of the personal appearance, and documentation provided with the written reply or at the time of the personal appearance, if any.

B. The Reviewing Official may request additional information from the appellant individual during the appeals process. If the Reviewing Official relies on additional information to uphold the Notice of Determination, copies of the additional information first need to be provided to the individual to the extent it would be available if requested under the FOIA, 5 USC § 552, or the Privacy Act of 1974, 5 USC § 552a. The individual is given an opportunity to file a written response or personal appearance to address the additional information before the Reviewing Official renders a decision on the Notice of Determination.

C. Upon completion of the review, the Reviewing Official provides a written decision to the individual, in accordance with E.O. 12968. The Notice of Review advises the individual whether the Notice of Determination is reversed or upheld.

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

E. If the decision is to uphold the Notice of Determination, the Notice of Review informs the individual that he or she has 15 calendar days from the date of the Notice of Review to file an appeal in writing with the Board, and a total of 30 calendar days from the date of the Notice of Review to provide the Board with

supplemental documents.

F. The Notice of Review informs the individual to send the written appeal to the address below, with a copy to the Reviewing Official:

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

G. In accordance with Section B of Presidential Policy Directive (PPD-19), "Protecting Whistleblowers with Access to Classified Information," a Notice of Review regarding eligibility for access to classified information only, is issued to a DHS federal employee informs the employee of his/her right to request the DHS Office of the Inspector General (OIG) review a claim that the action affecting the employee's eligibility for access to classified information was taken in reprisal for making a protected disclosure as defined in PPD-19. The Notice of Review further informs the employee that, should he/she choose to request a review by the OIG, the employee makes such request within 30 days receipt of the Notice of Review and the OIG is to further promptly notify the OCSO of such review. The notification is to include the OIG hotline telephone number, e-mail address and website.

a. If an employee requests review of a reprisal claim by the OIG, the timelines for appealing the Notice of Review to the DHS Security Appeals Board are tolled until the OIG issues its findings.

b. OIG is to provide proper notification to the OCSO that it has initiated an internal review. Upon completion of the OIG review, OIG is to notify the OCSO of its finding.

i. If the OIG issues a finding of no reprisal, the employee has 15 calendar days from the date of the OIG finding to file an appeal in writing with the Board, and a total of 30 calendar days from the date of the Notice of Review to provide the Board with supplemental documents.

ii. If the OIG issues a finding of reprisal, the Reviewing Official considers the findings and recommendations, consistent with the requirements of PPD-19.

H. The Board does not grant extensions of time to appeal the Notice of Review absent compelling circumstances.

I. When a notice of appeal is submitted, the DHS OCSO forwards the materials pertinent to the underlying denial or revocation matter to the Board.

8. DHS Security Appeals Board Process

A. The Security Appeals Board (SAB) decides appeals of adverse determinations under Executive Order 12968.

B. All appointments to the SAB are approved by the Secretary.

C. The Department's CSO selects an SAB Administrator. The SAB Administrator executes the administrative functions of the SAB. The SAB Administrator does not vote during SAB deliberations.

D. The DHS Office of the General Counsel (OGC), and Component legal programs at the request of the OGC, designate legal counsel for the SAB to advise the SAB of legal and procedural matters. Counsel for the SAB does not vote during SAB deliberations.

E. The SAB is comprised of the Chair and two Members, each of whom carries an equal vote (collectively, "the Members of the SAB"). The CSO chairs the SAB. The CSO selects two additional Members from a pool of DHS Senior Executive Service (SES) from inside DHS Headquarters or from Component SES nominated by voting members of the CSO Council, with approval of the Secretary. These Members are from outside the security field. In addition to being in the SES, these Members have supervisory experience and hold a security clearance commensurate with the appellant. When constituted, the Members serve for the first calendar year term with the possibility of selection by the CSO for a second calendar year term. Thereafter, Members are selected by the CSO with the Secretary's approval to serve on a calendar-year basis. The Chair has the authority to appoint eligible replacements for the Chair or for Members who cannot complete their terms, with the approval of the Secretary. Substitutes previously approved by the Secretary serve the balance of the term they are replacing and may be considered for subsequent calendar service without regard to their substitute service.

F. The SAB and its membership retain authority to resolve appeals heard during its term beyond its term.

G. Neither the Chair nor a Member may review an appeal having had prior involvement in the appeal or where they are or were in a supervisory, personal, or other relationship with the appellant which creates an actual or potential conflict of interest. When a particular appeal creates a conflict for the Chair, the SAB Administrator randomly selects a substitute Chair from eligible members of the CSO Council previously approved by the Secretary to chair that appeal. When a particular appeal creates a conflict for a Member, the SAB Administrator randomly selects a substitute Member from eligible members of the CSO Council or a pool of eligible participants previously approved by the Secretary to hear that appeal.

H. The appellant may provide the SAB with supplemental written documents, materials, and information. These documents, materials, and information are provided to the SAB within 30 calendar days of the date of the Notice of Review.

I. The Chair may request additional documents, materials, and information from the Component where the appeal originated. If relied upon in upholding the Notice of Determination, this information is provided to the appellant to the extent it would be available if requested under the Freedom of Information or Privacy Acts (See 5 U.S.C. §§ 552, 552a) and the appellant will be afforded a reasonable opportunity to file a written response to address the additional information by a date certain before the SAB votes on the appeal.

J. The SAB considers all appeals on a case-by-case basis, employing the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or ICD 704 as appropriate. The SAB considers the record of the appeal and any new information properly provided and determines whether to uphold or reverse the Reviewing Official's decision.

K. The decision of the SAB is made and provided to the appellant and/or his or her representative, with a copy to the security office of the employing Component.

L. The decision of the SAB is both final and not subject to further challenge. However, in accordance with Section C of PPD-19, "Protecting Whistleblowers with Access to Classified Information," any SAB decision issued to a DHS federal employee asserting a claim of reprisal informs the employee of his/her right to request an external review by a three-member Inspector General panel, chaired by the Inspector General of the Intelligence Community, of any claims that the action affecting the employee's eligibility for access to classified information was taken in reprisal for making a protected disclosure as defined in PPD-19.

1. <u>Reconsideration - Eligibility after a Denial or Revocation</u>

A. Following an unfavorable security determination, a request to reconsider eligibility can be submitted a minimum of one year from the date of the final determination by the appropriate security authority or the decision of the Board, if appeal rights were exercised, provided the Program/Directorate has a current requirement for the individual to have access to classified information or assignment to sensitive duties has been established. A request to reconsider or reinstate a previously denied or revoked security clearance is to be processed in the same manner as a new request for an adjudication, to include any applicable due process rights in the event of an unfavorable decision.

B. Pending reconsideration, temporary/interim access and/or temporary assignment to Sensitive positions is not authorized for individuals who have received an unfavorable eligibility determination.

10. Authority of the Secretary

A. When the Secretary or Deputy Secretary personally certifies that the procedure 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 E.O. 12968, the procedure set forth in this chapter is not to be made available. This certification is conclusive.

B. In accordance with E.O. 12968 (Part 5.2; Section E), this chapter is not deemed to limit or affect the responsibility of the Secretary, pursuant to any law or other Executive Order 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 pursuant to any law or other Executive Order may be exercised only where the Secretary determines that the procedures prescribed in this chapter cannot be invoked in a manner that is consistent with national security. This determination is conclusive.

C. In accordance with E.O. 12968 (Part 5.2; Section D), this chapter is not deemed to limit or affect the responsibility and power of the Secretary or Deputy Secretary to personally certify that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure is not to be made available. This certification is conclusive.

CHAPTER 6, Denial and Revocation of SCI Eligibility and Other Controlled Access Program Information

1. Scope

The procedures in this chapter apply to all DHS federal employees, state and local and tribal government or private sector individuals and contractor employees with SCI eligibility or other controlled access program information. It does not apply to decisions to administratively withdraw access or to suspend access to DHS facilities, sensitive information and/or information technology systems, nor to security clearances.

2. Denial or Revocation of SCI Eligibility

A. Determinations regarding eligibility for initial or continued access to SCI level information are made in accordance with ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information.

B. Individuals who have been considered for and denied initial or continued access for SCI and other controlled access programs pursuant to the provisions of ICD 704, to the extent provided herein, are to be afforded an opportunity to appeal the denial or revocation of such access.

3. Responsibilities of Officials in the Denial and Revocation of SCI Eligibility

A. The DHS officials responsible for personnel security determinations regarding denial, revocation, or reinstatement of SCI access eligibility include:

(1) The Deciding Official has responsibility for the implementation and management of the Personnel Security Program within the DHS Operational Component security office. For the Office of the Secretary and those Components without personnel security delegation, the Deciding Official is the Chief, PSD, DHS OCSO. The Deciding Official determines whether to deny or revoke eligibility for SCI access.

(2) The Reviewing Official is a supervisor of the Deciding Official within the DHS Component security office. For the Office of the Secretary and those Components without personnel security delegation, the Reviewing Official is the DHS Chief Security Officer or his or her designee. The Reviewing Official determines whether to uphold the decision to deny or revoke eligibility for SCI access. In cases where necessary or appropriate, the review may be completed by a Reviewing Official such as the DHS CSO or another Operational Component Chief Security Officer.

(3) A Third-Level Appeal Authority is the Cognizant Security Authority (CSA) or designee, who may make a final determination or appoint a high-level panel which is comprised of at least three members, two of whom are selected from outside the security arena. Recommendations of the panel need to be complete and in writing. They reserve the right per all IC regulations from personally exercising the appeal authority based upon recommendations from an appeal panel; in such a case the decision previously made is final.

4. Notice of Determination

A. The Deciding Official provides:

(1) A comprehensive written explanation of the basis for the denial or revocation as the national interests of the United States and other applicable laws permit.

(2) States the name and office address of the Reviewing Official to whom the individual should direct any reply, request, or filing.

(3) Informs the individual of his or her right to be represented by counsel or other representative at his/her own expense. The individual is responsible for providing a signed written designation of a representative. Even when a representative is appointed, DHS directs its written communications to the individual; the individual is then responsible for sharing this information with his/her representative.

(4) 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 national security and applicable laws.

a. If requested, the documents, records and reports are made available to the extent they would be available if requested under the FOIA, 5 USC § 552, or the Privacy Act of 1974, 5 USC § 552a.

(5) An opportunity to appear personally before an adjudicative or other authority, other that the investigative entity, as determined by the CSA or designee, is given to present relevant documents, materials and information. A written summary or recording of such an appearance is made a permanent part of the subject's security record. The decision of any appeal panel is made a permanent part of the subject's security record.

(6) The purpose of a personal appearance is for the individual to present information and evidence regarding the security determination. It is non-adversarial and the individual does not have the right to call or cross-examine witnesses.

(7) 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 is required to be submitted within 45 calendar days of the date of the final notification that all documents relied upon have been provided; the individual may be required to submit a formal request under the Freedom of Information Act or the Privacy Act. The DHS or Component Freedom of Information Act Officer and Privacy Act Officer work collaboratively to ensure that all documents that are to be provided to the individual are provided to the extent they would be available if requested under the FOIA, 5 USC § 552, or the Privacy Act of 1974, 5 USC § 552a. Accordingly, appropriate redactions that cite to these statutes are noted on the materials provided to the individual.

b. These documents, records and reports need to be requested no later than 15 calendar days following the receipt of the Notice of Determination.

c. If the individual does not request documents, records, or reports, the written reply is required to be submitted within 45 calendar days of the date of the Notice of Determination.

(8) Advises the individual that if no response is provided to the Notice of Determination as required, the Notice of Determination becomes final without further notice.

B. The Reviewing Official provides:

(1) Written notice of and reasons for results of the review/appeal, and the identity of the deciding authority in accordance with operational requirements.

(2) An opportunity to appeal to the Cognizant Security Authority (CSA) or designee, who may make a final determination, or who may appoint a high-level panel which is comprised of at least three members, two of whom are selected from outside the security arena. Recommendations of the panel need to be complete and in writing. The CSA reserves the right per all Intelligence Community (IC) regulations from personally exercising the appeal authority based upon recommendations from an appeal panel.

(3) DHS or its Components are not required to reimburse an individual's travel expenses or any associated costs; such costs may be reimbursed in accordance applicable travel regulations at the sole discretion of the agency.

(4) The individual and his or her representative, the Reviewing Official, counsel advising the Component and administrative support personnel requested by

the Reviewing Official 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.

(5) Written notice and reasons for results of the review/appeal is provided to the individual and agency in accordance with operational requirements. Results are conclusive.

5. Authority of the Cognizant Security Authority (CSA)

A. When the CSA personally certifies that a procedure set forth herein cannot be made available without damaging national security interests, the particular procedure is not made available. This certification is conclusive. Should it be determined that the appeal procedures prescribed in this directive cannot be invoked in a manner consistent with national security, the individual may be denied an appeal per ICD 704.

6. Authority of the Director of National Intelligence (DNI) or Principal Deputy DNI

A. Nothing in this Instruction or ICD 704 prohibits the DNI, in consultation with the relevant agency head, to take a lawful action(s) regarding an individual's access to SCI or other controlled access program information without regard to the provisions of this or other regulations or directives.

CHAPTER 7, State, Local, Tribal and Private Sector (SLTPS) Program Requirements

1. Scope

National security clearances for state, local, tribal and private sector (SLTPS) personnel are issued in accordance with E.O. 13549 and the guidance in "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive."

2. SLTPS Access to Classified National Security Information

A. The following pertain to eligibility to access classified national security information by state, local, tribal and private sector entities:

(1) SLTPS personnel who are processed for a security clearance undergo the same investigative and adjudicative criteria as their federal counterparts. No additional administrative or investigatory requirement is levied upon an SLTPS individual that is not applicable to other personnel to whom an equivalent level of access and security clearance is granted.

(2) Eligibility determination and subsequent clearance to access classified information is dependent upon the execution of a SF 312, "Classified Information Non-disclosure Agreement," or other approved non-disclosure agreement prescribed by the Information Security Oversight Office (ISOO) or the ODNI.

(3) SLTPS personnel who are granted a security clearance are required to comply with all reporting requirements and associated responsibilities that accompany the granting of access to classified information as required by statute, order, or regulation, and the Department of Homeland Security.

(4) Clearances may be issued to SLTPS personnel when the write-for-release principle that allows for the sanitization of classified information to the sensitive but unclassified level is inadequate to satisfy the effective integration of SLTPS personnel into a singular effort to protect the homeland. Those personnel selected for the granting of a security clearance need to have a demonstrated and foreseeable need for access to classified information. In determining the need for the granting of a security clearance the following criteria are applicable:

a. The granting of security clearances are required to be kept to the minimum necessary in support of mission activities where access to classified information by SLTPS personnel is essential to the national

security.

b. DHS recognizes that pursuant to E.O. 13526, under exigent circumstances classified information may be released by designated federal officials to personnel who are not otherwise cleared for access. Therefore, the granting of a security clearance strictly in support of potential contingencies is not necessarily justified or warranted.

(5) Security clearances are not to exceed the Secret level except in those situations where there is a demonstrated and foreseeable need and the person being considered for a higher level security clearance is to perform a function as cited below.

a. Top Secret security clearances may be granted on a case by case basis, when the person to whom the clearance is to be granted is officially designated and appointed as the state Homeland Security Advisor (HSA), or, the person will be an active and continuing participant in or member of a federally-sponsored board, committee, working group, task force, operations center, or other entity where the integration of SLTPS personnel is essential and participation or membership requires or will require access to Top Secret information, or, the sponsoring agency determines that a person has a particular expertise or role whereby there is a demonstrated and foreseeable need for access to Top Secret information.

b. Access to SCI may be granted on a case by case basis, when the person to whom the access is to be granted is or will be an active and continuing participant in or member of a federally-sponsored board, committee, working group, task force, operations center, or other entity where the integration of SLTPS personnel is essential and participation or membership requires or will require access to SCI, or, the sponsoring agency determines that a person has a particular expertise or role whereby there is a demonstrated and foreseeable need for access to SCI. In determining the appropriateness of granting SCI access, significant consideration is given to the value such access will bring to the effort for which the individual will participate, the contributions that can be made by the individual in support of the effort, and the fact that the use of the information to which access is granted is strictly limited to within the federally-sponsored effort. Access to SCI is only provided in an appropriately accredited SCI Facility (SCIF) under the direct control of DHS or another federal agency. Under no circumstances can SCI material be released to the physical custody of SLTPS personnel outside of an approved SCIF.

c. Prior to submitting a request for a Top Secret clearance and/or SCI eligibility, consideration is given to the length of time it takes between

the time a background investigation is requested and the time a security clearance can be issued to ensure the individual subjected to the investigation is still available for the assignment and valuable investigative and financial resources are not wasted. As such, prior to processing for a security clearance, agencies should ensure that the individual is committed to continued active participation in the specific activity for a period of no less than one year after being granted the security clearance.

d. SLTPS personnel who do not have a current, within scope Single Scope Background Investigation (SSBI) or equivalent investigation, Top Secret security clearance and/or SCI eligibility, granted by either DHS or another authorized federal agency, are subject to a reinvestigation.

(6) Absent disqualifying conduct as determined by the clearance granting official and upon the execution of a non-disclosure agreement prescribed, a duly elected or appointed governor, or the single most senior government official of a state, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or an official who has succeeded to that office under applicable law, may be granted access to classified information in support of a counter-terrorism or homeland security mission without a background investigation. This authorization of access may not be further delegated to any other person and is applicable to no other SLTPS personnel.

a. Access to classified information is not a right and is not absolute but is based on a need for access to such information in order to act on or otherwise fulfill an authorized governmental function associated with national security. An agency may exclude an individual from access to certain classified information to which they may otherwise be eligible when the information would provide insight into an investigation or other activity that may have a direct or indirect connection to the governor, or the single most senior government official, or the functions performed by that office.

(7) Security clearances for SLTPS personnel are limited to U.S. citizens only.

(8) Homeland Security Advisors (HSA) are authorized to receive Top Secret clearances if they otherwise satisfy the requirements for being granted a security clearance.

(9) 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, except for cases requiring SCI.

(10) DHS does not grant or accept interim Top Secret clearances for SLTPS personnel.

3. SLTPS Positions Eligible for a Security Clearance

A. State, local and tribal (SLT) personnel who may be considered for a security clearance include the following:

(1) Senior homeland security personnel, such as homeland security and emergency management coordinators, senior law enforcement personnel, senior public health officials and other senior personnel who are responsible to advise the governor on homeland security issues.

(2) For city, municipal and county governments and other political subdivisions of a state or territory of the United States, including the mayor of the District of Columbia: a mayor, county executive, city manager, senior law enforcement officer, senior firefighter, senior public health official, emergency manager or other senior government official employed by a city, municipality or county or other political subdivision of a state or territory of the United States involved in furthering United States homeland security.

(3) Other law enforcement, public health and first responder officials participating in a federally-sponsored or endorsed board, committee, working group, task force, operations center, Fusion Center, or similar entity where access to classified information is required, as determined by the sponsoring federal agency, may be considered for a security clearance.

B. Private sector (PS) personnel who do not fall under the purview of E.O.12829, "National Industrial Security Program," are processed for access eligibility in the same manner as SLT personnel. The granting of a security clearance to PS personnel is limited to the minimum number necessary to support the protection of critical infrastructure and security of the homeland.

(1) Eligibility for a security clearance for PS personnel under the SLTPS Program does not apply to any corporation, company, contractor employee, licensee, grantee, individual or other commercial entity, or their subcontractors, that has entered into or seeks to enter into a contractual arrangement or consulting agreement with an agency of the federal government pursuant to E.O. 12829, as amended; or, any corporation, company, contractor employee, licensee, grantee, individual or other commercial entity, or their subcontractors, that is eligible for the granting of a facility security clearance under the authority of E.O. 12829, as amended, except when uncleared PS personnel are not associated with such arrangement or agreement and therefore not eligible for a security clearance under E.O. 12829, as amended.

(2) National security clearances may be issued to those personnel who have a demonstrated and foreseeable need for access to classified information and are in leadership, managerial or executive level positions. Examples of such personnel include: leadership personnel (e.g., Sector Coordinating Council, Information Sharing and Analysis Centers as identified by their Sector Coordinating Council as the Sector's Information Sharing mechanism), who have the authority and stature to influence critical infrastructure and key resources (CIKR) owners/operators and others throughout the sector to take action; CIKR owners and operators (e.g., senior company executives including corporate security officers) of critical systems/assets/ functions/ networks that have been identified by DHS as critical infrastructure, including Level 1 and Level 2 facilities; subject matter experts who have been identified and selected to assist federal and state CIKR agencies to interpret operational information and translate intelligence information into actionable information for CIKR owners and operators and government officials; and PS personnel who are nominated to serve on boards, commissions, committees or other federally-sponsored groups where access to classified information is required in order to participate in and carry out the functions of the group.

a. PS personnel to whom a security clearance is issued under the SLTPS Program are required to have an executed "Statement of Understanding Relative to the Protection of Classified National Security Information." The purpose of the form is to inform and impress upon the signatory that the protection of classified information takes precedence over corporate loyalty and influence. As such they are legally obligated to abide by federal standards for the safeguarding of and access to classified information and are required to resist and report any undue influence on the part of cleared personnel, regardless of their position, to gain knowledge of classified information to which the signatory has been given access.

b. DHS SLTPS/Security Management Division (SMD), or the sponsoring federal agency, maintains the original executed form in the PS individual's personnel security folder and/or the electronic equivalent.

4. Extended Absences

A. Follow the guidelines in the Instruction 121-01-011, The Department of Homeland Security Administrative Security Program.

5. Denial, Suspension or Revocation of a Security Clearance

A. Follow the guidelines in Chapter 5 of this Instruction.

6. Reinvestigations
   A. See Appendix A for reinvestigation requirements.

CHAPTER 8, Integrated Security Management System (ISMS) – Safeguarding Personnel Security Records

1. Scope

This chapter describes the Integrated Security Management System (ISMS), a web-based personnel security case management tool designed to support the lifecycle of DHS personnel security and suitability cases to include the capture of information related to background checks, investigations and final determinations.

2. ISMS System Description

A. ISMS provides a common repository for personnel security records across DHS Components facilitating the aggregate reporting that DHS provides to the Office of Management and Budget (OMB), Office of the Director of National Intelligence (ODNI) and the U.S. Government Accountability Office (GAO). As a consolidated system, ISMS reduces the number of discrete interfaces that are established and maintained with external systems, as well as consolidates hardware/software infrastructure, disaster recovery configurations and support services across the enterprise. ISMS also provides the ability to shift personnel security resources from one DHS Operational Component to another for surge support without incurring extensive retraining.

B. ISMS supports the lifecycle of DHS's personnel security, administrative security and classified visit management records to include capturing the data related to suitability determinations, background investigations, security clearance processing, security container/document tracking, contract administration and incoming/outgoing classified visitor tracking. The records in this system reflect the tracking/status of activities related to the management and implementation of OCSO programs that support the protection of the Department's personnel, property, facilities and information.

3. ISMS Roles and Responsibilities

A. The OCSO is responsible for identifying, defining and providing support services to the ISMS user community during the implementation and operational phases of the project. In response to this commitment, OCSO has established the Security Systems Division (SSD) and has chartered them with ISMS operations, maintenance and customer support.

B. As a means to formalize the ISMS usage agreement between the OCSO and each DHS Operational Component a Memorandum of Understanding (MOU) is completed each fiscal year implementing the following requirements. SSD provides the following services:

(1) Web-based access to the ISMS production and test environments at DHS Data Center (DC1).

(2) Web-based access to the ISMS production and test environments at DHS Data Center 2 (DC2).

(3) Data storage for ISMS-related documents and attachments.

(4) Level II user support to ISMS points of contacts (POCs).

(5) Voting rights in the ISMS Change Control Board (CCB) to provide direction on future enhancements/modifications.

(6) Access to revised ISMS quick reference guides developed by the SSD.

(7) An ISMS Application Use Policy.

(8) ISMS Information Notices and procedures.

(9) Access to SSD report development and hosting services.

(10) Access to SSD ISMS newsletters and training materials.

(11) Notifications of planned system maintenance and downtime.

(12) Notifications of unexpected system outages.

(13) Information security services to ensure compliance with ISMS System Security Plan.

(14) Database backup and recovery services.

(15) Planning for disaster recovery/contingency events.

(16) Common interface execution (i.e., NFC, CVS, IDMS, 79A, agency delivery).

(17) Diagnostic support for network connectivity and network authentication services to determine if issue results from ISMS configuration issue or data center/Operational Component-supported function.

C. SSD is not be responsible for the following functions/services:

(1) Level I user support (i.e. account creation, password resets, role assignment) as this is provided by the Component ISMS administrators.

(2) Resolution of Component network issues that disrupt connectivity to data centers hosting ISMS.

(3) Resolution of network account authentication services provided by the Component.

D. Operational Components are responsible for the following:

(1) Provide annual funding via an Intra-Agency Agreement (IAA) or similar mechanism in an amount proportional to the respective Operational Component's use of the system as determined by SSD. The estimate is based on multiple factors including number of active users, number of positions, number of service requests, number of report requests and system storage requirements.

(2) Identify an ISMS Site Coordinator(s) to serve as the point of contact between SSD and their respective organization. The Site Coordinators are responsible for Operational Component related data migration/integrity activities, data management and user account administration, information distribution and for facilitating key events such as user training and system upgrades.

(3) Identify a representative for the ISMS Change Control Board (CCB).

(4) Provide Level I user support for their Operational Component users which includes account creation, basic ISMS usage questions, password resets and role assignments.

(5) Ensure that those providing Level I support have undergone ISMS Administrator training.

(6) Ensure that their users adhere to the ISMS Application Use Policy.

(7) Abide by ISMS Information Notices and procedures published by SSD to ensure compliance with the ISMS System Security Plan.

(8) Ensure that users protect ISMS data, in accordance with the Privacy Act of 1974, the Unauthorized Access Act (18 U.S. Code 2701 and 2710) and other applicable federal law and policy.

(9) Address issues with network connectivity and network account authentication services to the Operational Component OCIO.

(10) Promptly report any incidents regarding Use Policy violations, Privacy violations or security incidents to [redacted]. Security incidents should also be reported to the Chief, Security Systems Division.

4. Privacy Impact Assessment (PIA)

A. The ISMS Privacy Impact Assessment (PIA) provides information on records maintained by OCSO and DHS Operational Components within ISMS for DHS covered individuals.

B. ISMS personnel security data is used internally by DHS with the exception of data sharing requirements related to employment eligibility, clearance verification associated with the classified visitor management program, the transfer of relevant PII to OPM, the Scattered Castles database and the Department's Identity Management System (IDMS).

5. Privacy Act Statement of Records Notices (SORNs) Applicable to ISMS

A. Department of Homeland Security/ALL--023 Personnel Security Management System of Records, Federal Register: February 23, 2010 (Volume 75, Number 35, pages 8088-8092).

B. Department of Homeland Security/ALL--024 Facility and Perimeter Access Control and Visitor Management System of Records, Federal Register: February 3, 2010 (Volume 75, Number 22, pages 5609-5614).

6. ISMS Use Policy

A. ISMS users agree to protect their ISMS user account information (username & password) from disclosure by all reasonable means, and are not to willingly divulge it or permit its use knowingly by another person including System Administrators. If the ISMS user account is compromised, or used by another person, the account holder agrees to notify their immediate supervisor and the ISMS system owner.

B. ISMS users are not authorized to open, review, or create their own personal information (i.e. Person, Position, Case, or Special Access Information) in the ISMS application.

C. ISMS users are not authorized to use an ISMS user account of another user.

D. ISMS users are not authorized to open, review, create or update the information (i.e. Person, Position, Case, or Special Access Information) of another individual for reasons other than designated work duties.

E. ISMS users are not authorized to create sample, test, or training information in the live ISMS production environment.

F. ISMS users are to comply with all terms and conditions specified in DHS Management Directive 4900, Individual Use and Operation of DHS Information Systems and Computers and account holders are to protect ISMS information as outlined in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information.

G. Modification of any ISMS role definitions by anyone outside the DHS OCSO, Security Systems Division (SSD) is prohibited. Any modification is authorized by the Chief, Security Systems Division. The role definitions determine the screens available to each role and whether they are read-only.

H. DHS OCSO/SSD has the right to suspend/revoke any user's access or remove any role from a user including a Component ISMS Administrator if a potential risk to the system and/or a violation of this Use Policy has been identified. DHS OCSO/SSD may choose at its discretion to reinstate access after appropriate documented supervisory counseling on the ISMS Application Use Policy. Unauthorized reinstatement of an account suspended/terminated by the DHS OCSO/SSD or adding roles to a user account that have been removed by the DHS OCSO/SSD is considered a violation of this policy.

I. ISMS users should have no expectation of privacy associated with their use of the system. Furthermore, ISMS users consent to monitoring of system use, transaction logs, account login logs and record audit data.

7. Standards for Access

A. All ISMS users are required to have a minimum investigation of a moderate risk investigation. All ISMS users are required to have received DHS computer security training, Privacy Awareness training, and have been vetted and/or cleared for access to privacy, sensitive and/or classified information.

B. All users requesting access are required to read the ISMS Application Use Policy, complete the ISMS User Account Request form, sign the form and obtain their supervisor's and/or Site Coordinator's signature.

C. Waivers for access standards need to be justified and endorsed by the Operational Component's Chief Security Officer. Waiver requests are submitted to the Chief, Security Systems Division and are approved or denied by the DHS CSO.

8. Violations of ISMS Policy

A. DHS employees may be subject to disciplinary action for unauthorized use or misuse of ISMS. The ISMS Application Use Policy states that ISMS users are restricted from opening, reviewing, or creating their own personal information in

the ISMS application. The purpose of this policy is to protect the investigative and security action information stored in the system from unauthorized disclosure.

B. If an ISMS user attempts to view their ISMS record, the ISMS application closes and the user's account is locked out. In order to unlock the account the violator requires counseling by their supervisor and is required to re-sign the Application Use Policy.

9. Non-Security Personnel

A. The ISMS Information Notice, FY12-04, ISMS System Access Guidance, serves as a guideline for approving ISMS access requests for non-personnel security users and other professionals outside the Security Enterprise[1]. The guidance applies to DHS federal employees, contractor employees and detailees, referred to herein as "professionals" external to the Security Enterprise, or to those professionals within the Security Enterprise who are not responsible for processing personnel security records.

B. Requests for access to ISMS by non-security personnel are reviewed on a case-by-case basis by the ISMS Site Coordinator. The personnel security chief of the requestor's operational component is responsible for access approvals or denials. ISMS user accounts are individually approved by the appropriate personnel security office chief(s) before they are provisioned by the ISMS Site Coordinator. Read/Write access is role-based and data is only accessible if a specific user has been approved for access to the data.

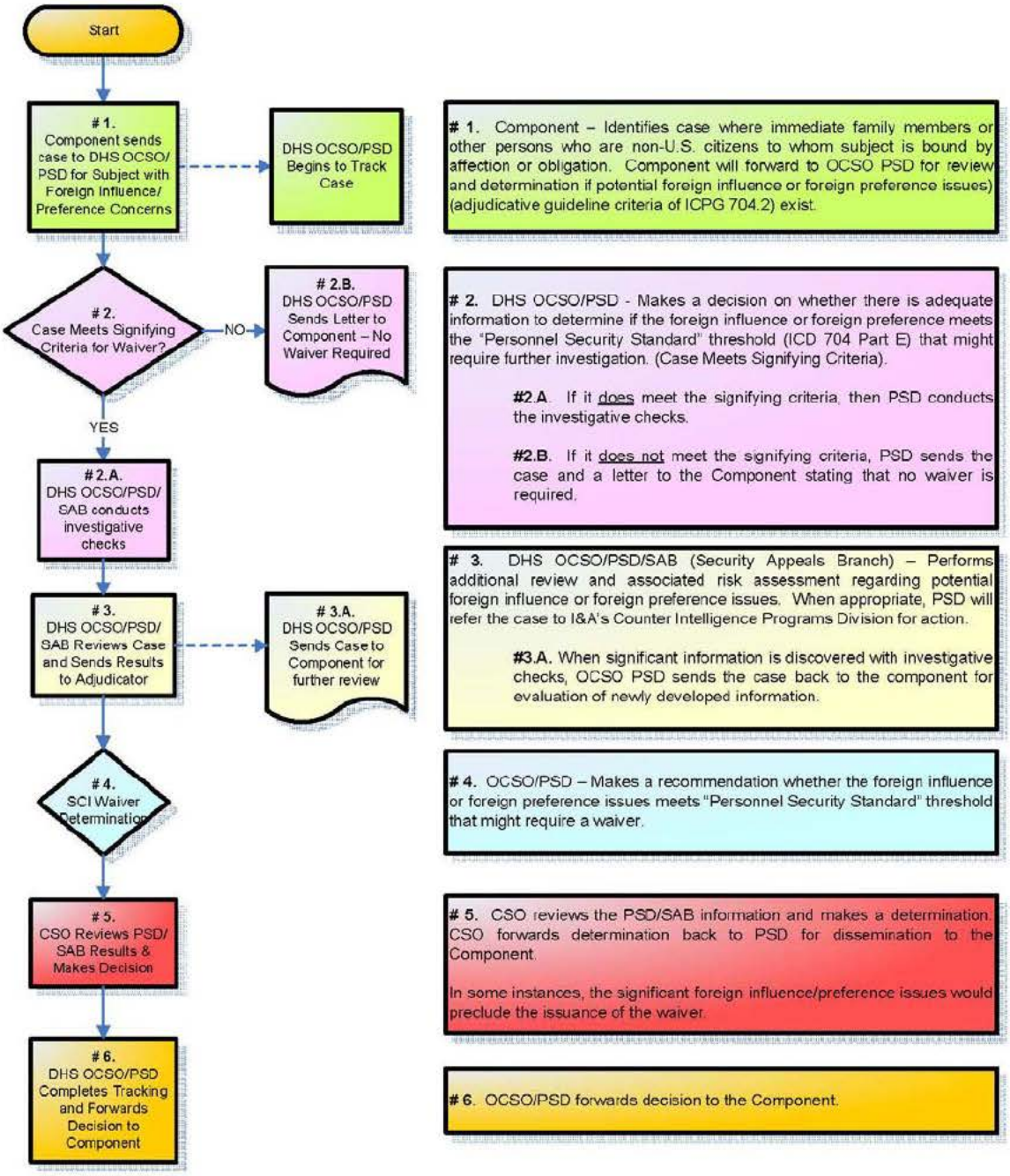
[1] The term "Security Enterprise" is used to represent those professionals dealing with personnel security, information security, administrative security, etc. across the Department of Homeland Security.

APPENDIX A, Federal Investigative Standards

- Investigations on Tiers 2 and above receive periodic reinvestigations every 5 years and may also be subject to Continuous Evaluation.

- For definitions and more information on position risk/sensitivity levels, the types of investigations, Standard Forms and additional forms required for the submission of investigations, refer to U.S. Office of Personnel Management (OPM) guidance.

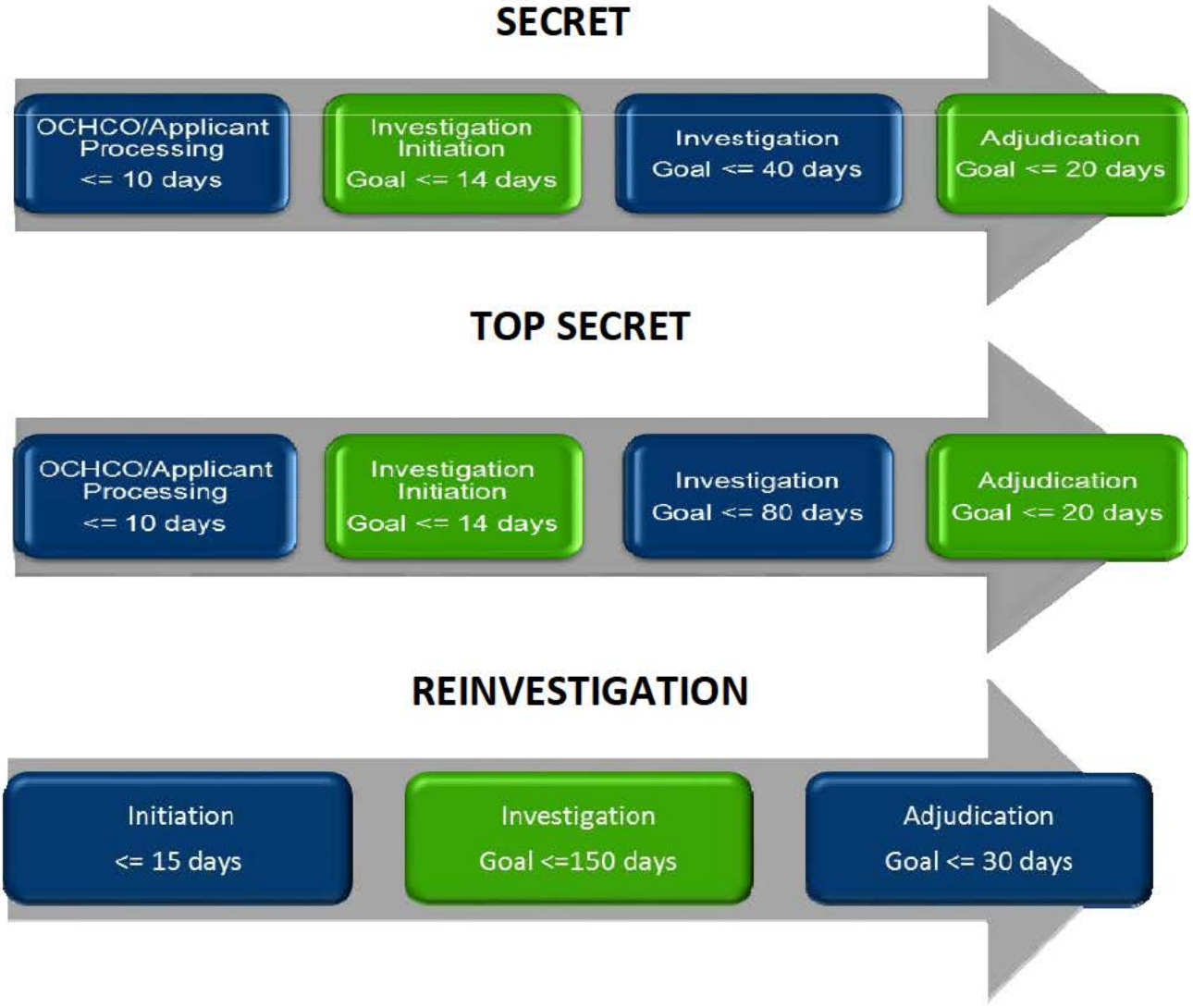
APPENDIX B, Intelligence Community Directive Number 704 (ICD 704) Exception Process



2/15/2013

APPENDIX C, Intelligence Reform and Terrorism Prevention Act (IRTPA) Metrics and Personnel Security Process Timeliness

Personnel Security Process With IRTPA Timelines



APPENDIX D, Definitions

For the purposes of this Instruction, the following terms have the definitions set forth below. Also refer to U.S. Office of Personnel Management guidance for definitions of the types of investigations and the security forms.

1. ***Access to Classified Information (access)***: The ability and opportunity to obtain knowledge of classified information in accordance with E.O. 12968.

2. ***Adjudication***: An examination of a person's character and conduct over a sufficient period of time designed to make a determination as to their suitability or fitness for employment; eligibility for access to Classified Information; Special Access Programs (SAP), materials, or areas; or for their retention in federal employment and continued access to classified information and Special Access Programs.

3. ***Adjudicator****:* A personnel security specialist who performs adjudications (see above).

4. ***Administrative Withdrawal:*** When regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties, the previously authorized access eligibility level needs to be administratively downgraded or withdrawn, as appropriate.

5. ***Appeal***: A formal request, submitted by an applicant, employee, former employee, or contractor employee for review of a decision.

6. ***Applicant****:* A person who is being considered or has been considered for employment.

7. ***Appointee***: A person who has entered on duty and is in the first year of a subject-to-investigation appointment.

8. ***Background Investigation***: A generic term used to describe the various types of personnel security investigations into an applicant's or an employee's history that are used to determine the individual's suitability or fitness for employment and whether the individual is eligible for access to classified information at the appropriate level for the position. These investigations are conducted using a variety of methods including the completion of standard form questionnaires, electronic inquiries, written or telephonic inquiries, or through personal contact with individuals.

9. ***Cognizant Security Authority (CSA)***: A senior security official designated by the Secretary for overseeing all aspects of security program management within an organization.

10. ***Chief Security Officer (CSO)***: The DHS official in charge of the OCSO, who

exercises leadership and authority over security policy and programs DHS-wide, in partnership with Component heads.

11. ***Classified Information***: Information that has been determined, pursuant to E.O. 13526 or any predecessor order, and the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

12. ***Competitive Service:*** As defined in 5 U.S.C. §2102, the federal competitive service consists of all civil service positions in the executive branch that are not specifically excepted from the civil service laws by or pursuant to statute, by the President, or by OPM under Rule VI, and that are not in the Senior Executive Service (SES).

13. ***Confidential Information***: Is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

14. ***Consultant****:* An individual that has a defined relationship with the Department to provide a product or perform services; not otherwise working on a contract.

15. ***Continuous Evaluation (CE)***: E.O. 13467 requires that an individual who has been determined to be eligible for, or who currently has access to classified information, be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence (DNI) as the Security Executive Agent.

16. ***Contract***: A mutually binding legal agreement 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.

17. ***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. 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.

18. ***Covered Individual***: For the purposes of this Instruction, a person who performs

work, or is an applicant to perform work, for or on behalf of the Department of Homeland Security.

19. ***Critical Sensitive (CS)***: Positions designated in accordance with 5 CFR Part 732, or subsequent iterations, that have duties with the potential to cause exceptionally grave damage to the national security. These positions may require eligibility for access up to Top Secret national security information or materials; or other positions related to national security, regardless of duties, that require the same degree of trust.

20. ***Denial of Eligibility for Access to National Security Information***: An adjudicative decision under E.O. 12968 that a covered individual is not eligible for access to classified information.

21. ***Deputy Secretary***: The Deputy Secretary of the United States Department of Homeland Security.

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

23. ***DHS Facility***: DHS-owned buildings or leased space and controlled access space, whether for single or multi-tenant occupancy, and its grounds and admittance, 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 employee-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.

24. ***Eligibility Determination***: Determinations of eligibility for access to classified information are based on criteria established under E.O. 12968.

25. ***Eligibility for Access to Classified Information***: The result of the determination whether an employee (a) is eligible for access to classified information in accordance with E.O. 12968 (relating to access to classified information), or any successor thereto, and E.O. 10865 of February 20, 1960, as amended (related to safeguarding classified information with industry), or any successor thereto; and (b) possess a need to know under such orders.

26. ***EOD***: Entry or Entrance on Duty.

27. ***EOD Determination***: An Entry on Duty (EOD) determination is a preliminary risk management decision (favorable or unfavorable) that an applicant may or may not commence work before the required background investigation is completed. The investigation should be submitted within 14 days of applicant certification. The EOD

determination does not substitute for the required background investigation and it does not represent a final suitability or fitness determination.

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

29. ***Federal Employee***: A person other than the President and Vice President, employed by an agency in the Federal Executive Branch. For purposes of this Instruction, it includes officers and members of the Armed Forces, but does not include members of the Coast Guard Auxiliary.

30. ***Fitness***: 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.

31. ***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.

32. ***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.

33. ***Information Technology (IT) Systems***: IT is defined by 40 U.S.C. §11101(6). For purposes of this Instruction, IT Systems include technology systems that are (1) owned, leased, or operated by a Component; (2) operated by a contractor employee on behalf of DHS; or (3) operated by another federal, state, or local government agency on behalf of DHS.

34. ***Integrated Security Management System (ISMS)***: A web-based personnel security case management tool designed to support the lifecycle of DHS personnel security and suitability cases to include the capture of information related to background checks, investigations and final determinations.

35. ***Investigator****:* A federal employee or contractor employee responsible for conducting background investigations (see Background Investigation).

36. ***Legal Permanent Resident (LPR)***: A person who has been granted lawful permanent residence in the United States.

37. ***Local***: (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under

state law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity.

38. ***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.

39. ***National Security Positions***: As defined in 5 CFR 732.102: (1) Those positions that involve activities of the Government that are concerned with the protection of the Nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) positions that require regular use of, or access to, classified information.

40. ***Need for Access***: A determination that an employee requires access to a particular level of classified information or a particular category of special nuclear materials in order to perform or assist in a lawful and authorized function.

41. ***Need-to-Know***: In accordance with E.O. 12968, 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.

42. **Nexus**: A direct or logical connection between a person's character or conduct and the integrity or efficiency of the service.

43. ***Non-Critical Sensitive (NCS)***: Positions that have the potential to cause damage to the national security, up to and including damage at the significant or serious level and may require eligibility for access to classified material at the Secret or Confidential level.

44. ***Non-Sensitive/Low Risk***: Positions that have the potential for limited impact on the integrity and efficiency of the federal service and have no clearance or other sensitive national security duties. These positions involve duties and responsibilities of limited relation to an agency or programmission.

45. ***Operational Component Security Office (Component)***: A Component with specific centralized program responsibility for directly achieving one or more of the Department's mission activities; generally has authority over its finance, human resources, information technology, procurement and security programs. The DHS OCSO, PSD and the personnel security offices of the following DHS Operational Components have the authority to make suitability, fitness and security clearance determinations:

A. United States Citizenship and Immigration Services (USCIS)
B. United States Coast Guard (USCG)
C. Customs and Border Protection (CBP)
D. Federal Emergency Management Agency (FEMA)
E. Transportation Security Administration (TSA)
F. U.S. Immigration and Customs Enforcement (ICE)
G. United States Secret Service (USSS)

46. ***Original Classification Authority (OCA)****:* An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

47. ***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, corporations, private voluntary organizations and non-public educational institutions, as well as all other nonprofit institutions.

48. ***Position Designation***: The position designation process determines, through the evaluation of national security and suitability requirements, what type of investigation is required and how closely an applicant or incumbent is screened for a position. In order to ensure a systematic, dependable and uniform way of making position designations across agencies for the purposes of reciprocity, OPM provides the Position Designation Automated Tool on their website for those individuals charged with position designation responsibilities.

49. ***Protected Disclosure***: (a) A disclosure of information by the employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; (b) any communication described by and that complies with subsection (a) (1), (d), or (h) or section 8H of the Inspector General Act of 1978 (5 U.S.C. App.); subsection (d) (5) (A) of section 17 of the Central Intelligence Agency Act of 1949 (50 USC 403q); or subsection (k) (5) (A), (D), or (G) of section 103H of the National Security Act of 1947 (50 U.S.C. 403-3h); (c) the exercise of any appeal, complaint, or grievance with regard to the violation of Section B of PPD-19.

50. ***Public Trust Positions***: Positions defined under 5 CFR 731.106(b) 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

finance records, with a significant risk for causing damage or realizing personal gain.

51. ***Reciprocity***: Recognition and acceptance of another federal agency's investigation or adjudication determination that meets the national standards, barring any exception or newly developed information.

52. ***Revocation of Eligibility for Access and/or 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.

53. ***Risk Level***: An assessment (low, moderate, or high) of a position to determine its potential for adverse impact to the integrity or efficiency of the service, its effect on the agency or on the agency's mission.

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

55. ***Secretary***: The Secretary of the United States Department of Homeland Security.

56. ***Security Clearance***: An administrative determination in accordance with E.O. 12968 made by competent authority that an individual is eligible, has a need-to-know, has been briefed and met all of the requirements from a security standpoint for access to classified information.

57. ***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 Office of the Director of National Intelligence.

58. ***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 all of the following categories of information:

    a. ***Controlled Unclassified Information (CUI)***: E.O. 13556 defines and addresses CUI.
    b. ***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 CFR Part 29, or the applicable PCII Procedures Manual.
    c. ***Sensitive Security Information (SSI)***: As described in 49 CFR Part

1520.

59. ***Sensitive Position***: Any position within a department or agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security as defined in Section 3(b) of E.O. 10450.

60. ***Sensitivity Level***: A position assessment designation indicating the degree of damage an individual in the position could effect to the national security.

61. ***Special Access Program (SAP)***: A program that is established for a specific class of classified information that imposes safe guarding and access requirements that exceed those normally required for information at the same classification level. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 13526.

62. ***Special Security Officer (SSO)***: Administers the receipt, control and accountability of SCI. The SSO oversees SCI security functions and reporting requirements.

63. ***Special Sensitive (SS)***: Any position designated at a level higher than Critical Sensitive. These positions have duties with the potential to cause inestimable damage to the national security. These positions may require eligibility for access up to, and including, Top Secret, SCI, or Special Access Program (SAP) levels.

64. ***State***: The term ‘‘state’’ means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands and any possession of the United States.

65. ***Suitability:*** An evaluation in accordance with 5 CFR Part 731, based on a person’s character or conduct, to decide whether an individual’s employment or continued employment would or would not protect the integrity or promote the efficiency of the service. A suitability determination is a process separate and distinct from a security clearance determination.

66. ***Suitability Action***: Per 5 CFR § 731.101(b), a suitability action means an outcome described in 5 CFR 731.203 (cancellation of eligibility, removal, cancellation of reinstatement eligibility, debarment) that may be taken by OPM or an agency with delegated authority under the procedures in 5 CFR 731 subparts C and D.

67. ***Suitability Determination***: Per 5 CFR § 731.101(b), a suitability determination is a decision made by OPM or an agency with delegated investigative authority, such as DHS, that a person is suitable or not suitable for employment in covered positions in the federal government or a specific federal agency.

68. ***Support Component***: A Component that generally provides specific assistance and/or guidance to other DHS Components and/or external organizations. Support

Components generally utilize shared services through Management.

69. ***Suspension of Security Clearance***: A temporary action in which a person who had access to classified information is rendered ineligible to continue such access. It is not considered an adverse action and it is not appealable.

70. ***Temporary Employee***: An employee appointed within DHS for six months or less.

71. ***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.

72. ***U.S. Entity (including Tribal entities):*** (1) state, local, or tribal governments; (2) state, local and tribal law enforcement and firefighting entities;(3) public health and medical entities; (4) regional, state, local and tribal emergency management entities, or (5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources (CIKR).

73. ***Volunteer****:* A person who renders aid, performs a service, or assumes an obligation voluntarily.