U.S. Department of Transportation
Office of the Secretary of Transportation

ORDER

1630.2C

Subject: PERSONNEL SECURITY MANAGEMENT

1. PURPOSE

This Order prescribes policies to ensure an effective and efficient personnel security program for the U.S. Department of Transportation (DOT) and to implement within DOT all applicable laws, Executive Orders (EO), and Government-wide regulations pertaining to personnel security. The Order assigns responsibilities for DOT's program to determine the suitability of employees being considered for initial or continued access to classified national security information.

2. BACKGROUND

A background investigation is conducted to ensure the candidate is suitable for employment, i.e. reliable, trustworthy, of good conduct and character, and loyal to the United States. Additionally, background investigations are conducted to determine whether new Federal or contractor employees' past conduct or behavior will have a negative impact within DOT. The scope of the investigation varies with the level of clearance being sought. The investigation is conducted to allow the government to assess whether a candidate is sufficiently trustworthy to be granted access to classified information.

The background investigation and records checks for Secret and Top Secret security clearances are mandated by Presidential Executive Order. The EO requires these procedures to be followed prior to the granting of a security clearance. The attached manual outlines these procedures.

Previously, new Federal employees and contractor employees were given access to DOT facilities, sensitive information and information technology systems prior to completion of an initial suitability determination. In some cases, subsequent to a favorable adjudication, background investigations revealed suitability issues with some individuals hired as Federal employees or assigned to work on DOT contracts which precluded their retention. With the development and publishing of DOT Order 1631.1, Agency Access Order, a process has been established to provide minimum requirements for the pre-appointment and on-boarding of new Federal employees and contractors.

3. SCOPE

This Order applies to all DOT Secretarial Offices (OST) and Operating Administrations (OAs) with the exception of the Federal Aviation Administration.

4. CANCELLATIONS

a. This Order cancels the following publication:

DOT Order 1630.2B, Personnel Security Management, dated May 30, 2001.

b. The following publications were cancelled by an earlier version of this Order and are listed here for informational purposes:

(1) DOT Order 1630.2A, DOT Personnel Security Program Handbook, May 27, 1988.

(2) DOT Order 1630.3, U.S. Department of Transportation Personnel Security Policies, November 17, 1972.

(3) DOT Security Bulletin SEC 96-02, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, August 6, 1996.

(4) DOT Security Bulletin SEC 96-04, Reciprocal Acceptance of Access Eligibility Determinations, June 13, 1997.

5. REFERENCES

a. 5 C.F.R. § 731 (2014), Personnel Suitability.

b. 5 C.F.R. § 732 (2014), National Security Positions.

c. 5 C.F.R. § 736 (2014), Personnel Investigations.

d. 32 C.F.R. 147 (2013), Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

e. Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004, Schedule 18, Security and Protective Services Records, December 17, 2004.

f. Executive Order 10450, Security Requirements for Government Employment, August 10, 1961, as amended.

g. Executive Order 10577, Amending the Civil Service Rules and authorizing a new appointment system for the competitive service, November 22, 1954, as amended.

h. Executive Order 12829, National Industrial Security Program, January 6, 1993, as amended.

i. Executive Order 12968, Access to Classified Information, August 2, 1995, as amended.

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

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

l. Executive Order 13526, Classified National Security Information,December 29, 2009.

m. Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

n. Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.

o. Presidential Policy Directive 19 (PPD-19), Protecting Whistleblowers with Access to Classified Information, October 10, 2012.

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

q. Office of Management and Budget Memorandum, Reciprocal Recognition of Existing Personnel Security Clearances, December 12, 2005.

r. Memorandum from the Assistant to the President for National Security Affairs, "Adjudicative Guidelines", December 29, 2005.

s. Memorandum from the Director, Office of Personnel Management, Guidance on Implementing Executive Order 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust", September 24, 2009.

t. Memorandum from the Director, Office of Personnel Management, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12", July 31, 2008.

u. Joint Memorandum from the Office of the Director of National Intelligence and the Office of Personnel Management, Approval of Federal Investigative Standards, December 13, 2008.

v. Security Executive Agent Directive 1, Security Executive Agent Authorities and Responsibilities, March 13, 2012.

w. Intelligence Community Directive Number 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, October 1, 2008.

x. Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, revised February 8, 1996.

y. Office of Management and Budget Memorandum, Reciprocal Recognition of Existing Personnel Security Clearances, July 17, 2006.

z. Department of Transportation Order 1642.1, Defensive Counterintelligence and Insider Threat Program Order, October 21, 2013.

aa. Department of Transportation Order 1631.1, Granting New Federal and Contractor Employees Access to Department of Transportation Facilities, Resources, and Systems, April 3, 2013.

bb. Department of Transportation Order 1681.2, HSPD-12 PIV Card Program, December 21, 2011.

6. POLICY

a. DOT shall not employ or retain an individual in a position requiring access to classified information unless a determination has been made on behalf of the Secretary of Transportation that such employment or retention is consistent with the interests of national security.

b. DOT shall grant an individual eligibility for access to classified national security information only when facts and circumstances indicate that access to such information is clearly consistent with the national security interests of the United States. Any doubt shall be resolved in favor of national security.

c. All personnel responsible for determining individuals' eligibility for access to classified information shall have completed a minimum of 2 weeks of formal

suitability training. The training curriculum shall meet current criteria specified and/or used by the Office of Personnel Management or the Office of the Director of National Intelligence and shall comply with standards in effect for the Executive Branch.

d. DOT shall grant no one access to classified national security information unless the required background investigation has been completed for the level required, the background investigation has been favorably adjudicated, the individual has a foreseeable need for access to classified national security information to perform his or her duties, and the individual has signed an approved classified information nondisclosure agreement. In rare circumstances personnel security adjudicators may grant access to classified information to persons for whom the required investigations have not been completed, consistent with government-wide requirements for granting interim or temporary access.

e. DOT shall afford fair, impartial, and equitable treatment, including the provision of reasonable accommodation, to all DOT employees and applicants, contractor employees, and affiliated personnel through consistent application of personnel security standards, criteria, and procedures as specified in applicable laws, regulations, and orders. The Department shall not discriminate on the basis of race, color, religion, sex, national origin, genetic information, age, disability, protected activity or sexual orientation in any personnel security actions, including the granting of access to classified national security information.

f. DOT shall not use the denial or revocation of access to classified information as a substitute for, or in lieu of, personnel suitability determinations or other personnel actions when those determinations or actions are warranted.

g. Nothing in this Order shall limit or affect the responsibility and power of the Secretary, pursuant to any law or Executive Order, to deny or terminate an individual's access to classified national security information in the interest of national security.

h. DOT shall provide to all applicants, employees, and contractor personnel the opportunity to explain or refute any unfavorable information before the Department uses the information as a basis for any adverse personnel, security, or similar action against them. The applicant, employee and/or contractor shall have 30 days upon notification to respond to such notice.

i. No person whom the Secretary has removed from employment for security reasons shall be re-employed by DOT without the Secretary's prior approval.

j. Investigative and personnel security records may be disclosed to the public only to the extent required by the Privacy Act and the Freedom of Information Act.

7. RESPONSIBILITIES:

a. The Office of Assistant Secretary for Administration shall:

(1) Direct and administer the DOT personnel security program.

(2) Administer and implement DOT personnel security policies and ensure effective compliance with all laws, Executive Orders, and regulations that govern the personnel security program.

(3) Represent DOT on personnel security matters to other agencies and organizations both within and outside the Federal Government.

(4) Periodically evaluate DOT's implementation of and adherence to personnel security policies and requirements.

(5) Provide, through the Director, Office of Security, needed personnel security support services for the Office of the Secretary and for those DOT OAs and other organizations that have not been delegated their own personnel security operating authority.

(6) As required, prepare consolidated personnel security program reports for and on behalf of the Department.

b. Secretarial Officers and Heads of Operating Administrations shall:

(1) Implement policies promulgated by the Office of the Assistant Secretary for Administration and ensure all provisions are effectively administered.

(2) Ensure sufficient personnel and funding are provided to implement all DOT personnel security policies.

(3) Fulfill Personnel Security Office reporting requirements.

(4) Timely inform the Office of Security of any significant personnel security problems or issues.

(5) As warranted, promptly take all steps necessary to correct any personnel security program deficiencies.

c. Director, Office of Security (M-40) shall:

(1) Provide guidance and direction throughout DOT on all personnel security matters.

(2) Provide personnel security support services for OST and all DOT OAs to which the Assistant Secretary for Administration has not delegated specific personnel security operating authority.

(3) Evaluate all DOT personnel security activities and, as appropriate, either make or recommend needed changes in policies and procedures.

(4) Serve as the liaison with other Government agencies on personnel security matters.

(5) Authorize exceptions to DOT personnel security policies and procedures when doing so meets an urgent management need, is consistent with the interests of national security, does not infringe on the rights of any employee or applicant, and does not conflict with authority reserved by either the Secretary or the Assistant Secretary for Administration.

d. Responsibilities for all Employees:

(1) Awareness: Be aware of the standards of conduct required for persons holding positions of trust. Recognize and avoid the kind of personal behavior that could result in rendering one ineligible for continued assignment in such a position. Be aware of responsibilities when traveling abroad including attendance at international conferences. Employees are ultimately responsible for maintaining continued eligibility for these positions.

(2) Personal Information: Individuals who hold a security clearance shall immediately inform their servicing security organization of changes in their personal life and of activities that might affect their eligibility for access to classified information, as required by EO 12968.

(3) Report: As required by EO 12968, report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security. Employees should report such information to their servicing security organization.

(4) Familiarize: Be familiar with security regulations and the contents of this Order and DOT M 1630.2C, Personnel Security Management Manual, pertaining to their assigned duties.

(5) Protect: Properly protect all classified information from unauthorized disclosure and report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to such information.

(6) Violations: Report all violations of security regulations to their servicing security organization.

8. DELEGATED PROGRAM AUTHORITY

The Federal Aviation Administration (FAA) is delegated authority to administer its own personnel security program. The FAA's program shall implement the policies of this Order and DOT M 1630.2C, Personnel Security Management Manual. Subject to M-40 concurrence, the FAA may adopt procedures that implement DOT personnel security policies in ways that are different from those prescribed in the manual.

9. IMPLEMENTATION

Except as permitted by Paragraph 8, the policies and responsibilities set forth in this Order and the procedural requirements contained in the Personnel Security Management Manual, DOT M 1630.2C, are for uniform application throughout DOT.

ASSISTANT SECRETARY FOR ADMINISTRATION

KEITH E WASHINGTON

Digitally signed by KEITH E WASHINGTON
DN: c=US, o=U.S. Government, ou=DOT Headquarters, ou=OSTHQ, cn=KEITH E WASHINGTON
Date: 2015.04.27 15:54:56 -04'00'

Signature Date

DOT Order 1630.2C

PERSONNEL SECURITY

MANAGEMENT

MANUAL

Office of Security
Office of the Assistant Secretary for Administration
Office of the Secretary

TABLE OF CONTENTS

Chapter VI - Investigative Requirements for Contractor Employees

Chapter VII - Initial Access to DOT Facilities, Resources, and Information Technology Systems

Chapter VIII - Reciprocity and Standards for Using Previous Investigations

Chapter IX - Role of M-40 in Suitability or Fitness Adjudication

Chapter X - Security Adjudication - Granting Eligibility for Access to Classified Information

Chapter XI – Eligibility for Access to Classified Information

Chapter XII - Adverse Security Actions

Chapter XIII - Foreign Assignments and Travel

Appendix 1 – Definitions

Appendix 2 – Acronyms

Chapter I

GENERAL INFORMATION

1. Purpose

a. The purpose of this manual and its appendices is to implement the policies of U.S. Department of Transportation (DOT) Order 1630.2C, Personnel Security Management, and to establish a uniform personnel security program for DOT. This program is designed to protect classified national security information (hereafter "classified information"), ensure cost effectiveness of the Personnel Security Program, and provide fair and equitable treatment to all DOT employees and applicants considered for initial or continued access to classified information, consistent with the interests of national security. Reasonable accommodations shall be provided to persons with a disability in connection with interviews and other information collection procedures. The program also includes the initiation and processing of required background investigations on all Federal and contractor employees.

b. This manual sets forth the standards, criteria, and guidelines for personnel security determinations, describes the types and scopes of personnel security investigations, specifies investigative requirements, and states the procedures necessary to appeal adverse security actions in regard to individuals' access to classified information. Additionally, it provides guidance for employees whose security clearance has been denied or revoked.

c. This manual addresses the relationship between security and suitability determinations with respect to the hiring and retention of persons for DOT employment.

d. This manual contains requirements and procedures for conducting investigations of contractor employees and child care center workers. It also contains basic procedures for processing contractor employees for access to classified information under the provisions of the National Industrial Security Program.

e. This manual addresses protections offered to those employees currently holding classified national security clearances who have engaged in whistleblower activities.

2. Delegated Program Authority

The Federal Aviation Administration (FAA) is delegated authority to administer its own personnel security program, including the authority to grant security clearances for access to classified national security information. The FAA program shall implement the policies of DOT Order 1630.2C and this manual. Subject to concurrence of the Director, Office of Security (M-40), the FAA may adopt procedures that implement DOT personnel security policies in ways different from those prescribed in this manual provided they are sufficient to meet the requirements contained in Order 1630.2C.

Chapter II

PERSONNEL SECURITY OPERATIONS AND RESPONSIBILITIES

1. Standards of Operation and Specific Responsibilities

a. Standards. DOT personnel security operations shall meet the following standards:

(1) Each Operating Administration (OA) and Secretarial Office shall appoint a Personnel Security Coordinator to become the liaison between the hiring organization, the applicant or contractor and the Office of Security (M-40).

(2) In M-40's Personnel Security Division, only professionally qualified personnel security managers shall direct personnel security operations. Personnel Security Adjudicators must be fully trained in accordance with national standards to evaluate reports and results of background investigations and must have successfully completed an approved adjudication course. Adjudicators who are new in their positions may be delegated limited adjudication responsibilities pending completion of an adjudication course, but only under the close supervision of managers or fully trained adjudicators who shall review their adjudications, including all adjudications involving significant issues.

(3) The Office of Personnel Management (OPM) delegates to the Secretary of Transportation authority for making suitability determinations and taking suitability actions (including limited, agency-specific debarments under 5 C.F.R. § 731.205) in cases involving applicants for and appointees to covered positions in DOT. Operating Administration Office of Human Resources (OAHR) shall appoint Labor and Employee Relations Specialists trained in accordance with national standards to adjudicate suitability investigations.

b. Operational responsibilities. The M-40 Personnel Security Manager and specialists have primary responsibility for personnel security operations. The OAHR employing office and contracting officials shall assist M-40 by performing certain personnel security operational duties. The following paragraphs state specific responsibilities for the respective offices.

(1) The M-40 Personnel Security Office shall:

(a) Work with employing offices and OAHR as needed to ensure that position sensitivity and risk level designations are accurate for all positions within their area of responsibility.

(b) Conduct final review of investigative forms prior to release to the OPM.

(c) Check national investigation indices for prior investigations concerning applicants, employees, and contractor employees.

(d) Request/receive from OPM or other sources results of all investigations on applicants, employees, and contractor employees. Review investigative reports to determine the adequacy of the investigations and to identify security and fitness issues. Forward suitability cases to the appropriate OAHR office.

(e) Conduct or arrange for any additional investigation necessary to resolve security, suitability, and fitness issues.

(f) Provide due process to applicants and employees regarding their security investigations as required by Section 2 of this chapter.

(g) Make security determinations on all cases involving sensitive positions. Grant or deny access to classified information (i.e., security clearances). Advise employing organizations and, as necessary, OAHR, of these determinations.

(h) Make initial access determinations as required by DOT Order 1631.1, Granting Access to DOT Facilities, Systems and Information for New Federal and Contractor Employees (Agency Access Order) and in support of HSPD-12 implementation and Entry-on-Duty (EOD) determinations.

(i) Make fitness determinations on contractor employees and other individuals who are not employees but who are being granted access to DOT facilities as described in Chapter 6 of this manual.

(j) When requested, advise and assist OAHR and/or employing offices when they are adjudicating suitability of applicants or employees.

(k) Prepare and conduct initial indoctrination and yearly refresher briefings for security clearance holders.

(l) Provide guidance to OAHR and employing offices on personnel security policies and operating procedures.

(m) Periodically evaluate the personnel security program to ensure it is operating effectively and efficiently.

(n) Process facility visitor clearance requests and certify security clearances as requested.

(o) Advise employing offices and OAHR of all changes in background investigation costs.

(p) Maintain records of the security clearances held by DOT employees. Records will be maintained as required by the Privacy Act.

(2) The employing organization shall:

(a) Determine position sensitivity and risk level designations on positions under its jurisdiction and coordinate with the servicing OAHR and, as needed, the M-40 Personnel Security Office regarding final designations.

(b) Ensure all Optional Form 8 (OF-8) Position Descriptions, or equivalent, either electronic or hard-copy, show the approved sensitivity or risk level designation, as well as any requirement for access to classified information.

(c) When applicable, ensure vacancy announcements state that appointment is subject to a favorably adjudicated background investigation enabling the granting of a security clearance.

(d) Ensure that before placing, or making any commitment to place, a person in a special-sensitive, critical-sensitive, or noncritical-sensitive position, the M-40 Personnel Security Office has determined the pre-placement investigative requirement has been met or an appropriate waiver has been granted.

(e) Request waivers of pre-placement investigative requirements from the M-40 Personnel Security Office when emergency conditions exist which preclude the ability to meet requirements.

(f) Review investigative forms for completeness, confirm the necessity for investigations, and initiate personnel security investigations as required.

(g) Coordinate with the M-40 Personnel Security Office all budgeting for the conduct of personnel investigations and provide to M-40 organizational staffing projections for investigative budgeting per OPM mandates.

(h) Assist applicants and employees, in a timely manner, to provide the required electronic submissions [e.g., completing forms in Electronic Questionnaires for Investigations Processing (e-QIP)] to M-40, report as necessary for fingerprinting, and provide any forms or other information required to initiate required background investigations per the Agency Access Order.

(i) Advise the M-40 Personnel Security Office of any questionable conduct or activity by an employee or contractor employee which could raise a security or suitability issue.

(3) The OAHR shall:

(a) Coordinate with the M-40 Personnel Security Office on each new or revised position description to ensure the original OF-8 or equivalent shows the approved risk or sensitivity level.

(b) Ensure all designations are correctly entered into the HR databases.

(c) Ensure all vacancy announcements contain appropriate information about any investigative or personnel security clearance requirements that are a condition of employment for the advertised the position.

(d) Assist employing offices with accessing personnel security questionnaires in e-QIP, fingerprints, and other forms as required for personnel security processing. Ensure required documents are properly completed and submitted in time to initiate investigations as required by Chapter 5 in this Manual.

(e) Obtain available Electronic Official Personnel Folder (eOPF) data about previous investigation(s) when an applicant is a current or former Federal employee. Provide this information to the M-40 Personnel Security Office when the person is applying for other than a low-risk position, and advise M-40 whenever the eOPF contains no conclusive proof of a prior investigation.

(f) Coordinate with M-40 regarding any information about an applicant that would raise a security or suitability issue. This includes information disclosed on an employment application or personnel security questionnaire, or from pre-placement inquiries, prior employers, the eOPF, or any other sources.

(g) Refer to M-40 any information about an employee that could raise a security or suitability issue.

(h) Review investigative forms for completeness, confirm the necessity for investigations, and initiate personnel security investigations as required.

(i) Request from M-40 or other sources the results of all investigations on applicants and employees. Review investigative reports to determine the adequacy of the investigations and to identify suitability issues.

(j) Obtain approval from the M-40 Personnel Security Office before placing any person in a special-sensitive, critical-sensitive, or noncritical-sensitive position.

(k) Maintain accurate and current records of the sensitivity or risk-level designation for each position.

2. Safeguarding the Rights and Privacy of Employees and Applicants

a. Prior to making a final determination that is unfavorable to the applicant or employee, applicants and employees shall be notified in writing and afforded an opportunity to explain, refute, or deny any unfavorable information obtained as the result of a personnel security investigation before DOT may take any unfavorable action based on that information, including denial of a benefit to which an individual would otherwise be entitled. Any information provided by an employee or applicant must be considered prior to making a final determination. This practice prevents errors

which might otherwise result from mistakes in identity or erroneous information and provides the applicant or employee the opportunity to refute the findings and present mitigating information which may be unknown to the adjudicating officials. The applicant or employee must also be provided any appropriate Privacy Act advisement as mandated by the Privacy Act of 1974 and the E-Government Act of 2002. Any record of the unfavorable information, to include the applicant's or employee's response, may be furnished only to those DOT employees or contractors who, in their official capacity, have a need to know such information and may be disclosed outside DOT only as expressly permitted by the Privacy Act.

b. DOT has established, by Charter, the Personnel Security Review Board (PSRB). The Charter establishes an appeal process for those employees whose security clearance for access to classified information has been revoked or denied. For additional information concerning this process, refer to Chapter 12 - Adverse Security Actions.

c. Medical information of a sensitive or personal nature obtained in conjunction with an investigation shall be carefully controlled to ensure it is not disclosed to unauthorized individuals. This information shall not be used to make a security or suitability determination until it has been properly interpreted by a medical official trained in the analysis of the specific type of medical condition as specified in the Genetic Information Non-discrimination Act of 2008.

d. The M-40 Personnel Security Office shall ensure that before releasing investigative information to anyone in DOT, the persons to whom the information is being disclosed have an official "need to know." Information released to persons outside DOT shall follow the mandates outlined in the Privacy Act. Any release should only be made in order to carry out a responsibility prescribed by this Order and associated Manual. All persons receiving investigative information shall similarly ensure it is disclosed only to persons who have an official "need to know."

e. All personnel security files (PSFs), reports of personnel investigations, personal history statements, records of response to derogatory information, computerized personnel security data, and other personnel security records and documents shall be regarded as Privacy Act information. During handling, transmission, release, and storage, these materials shall be carefully protected in accordance with all DOT policies and procedures regarding this type of information. The information may not be disclosed except to the extent required by law, or when responding to Freedom of Information Act requests for these types of records.

3. **Release of Personnel Security Records**

a. Upon request, the M-40 Personnel Security Office shall provide an employee the opportunity to review his or her Personnel Security File (PSF). The employee may also, in writing, authorize a representative to review the file. An employee who provides authorization for his or her representative to review the file must provide proof of his or her identity along with the written authorization. Identity may be established by submitting the written authorization to M-40 in person, providing the

employee's notarized signature, or other means the M-40 Personnel Security Office deems satisfactory. M-40 shall complete the following actions when complying with a request for a PSF review:

(1) Review the file before release to the employee or representative, or before sending it to a field facility for review.

(2) Remove any report of investigation completed by another agency, such as OPM, the Defense Security Service (DSS), or the Federal Bureau of Investigation (FBI). If such a report is removed, inform the employee or representative in writing the original PSF contains a report completed by (name of agency), that neither DOT nor an individual DOT administration is authorized to release it directly to the employee or representative, and that the employee should contact the investigating agency directly in order to request a copy.

(3) Remove from the file any other documents, such as identification of a confidential source or information concerning an ongoing investigation, which are exempt from release under the Privacy Act.

(4) Respond to requests from employees who work at field locations distant from M-40. Requests shall be mailed as certified true copies of the PSF to the employee's facility, retaining the original in M-40. Enclose the copy in an envelope addressed to the employee and marked, "TO BE OPENED BY ADDRESSEE ONLY."

(5) For reviews that take place at the security organization, permit the employee or representative to review the PSF only under the direct observation of an Office of Security employee. Provide the employee or representative a reasonable amount of time to review the file and ensure he or she does not remove any documents or pages. Upon request by the employee or their representative, copies of the records to which the person has a right of access under the Privacy Act shall be provided.

b. When responding to requests under the Privacy Act for disclosure of information in PSFs and/or reports of investigation, DOT personnel shall follow all DOT policies implementing the Privacy Act as well as policies of their organization. However, no report of investigation completed by another Federal agency shall be released in response to a Privacy Act request without consent from that agency. Neither DOT nor an individual DOT administration is authorized to release such a report outright, as that is the prerogative of the originating agency. If an employee or representative requests a copy of his or her PSF, and the PSF contains another agency's report of investigation, the employee or representative shall be advised the PSF contains the report, the name of the originating agency, and that DOT is not authorized to release it without the other agency's consent. In the case of an OPM report of investigation, the employee or representative will be told to contact OPM to request a copy.

c. Unless authorized by law, without the concurrence from the M-40 Personnel Security Office, no DOT employee shall enter into any agreement with an individual requiring DOT or any DOT administration or organization to release any personnel security records. Under no circumstances shall an employee enter into any agreement requiring DOT to release a report of investigation completed by another Federal agency.

Chapter III

SUITABILITY, FITNESS AND ELIGIBILITY STANDARDS

1. Relationship Between Suitability, Fitness and Eligibility

a. *Suitability* determination means a decision by OPM or an agency with delegated authority (DOT) that a person is suitable or is not suitable for employment in covered positions in the Federal Government or a specific Federal agency. Suitability for employment refers to identifiable character traits and past conduct which are sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate efficiency and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities. The focus of suitability adjudication is on whether the employment or continued employment of an individual can reasonably be expected to promote the efficiency of the Federal service. Part 731 of title 5 Code of Federal Regulations (C.F.R.), Suitability, contains the criteria to be considered in making suitability determinations.

b. *Fitness* determination is a decision by an agency that an individual 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 a contractor employee.

c. *Eligibility* relates to requirements for an individual occupying a specific position to have access to classified information. An eligibility determination focuses on the question of whether access to such information is clearly consistent with the interests of national security and that the individual has a clear and documented need-to-know. Access to classified information is a privilege, and the decision to entrust an individual with access to classified information is a critical decision the United States Government takes very seriously. EO 12968 expressly directs agencies to keep the number of employees with eligibility for access to classified information to the minimum required to conduct agency functions and expressly prohibits requesting eligibility in excess of actual requirements. Moreover, pursuant to EO 12968, eligibility shall be granted only where facts and circumstances indicate that doing so is clearly consistent with the interests of national security, and all doubts are to be resolved in favor of national security. Section 2 contains the "standard" and "criteria" specified in EO 10450 and EO 12968, which shall be used in making an eligibility determination.

d. While processing applicants for employment, M-40 will make a security determination based upon guidance contained in EO 10450 and/or EO 12968. This determination will usually be made subsequent to a favorable suitability adjudication. A human resources office may favorably adjudicate a background investigation (for

suitability) or information provided by the applicant and find the person suitable for employment in a specific sensitive position, but the M-40 Personnel Security Office must separately determine whether the person should be eligible for access to classified information. In the case of an employee, however, neither suitability adjudication nor an eligibility determination is contingent upon the other.

> **Example** – An eligibility determination may result in reassignment or removal from a position under the provisions of Chapter 12, even if the servicing human resources office has made no suitability determination. Also under those provisions, an eligibility determination that an employee may not be granted a security clearance could prevent promotion or reassignment to a sensitive position.

e. Certain employees may not be subject to a suitability determination by their human resources office, depending on such factors as their status and length of employment. They are, however, subject to disciplinary and removal actions when an investigation develops information warranting such action. Whenever a personnel security investigation develops unfavorable information that could potentially be the basis for disciplinary or removal action, the M-40 Personnel Security Office shall provide human resources and other management officials, as appropriate and on a "need to know" basis, all investigative reports and other information necessary to enable these officials to take appropriate action.

2. Personnel Eligibility Standards and Criteria

a. Eligibility Standard

The granting of access to classified information to any person shall be clearly consistent with the interests of national security and requires that the individual has a clear and documented need-to-know. Eligibility for access to classified information shall be documented in an individual's position description. In making this determination, the adjudicator assesses past and present conduct and considers whether the granting of such access conforms to this standard. Conduct relating to any of the criteria listed below is grounds for denying access to classified information if the conduct indicates the person would pose a risk for damage to national security. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. The M-40 Personnel Security Office shall grant this eligibility only when doing so is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of national security.

b. Criteria

EO 12968 states eligibility for access to classified information shall be granted only to persons whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability,

discretion, and sound judgment; freedom from conflicting allegiances and potential for coercion; and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. EO 10450 enumerates the following criteria which shall be considered in making eligibility determinations:

(1) Any behavior, activities, or associations which tend to show the individual is not reliable or trustworthy.

(2) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(3) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

(4) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case. Discrimination is prohibited under the Genetic Information Non-Discrimination Act of 2008.

(5) Any facts which furnish reason to believe the individual may be subjected to coercion, influence, or pressure which may cause the person to act contrary to the best interests of national security.

(6) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefore, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(7) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interest may be inimical to the interest of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

(8) Advocacy of use of force or violence to overthrow the Government of the United States, or of the alteration of the form of Government of the United States by unconstitutional means.

(9) Knowing membership with specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

(10) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(11) Performing or attempting to perform duties or otherwise acting so as to serve the interest of another government in preference to the interests of the United States.

(12) Refusal by the individual, upon the grounds of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of alleged disloyalty or other misconduct.

c. Restrictions

(1) EO 12968 specifies the following restrictions in applying the security standard and criteria:

(a) In granting access to classified information, there shall be no discrimination on the basis of race, color, religion, sex, national origin, disability, genetic information, age, protected activity or sexual orientation.

(b) In determining eligibility for access, an agency may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. However, no inference concerning the security standard and criteria may be raised solely on the basis of a person's sexual orientation.

(c) No negative inference concerning the security standard and criteria may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standard and criteria are satisfied, and mental health may be considered when it directly relates to those standards.

(2) Federal Investigations Notice 13-02

(a) OPM has revised the Standard Form (SF) 86 instructions at Question 21 in e-QIP as approved by OMB. Effective April 14, 2013, the SF 86 in e-QIP now displays the following additional instructions at Question 21:

> "Victims of sexual assault who have consulted with the health care professional regarding an emotional or mental health condition during this period strictly in relation to the sexual assault are instructed to answer 'No'."

d. Responsibilities and Reporting Requirements

(1) DOT Human Resource Officials and DOT Supervisors

Human resource management officials and all DOT supervisors shall furnish to the M-40 Personnel Security Office any information they receive concerning employees or applicants which may affect that employee or applicant's suitability for employment or their eligibility for holding a security clearance. They must also correctly identify the duties requiring access to classified information and ensure the requirement is included in the Position Descriptions and entered into HR databases.

(2) DOT Employees

(a) Employees who are granted eligibility for access to classified information shall:

(i) Sign an SF 312, Classified Information Nondisclosure Agreement as outlined Chapter XI, 7.b.(1).

(ii) Protect classified information in their custody from unauthorized disclosure.

(iii) Report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information.

(iv) Report all violations of security regulations to the appropriate security officials.

(v) Comply with all security requirements set forth in this Order (DOT Order 1630.2C).

(vi) Complete initial and annual refresher clearance holder training.

(vii) Adhere to all requirements concerning foreign travel (both for business and personal) and related requirements for attendance at international conferences.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with national security.

Chapter IV

RISK LEVEL DESIGNATION AND POSITION SENSITIVITY

1. General Requirements and Definitions

a. All covered DOT positions (covered positions) must be designated as to their level of risk in terms of suitability and access to information technology systems (ITS) and level of sensitivity in terms of national security.

(1) Risk Level Designation

Every position shall be designated at a position risk level commensurate with the public trust responsibilities and attributes of the position as they relate to the efficiency and integrity of the service. The suitability risk levels are ranked according to the degree of adverse impact on the efficiency of the service that an unsuitable person could cause. Every position where the incumbent has access to or is responsible for ITS facilities, systems, or activities must be designated at a risk level commensurate with the responsibilities and other attributes of the position based on the extent to which an incumbent could cause damage to ITS or realize significant personal gain.

(2) Sensitivity Designation

Every position having national security duties must be designated at a national security sensitivity level necessary to ensure appropriate screening under EO 10450. Sensitivity designation is based on an assessment of the degree of damage that an individual occupying a particular position could cause to the national security.

b. OA Human Resource Offices have the authority to designate every covered position at a risk level as determined by the position's potential for adverse impact to the efficiency or integrity of the service. All new position descriptions, or groups of position descriptions, should be coordinated with M-40 before sensitivity levels are designated. Designations may be by class, group, or categories of positions, when appropriate, or may be assigned for an individual position when circumstances warrant.

c. There are three position risk levels. These levels are defined as follows:

(1) Low Risk

Positions which involve duties and responsibilities of limited relation to an agency or program mission having the potential for limited impact on the integrity

and efficiency of the service. This level includes positions which have limited impact on ITS.

(2) Moderate Risk

These are public trust positions which have the potential for moderate to serious impact involving duties of considerable importance to the agency or program mission with significant program responsibilities and delivery of customer services to the public. This level includes positions which have significant program responsibilities which affect large ITS.

(3) High Risk

These are public trust positions which have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority. This level includes positions which have major program responsibilities affecting ITS.

d. Positions at the moderate or high risk levels would normally be designated as "public trust" positions. Such positions 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, and positions involving access to or operation or control of financial records, with a significant risk for causing damage or realizing personal gain.

e. The designation of National Security positions is outlined in Section 3 of EO 10450, as amended, and in Section 732.201 of 5 C.F.R. Each position in the Federal service not designated as Non-Sensitive must be designated as Noncritical-Sensitive, Critical-Sensitive, or Special-Sensitive, depending on the degree to which, by virtue of the nature of the position, the occupant could bring about a material adverse effect on the national security. The nature of the position includes the incumbent's foreseeable need for access to classified information; under EO 12968, eligibility for access to classified information cannot be granted unless such access is clearly consistent with the national security. There are three sensitivity levels for designating positions with regard to national security as follows:

(1) Noncritical-Sensitive (NCS)

Positions with the potential to cause damage to the national security up to and including damage at the significant or serious level. These positions include:

(a) Access to Secret, "L" [Department of Energy (DOE)], or Confidential classified information.

(b) Any other positions with the potential to cause harm to national security to a moderate degree [these positions do not rise to the level of the positions listed in (a) above].

(2) Critical-Sensitive (CS)

Positions with the potential to cause exceptionally grave damage to the national security, including:

(a) Access to Top Secret or "Q" (DOE) classified information.

(b) National security policy-making or policy-determining positions, the duties of which have the potential to cause exceptional or grave damage to the national security.

(c) Investigative duties, the nature of which has the potential to cause exceptional or grave damage to the national security, such as counterintelligence investigations.

(d) The adjudication, recommendation of adjudicative determinations, and/or granting of personnel security clearances.

(e) Duty on personnel security boards.

(f) Any other positions related to national security requiring the same degree of trust.

(3) Special-Sensitive (SS)

Positions with the potential to cause inestimable damage to the national security, including:

(a) Access to Sensitive Compartmented Information (SCI).

(b) Access to any other intelligence-related Special Sensitive information or involvement in Top Secret Special Access Programs (SAP).

(c) Any other position the agency head determines to be at a higher level than Critical-Sensitive due to special requirements that complement EO 10450 and EO 12968.

f. The OA Human Resource Offices shall use OPM's Position Designation System and Automated Tool for Position Designation of National Security and Public Trust Positions to ensure DOT designates positions uniformly and consistently. The tool is available on the OPM Web site at www.opm.gov/investigate. The use of this tool is

required for all positions in the competitive service, positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service and career appointments in the Senior Executive Service (SES). The M-40 Personnel Security Office shall use the national security criteria for determining sensitivity levels in conjunction with the HR risk level designation process to ensure proper designation of national security positions.

(1) All positions requiring access to classified information are sensitive positions and shall be designated at one of the three sensitivity levels.

(2) In many cases, particularly at the Low Risk level, position risk is relatively clear and it may not be necessary to apply all of the specific designating procedures. Similarly, essentially identical positions may require only occasional case-by-case analysis. Even when risk levels may appear to be obvious, specific procedures should be applied on at least a random basis to ensure proper designations.

(3) National security positions, particularly those requiring Top Secret or SCI access, can frequently be designated at the appropriate sensitivity level without applying more detailed procedures. However, if the duties and responsibilities of a national security position would warrant designation as a high-risk position, the position must be designated at least Critical-Sensitive, even if the level of access required is no higher than Secret.

g. The human resources organization shall maintain a record of each designation. The record may be maintained electronically in lieu of retaining a hard copy.

h. The following coding of position risk and sensitivity levels is required for Government-wide use on appropriate personnel documents such as the OF 8, Position Description; SF 50, Notification of Personnel Action; and SF-52, Request for Personnel Action. It shall be used to record a position's level in any DOT automated system containing that information.

RISK/SENSITIVITY LEVEL	CODING
High Risk	6
Moderate Risk	5
Special-Sensitive	4
Critical-Sensitive	3
Noncritical-Sensitive	2
Low Risk	1

Chapter V

PERSONNEL SECURITY INVESTIGATION REQUIREMENTS

This Chapter prescribes investigative requirements and procedures for exceptions to those requirements. The position risk or sensitivity level, and in some cases the security clearance required of a person holding the position, governs the type of investigation required.

1. Introduction

a. The following standards are established for investigations to determine eligibility for logical and physical access, suitability for Government employment, eligibility for access to classified information, eligibility to hold a sensitive position, and fitness to perform work for or on behalf of the Government as a contractor employee.

b. The investigative standards in this Chapter supersede previously issued Federal Investigative Standards and take into account the counterintelligence interests of the United States, as appropriate. Counterintelligence, security, and suitability concerns share a common protective purpose but are functionally distinct; when integrated, all three support prudent decision-making in the interest of national security and promote the integrity and the efficiency of the Government.

c. For investigations covered by these Standards, Federal agencies may not establish additional investigative requirements that exceed these standards (other than requirements for the conduct of a polygraph examination consistent with law, directive, or regulation) without the approval of the Suitability and/or Security Executive Agent, as stated in EO 13467. The Executive Agents shall ensure any approval to establish additional requirements shall be limited to circumstances where additional requirements are necessary to address significant needs unique to the agency involved or to protect national security and shall ensure investigations conducted under these Standards remain aligned to the extent possible.

2. Investigative Tiers

a. There are five investigative tiers:

(1) Tier 1

Investigations conducted to this standard are for positions designated as low risk, non-sensitive, and for physical and/or logical access, pursuant to Federal Information Processing Standards Publication 201 and HSPD-12, using SF 85, or its successor form.

(2) Tier 2

Investigations conducted to this standard are for non-sensitive positions designated as moderate risk public trust, using SF 85P, or its successor form.

(3) Tier 3

Investigations conducted to this standard are for positions designated as noncritical sensitive, and/or requiring eligibility for DOE "L" access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information, using SF 86, or its successor form.

(4) Tier 4

Investigations conducted to this standard are for non-sensitive positions designated as high risk public trust, using SF 85P, or its successor form.

(5) Tier 5

Investigations conducted to this standard are for positions designated as critical sensitive, special sensitive, and/or requiring eligibility for "Q" access or access to Top Secret or SCI, using SF 86, or its successor form.

b. Each successively higher tier of investigation shall build upon, but not duplicate, those lower tiers.

3. Reciprocity of Investigations

a. Requesting agencies shall conduct appropriate checks of indices and databases to validate whether there is an existing investigation that meets current needs.

b. Investigations that meet the requirements specified for a given tier shall be reciprocally accepted for that tier and for lower tiers subject to reciprocity guidance issued by the Suitability and/or Security Executive Agents.

c. Employees who change positions and whose new position requires a higher investigative tier shall be subject to the investigative requirements of the higher tier. The exceptions involve those investigative elements conducted in prior investigations, the results of which are not expected to change (e.g., education degree), shall not be repeated in the new investigation. Copies of prior investigative files shall be provided to the requesting investigative agency in a timely manner.

d. When a gaining agency obtains new information that calls into question the employee's suitability for Federal employment, eligibility for a sensitive position, eligibility for

access to classified information, or a fitness determination, a new investigation shall be conducted in accordance with Chapter 8.

4. Investigative Methodology

a. Investigative Coverage

(1) Investigative coverage shall be accomplished by using automation to the greatest extent practicable to collect, verify, corroborate, or ascertain information about the employee, as documented on e-QIP or developed from other sources. Automated Record Checks (ARC) and queries are an acceptable replacement for written inquiries prescribed by EO 10450 where they meet the requirements of each investigative tier. Subject to applicable law and policy, investigations may include publicly available electronic information as it pertains to the employee's behavior and conduct and as it aligns with the applicable adjudicative criteria.

(2) Each interview shall cover all areas of adjudicative concern and be conducted in person. Exceptions to the in-person requirement may only be made in rare or exigent circumstances that shall be documented in the report of the interview. The investigator shall not use the results of a single interview to satisfy multiple investigative components. This does not preclude the investigator from corroborating and addressing any adjudicatively relevant information with any interviewee.

(3) When information is corroborated or verified by a Trusted Information Provider (TIP) or requester as specified in the Continuous Evaluation (CE) program, it shall be documented and incorporated into the employee's Investigative Record. It shall not be repeated as part of subsequent investigations. Investigative Service Providers (ISPs) are not precluded from corroborating and addressing any adjudicatively relevant information. These checks shall be subject to the standards and a system of oversight prescribed by the Security and Suitability Executive Agents. Other checks conducted by these providers may not be incorporated into the investigation without the approval of the Security and/or Suitability Executive Agents, as appropriate.

(4) Information validated in a prior investigation, the results of which are not expected to change (e.g., verification of education degree), shall not be repeated as part of subsequent investigations.

(5) When the investigation does not meet the investigative standards for that tier, the ISP will document in the report of investigation the lack of coverage or response and attempts to obtain investigative coverage.

(6) The timeframe for the investigative components specified in these standards shall be followed, except when doing so extends coverage prior to the employee's 18th birthday. Investigative coverage may extend prior to the employee's 18th birthday only when necessary to obtain a minimum of 2 years of coverage. This does not, however, preclude reporting information that pertains to the employee's behavior and

conduct prior to his or her 18th birthday, such as information reported by a reference or a lawfully-accessed juvenile record.

b. Acceptable Documentation for Citizenship/Legal Status

All documents evidencing U.S. citizenship or the legal status of non-U.S. citizens shall be the original or certified copies of the original documents. The ISP may use the information from these documents as an authoritative source to verify U.S. citizenship or legal status. This information shall be collected on a consistent basis for all applicants.

(1) One or more of the following documents, or their successors, are acceptable documents to corroborate U.S. citizenship by birth, including by birth abroad to a U.S. citizen:

(a) A birth certificate certified with the registrar's signature, which bears the raised, embossed, impressed, or multicolored seal of the registrar's office.

(b) A current or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.

(c) A Department of State Form FS-240, Consular Report of Birth Abroad of a Citizen of the United States of America.

(d) A Department of State Form FS-545 or DS-1350, Certification of Report of Birth.

(2) One or more of the following documents, or their successors, shall be used to corroborate U.S. citizenship by certification, naturalization, or birth abroad to a U.S. citizen:

(a) A U.S. Citizenship and Immigration Services (USCIS) Form N-560 or N-561, Certificate of U.S. Citizenship.

(b) A USCIS Form 550, 551 or 570, Naturalization Certificate.

(c) A valid or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.

(3) One or more of the following documents, or their successors, shall be used to corroborate legal status:

(a) A current USCIS Form 1-551, Permanent Resident Card or Resident Alien Card.

(b) A Form 1-94 Departure Record with an acceptable visa that authorizes employment in the United States.

(c) A valid USCIS Form 1-766, Employment Authorization Card.

(d) A valid U.S. Travel Document issued as a Permit to Re-enter the United States,

Form 1-327, or as a Refugee Travel Document, Form 1-571.

c. Fingerprint Collection

Digital fingerprints shall be used to the greatest extent practicable. Fingerprints shall be submitted in accordance with FBI requirements. If after two submissions the fingerprints are determined to be unclassifiable, the employee's name and unclassifiable fingerprint results will be submitted to the FBI's "Name Check Bureau." The name check process could take up to 3 weeks to process.

d. Overseas Investigations

(1) Host nation laws generally restrict the level of investigation that can reasonably be performed internationally. Additionally, certain investigative activities (e.g., residence checks, local agency checks) may result in unwelcome attention to the subject of an investigation.

(2) To the extent practicable and warranted by the investigative findings, investigative standards should be met through use of the best sources and records located within the United States or located within U.S. facilities or installations overseas. Unfavorable information, discrepancies, information of security or suitability significance, or significant time period gaps might be cause for tailored international coverage.

(3) If the investigation requires a subject interview and the subject is outside the United States, the interview shall be conducted in person, except under very limited circumstances, such as the subject's deployment to a remote location or to a war zone; the subject may be interviewed via secure communications.

5. Investigative Requirements

a. Tier 1 Investigation

(1) Purpose

Investigations conducted to this standard are for positions designated as low risk, non-sensitive, and for physical and logical access. ARC will be used to the greatest extent possible.

b. Tier 2 Investigation

(1) Purpose

Investigations conducted to this standard are for positions designated as moderate risk public trust.

(2) Reinvestigation

(a) Frequency

Employees in Tier 2 positions shall be reinvestigated at least once every 5 years and as event-driven, subject to OPM implementing guidance.

(b) Validate Need

The requesting agency shall validate that the employee continues to occupy a moderate risk public trust position before initiating a reinvestigation.

ARC must be used to the greatest extent practicable.

(3) Optional Enhanced Subject Interview (ESI)

Due to an agency's suitability or fitness requirements, an agency head or designee may elect to require an ESI as part of the Tier 2 reinvestigation.

c. Tier 3 Investigation

(1) Purpose

Investigations conducted to this standard are for positions designated as noncritical sensitive, military accessions, and/or requiring eligibility for DOE "L" access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information or assignment to a sensitive position.

(2) Reinvestigation

(a) Frequency

Employees occupying Tier 3 positions, as defined in Section 5, Investigative Requirements, paragraph c.1, shall be reinvestigated such that 100 percent of the investigations for the Tier 3 positions are conducted at least once every 5 years and are event-driven, subject to implementing guidance. These reinvestigations shall include a percentage selected by random sampling. Successful completion of a reinvestigation allows the agency to reset the cycle for the employee's next reinvestigation. Those sampled remain eligible for a future random reinvestigation.

(3) Validate Need

The requesting agency shall confirm that the employee requires continued eligibility for a sensitive position and/or eligibility for access to classified information before initiating the reinvestigation.

ARC must be used to the greatest extent practicable.

d. Tier 4 Investigation

(1) Purpose

Investigations conducted to this standard are for positions solely designated as high risk public trust.

(2) Reinvestigation

(a) Frequency

Employees occupying Tier 4 positions, as defined in Section 5, Investigative Requirements, paragraph d (1), shall be subject to reinvestigation at least every 5 years and as event-driven, subject to implementing guidance.

(b) The requesting agency shall validate that the employee continues to occupy a high risk public trust position before initiating the reinvestigation.

ARC must be used to the greatest extent practicable.

e. Tier 5 Investigation

(1) Purpose.

Investigations conducted to this standard are for positions designated as critical-sensitive, special-sensitive, and/or requiring eligibility for DOE "Q" access or access to Top Secret or SCI.

ARC shall be used to the greatest extent practicable.

(2) Reinvestigation

(a) Frequency

Employees occupying Tier 5 positions as defined in Investigative Requirements, Section 5, paragraph e. (1), shall be subject to reinvestigation at least every 5 years and as event-driven.

(b) Validate Need

The agency shall validate that the employee requires continued eligibility for a sensitive position and/or eligibility for access to classified information before initiating a reinvestigation.

ARC shall be used to the greatest extent practicable.

(3) Continuous Evaluation

Pursuant to guidance prescribed by the Security Executive Agent, employees may be reevaluated on a random or continuous basis between investigative cycles. Each agency will ensure that no fewer than 5 percent of those subject to continuous evaluation are reevaluated on an annual basis.

6. Expandable Focused Investigation

a. General Information

(1) The decision to expand an investigation is generally based on significant derogatory information or discrepancies that are known when the investigation is opened or are developed during the investigation. Issues meeting certain threshold criteria shall be identified for expansion as appropriate to the tier.

(2) Unless otherwise specified, the timeframe for the flags corresponds to the collection on the investigative questionnaire at each tier. Issues previously investigated or adjudicated to the applicable standards do not qualify as a current flag unless there is new information or the issue extends into the current period of investigation.

b. Expansion Criteria

(1) Unless otherwise noted, investigations meeting the flagging thresholds will include the standard investigative expansion for that tier and may be expanded to include tailored investigative coverage to resolve the specific issues for an area of concern.

(2) The expandable focused investigation (EFI) may include a review of pertinent records or initial or follow-up interviews with individuals who can provide relevant information or resolve issues, including but not limited to the employee, cohabitants, relatives, references (social, employment, and neighborhood, as appropriate), psychiatrists, psychologists, other health care professionals, and law enforcement professionals, as appropriate. When appropriate, statements shall be taken from the employee and signed pursuant to 28 U.S.C. § 1746.

(3) When issues or discrepant information is present and the investigation is expanded pursuant to these standards, the investigator shall address and report all pertinent facts and circumstances necessary to fully develop or resolve those issues, and any other issues of concern that may arise during the expansion. Investigators will investigate additional leads as necessary to fully resolve all known and developed issues. As appropriate to the issue or issues, this shall include inquiry into:

(a) The nature, extent, and seriousness of the conduct.

(b) The circumstances surrounding the conduct, to include knowledgeable participation.

(c) The frequency and recency of the conduct.

(d) The employee's age and maturity at the time of the conduct.

(e) The voluntariness of participation.

(f) The presence or absence of rehabilitation and other pertinent behavioral changes.

(g) The motivation for the conduct.

(h) The potential for pressure, coercion, exploitation, or duress.

(i) The likelihood of continuation or recurrence.

(4) When an investigation is expanded for issue resolution, a reference that is knowledgeable about multiple areas of concern and/or specific flagged issues may be used to satisfy more than one EFI expansion requirement. There is no expectation under these circumstances that each area of concern requires additional independent references.

(5) Agencies have the flexibility to request an additional investigation from the ISP for any information necessary to resolve issues in order to render an adjudicative determination.

7. Initiating Investigations

The OA Personnel Security Coordinator and M-40 will initiate all background investigations using OPM's e-QIP. All individuals, on whom DOT is initiating background investigations, including applicants for DOT Federal employee positions, current employees, contractor employees and applicants for contractor positions and other non-Federal personnel, shall submit all required forms through e-QIP. M-40 shall not accept any hard-copy forms that an individual can submit through e-QIP.

8. Pre-Appointment Requirements

Outlined below are the minimum investigative requirements for all positions within DOT:

a. Special-Sensitive Position

A person in a special-sensitive position shall have a completed Tier 5 investigation. The investigation shall be completed, evaluated and favorably adjudicated for both suitability and eligibility before the person is placed in the position. A completed, evaluated and favorably adjudicated Tier 5 investigation is required before a Top Secret clearance may be granted. If the person is required to have access to SCI, a completed, evaluated, and favorably adjudicated Tier 5 investigation is required.

b. Critical-Sensitive Position

A person in a critical-sensitive position shall have a completed Tier 5 investigation. The investigation shall be completed, evaluated, and favorably adjudicated for both suitability and eligibility before the person is placed in the position. If the person will be required to hold a Top Secret clearance, a Tier 5 investigation is required before the final clearance can be granted, however, with M-40's documented approval the person may be placed in the position prior to completion of the Tier 5 investigation. Before giving its approval, M-40 shall review the current e-QIP SF 86 Questionnaire for National Security Positions, resume and a current OF-306 Declaration for Federal Employment and the fingerprint results.

c. Noncritical-Sensitive Position

A person in a noncritical-sensitive position shall have a completed Tier 3 investigation or higher-level investigation. If possible, the investigation should be completed, evaluated, and favorably adjudicated for both suitability and eligibility before the person is placed in the position. However, with M-40's documented approval, the person may be placed in the position prior to completion of the Tier 3 investigation. Before giving its approval, M-40 shall review the current e-QIP Standard Form 86 Questionnaire for National Security Positions, resume, and a current OF-306, Declaration for Federal Employment and the fingerprint results.

d. High Risk Position

A person in a high risk position shall have a completed Tier 4 investigation. If possible, the investigation should be completed, evaluated, and favorably adjudicated before the person is placed in the position. However, M-40 may approve a person's placement in a high-risk position prior to completion of a Tier 4 investigation. At a minimum, M-40 shall have reviewed the Standard Form 85-P Questionnaire for Public Trust Positions, resume, OF-306, and fingerprints, and should have initiated the Tier 4 investigation before onboarding approval.

e. Moderate Risk Position

A person in a moderate risk position shall have a completed Tier 2 investigation or higher level investigation. If possible, the investigation should be completed, evaluated, and favorably adjudicated before the person is placed in the position. However, M-40 may approve a person's placement in a moderate-risk position prior to completion of the investigation. At a minimum, M-40 shall have reviewed the SF 85-P Questionnaire for Public Trust, resume, OF-306, and fingerprints, to determine approval to onboard.

f. Low Risk Position

A person in a low risk position will have a minimum of a Tier 1 investigation to meet suitability and HSPD-12 requirements. This Tier 1 investigation shall be requested before placement in the position using an SF-85 Questionnaire for Non-Sensitive Position, resume, OF-306, and fingerprints. Once a preliminary risk-based adjudicative determination is made based upon the forms received, the person can enter-on-duty (EOD) and the investigative request is sent to OPM within 14 after the person EODs. The Tier 1 investigation shall be evaluated and adjudicated for suitability and HSPD-12 approval once the investigation is completed by OPM.

g. Periodic Reinvestigations

All periodic reinvestigations will be initiated in e-QIP for all Moderate and High Risk positions as well as all National Security Positions within 5 years of the previous investigation.

h. Break in Service or Break in Access

The investigation required for a position shall be conducted on any former Federal employee who has had a break in service in excess of 24 months. If the person has had no break in service in excess of 24 months, no new investigation is required unless a periodic reinvestigation requirement applies.

9. Exceptions to Investigative Requirements

a. Exempt Positions

(1) Certain low risk positions are exempt from the investigative requirements. This exception shall not be viewed as a prohibition from processing the person under the normal investigative requirements. Persons appointed without investigation shall not have access to classified information or to restricted areas. In accordance with DOT Order 1681.2, Personal Identity Verification (PIV) Card Program, issuing offices will issue non-PIV cards to other categories of personnel who would otherwise meet the criteria for DOT identification cards but who do not require access to other Federal facilities on behalf of DOT and who do not need logical access.

(2) Fingerprint collection will be in accordance with Paragraph 4c., above.

(3) The categories of exempt positions may include, but are not limited to:

(a) Intermittent, seasonal, per diem, or temporary, in which a person's employment does not exceed an aggregate of 6 months in either a single continuous appointment or series of appointments.

(b) Employees and contractor employees of the landlords of leased facilities which include:

(i) Custodial and maintenance personnel

(ii) Cafeteria and snack bar workers

(iii) Credit union personnel

(iv) Child care workers, volunteers, and parents of children receiving care at DOT facilities. The Crime Control Act of 1990 requires a background check for Federal Government employees who work in Federal child care programs. The law requires that the checks be based on fingerprints and that the checks are conducted through the FBI and each State's criminal history records for which an employee lists current or former residence.

(v) Members of carpools using DOT parking facilities

(vi) Visitors

(c) Positions located outside the United States which are occupied by persons who are not U.S. citizens.

b. Detailed Positions

Individuals occupying permanent positions who are detailed formally or informally into critical-sensitive, noncritical-sensitive, high risk, or moderate risk positions must meet the normal investigative requirements prior to the detail if the detail is to be in excess of 120 days. If access to classified information is required, the person must have the investigation required for the clearance, or M-40 must be able to grant a temporary clearance under the provisions of Chapter 11, Section 6. If the detail is to a critical-sensitive, or high risk position and will be less than 120 days, M-40 shall review the prior investigation, eOPF, Personnel Security File, and the current e-QIP forms SF-86 or SF-85P, Questionnaire for Public Trust Positions, and SF-85 P-S, Supplemental Questionnaire for Selected Positions, as applicable. If a detail originally scheduled for 120 days or less is unexpectedly extended for another period of 120 days or less, the individual may continue in the position without meeting the normal investigative

requirements. However, no person may be continued in a series of details in excess of 240 days unless the required investigation is in progress and M-40 has granted temporary eligibility access to classified information.

10. Special Circumstances for Granting Temporary Eligibility for Access to Classified Information

EO 12968 specifies 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. M-40 shall be responsible for granting such requests. When such eligibility is granted, the initial investigation shall be expedited. Refer to Chapter 11 for additional information.

11. Financial and Foreign Travel Disclosure Requirements

a. The Director, M-40, may designate positions or categories of positions within DOT that require the incumbents to provide financial disclosure statements and relevant foreign travel information as necessary to comply with Section 1.3 of EO 12968. Disclosed statements or information would be consistent with the requirements specified by the Security Executive Agent.

b. Before obtaining a report from a credit reporting agency concerning an individual, or initiating any investigation that will include obtaining such a report, M-40 shall provide the individual written notice that a credit report may be used for employment purposes and shall obtain written authorization from the individual to obtain the report. As required by 15 U.S.C. § 1681b, this notice and authorization shall be in a document consisting solely of the notice and authorization. Organizations may use DOT Form 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act, or a comparable form to meet this requirement.

12. Investigative Requirements for Non-Federal Personnel

a. Chapter 6 of this Manual, Investigative Requirements for Contractor Employees, contains the investigative requirements for DOT contractor personnel who do not need access to classified information.

b. Established in EO 12829, the National Industrial Security Program (NISP) is a partnership between the Federal Government and private industry to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. An important component of the NISP is the National Industrial Security Program Operating Manual ("Manual"), which prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD),

Formerly Restricted Data (FRD), intelligence sources and methods information, SCI, and SAP information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. The procedures apply whenever contractors, contractor employees, consultants, or other persons performing work for or under the direction of DOT require access to classified information in order to perform their duties.

Chapter VI

INVESTIGATIVE REQUIREMENTS FOR CONTRACTOR EMPLOYEES

1. General

This chapter provides policy and procedures for the Personnel Security Program as it relates to DOT contractor employees. It applies to contractor employees who have access to DOT facilities, ITS, Classified National Security Information (CNSI) and/or resources; and other persons who have such access by agreement with a DOT Operating Administration.

2. Background

Many contractor employees are part of the DOT work force or closely support DOT missions. Because of their DOT identification, the extent of their responsibilities, and the risk levels of the positions they occupy, DOT investigates contractor employees and other persons who have such access by agreement with a DOT Operating Administration to determine their fitness for access to DOT facilities, ITS, CNSI, and/or resources.

3. Authority to Investigate Contractor Employees

a. The Department of Justice (DOJ) rendered an opinion on October 1, 1979, that Federal agencies have the authority to screen contractor employees in any reasonable manner and such screening must be consistent with the due process of law. DOJ cited from the U.S.C. three statutory sources of agency authority to investigate and determine the fitness of contractor employees. The following statutes, Executive Orders and DOT Orders are applicable to the authority to perform background investigations of contractors.

(1) 5 U.S.C. § 301

This statute authorizes the head of each executive department to "prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property."

(2) 44 U.S.C. § 3102

This statute requires each Federal agency to provide for "effective controls over the creation and over the maintenance and use of records in the conduct of current business" and in cooperation with the Administrator of the General Services

Administration to "promote the maintenance and security of records deemed appropriate for preservation."

(3) 5 U.S.C. §§ 552a (e) (9) and (10)

This statute requires each agency establish:

(a) Rules of conduct for persons involved in the design, operation, or maintenance of any system of records;

(b) Appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.

The DOJ noted in 5 U.S.C. § 552a, while applicable only to systems of records containing information on individuals, does provide that agencies, consistent with their authority, shall extend the requirements of the section to Government contractors who operate such a system of records to accomplish agency functions.

(4) EO 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information

Executive branch policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to Federally controlled facilities and automated information systems, and eligibility for access to CNSI shall be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation's business and protect national security.

(5) EO 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust

When agencies determine the fitness of individuals to perform work as employees in the excepted service or as contractor employees, prior favorable fitness or suitability determinations should be granted reciprocal recognition, to the extent practicable.

(6) OMB Circular A-130 - Management of Federal Information Resources

Requires Federal agencies to establish personnel security policies for Federal and contractor personnel as needed to ensure an adequate level of security for Federal automated information systems. These policies should include requirements for screening all individuals participating in the design, development, operation, or

maintenance of sensitive applications, as well as those persons having access to sensitive data.

(7) DOT Order 1681.2 - DOT HSPD-12 PIV Card Program

DOT shall issue identification cards meeting the requirements of HSPD-12 and FIPS 201 (and all its successors), identified as Personal Identity Verification (PIV) cards, to its Federal employees and contractor employees who require access to DOT facilities and/or automated information systems.

(8) DOT Order 1631.1 – Granting New Federal and Contractor Employees Access to Department of Transportation Facilities, Resources, and Systems (Agency Access Order)

New Federal or contractor employees will be authorized to enter on duty and/or have access to any automated information system (excluding those available to the general public) only with specific authorization from the Office of Security (M-40), Office of the Secretary.

4. Definition of Sensitive Information

Sensitive information is any information which if subject to unauthorized access, modification, loss, or misuse, could adversely affect the national 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 established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive data at DOT also includes DOT-created, non-public proprietary data (FOUO).

5. Policy

a. M-40, after coordination and consultation with the contracting office, is responsible for adjudicating the fitness of contractor employees.

b. Except as stated in this chapter, the personnel security program requirements and procedures applicable to DOT employees shall also apply to contractor employees who have comparable access to the agency's facilities, ITS, CNSI, or monetary or material resources, including equipment.

c. Notwithstanding the following exception and in accordance with Paragraph 10.c. of this chapter, no contractor employee or applicant for contractor employment shall be prevented from having access to DOT facilities, ITS, CNSI, or resources because of information revealed in a background investigation unless DOT has given that person an opportunity to respond to any information used as a basis to deny such access. Exception - In some circumstances, with approval by the Director of Security (M-40),

access can be suspended pending a review of information provided by the affected person.

d. Contracts requiring contractor employees to have access to CNSI shall be prepared and processed according to the procedures of the NISP.

6. Responsibilities

a. DOT Operating Administrations shall :

(1) Ensure contracting officers follow the DOT Acquisition Policy Letter (APL-2012-01) that governs Contractors Personnel Security and Agency Access.

(2) Ensure all proposed solicitations and contracts are reviewed to determine whether contractors or contractor employees will have access to DOT facilities, ITS, CNSI, or resources. When access is specified, the organization shall ensure coordination with M-40 prior to issuance of the solicitation to determine any applicable personnel security investigative requirements. This could include the completion of a Department of Defense (DD) Form 254. These requirements also apply to any proposed agreements with outside parties, other than contractors, that would result in non-DOT personnel having such access.

(3) Whenever a solicitation, contract, or agreement requires investigation of any contractor employees or other persons, ensure the document contains language sufficient to achieve this objective in an orderly and expeditious manner. The document shall also contain language allowing the DOT OA to deny a contractor employee or other person access to DOT facilities, ITS, CNSI, and/or resources if M-40 determines the person is unfit.

(4) Ensure M-40 is notified whenever there is a change in the status of a contract where contractor employees are subject to investigation (i.e., replaced, defaulted, terminated, etc.).

(5) Ensure contractors and contractor employees (including prospective contractor employees) submit to M-40 completed forms and information for each person subject to investigation, as required by the applicable contract.

(6) Ensure that when a prospective contractor employee has a completed background investigation meeting the requirements for the individual's new DOT assignment, OA contracting officials shall notify M-40, through the Personnel Security Coordinator, as soon as possible in order to allow sufficient time to obtain information about the individual's previous investigation. If M-40 finds the

individual does not have an investigation meeting the requirements for the work assignment at DOT, M-40 will instruct the Personnel Security Coordinator to initiate an investigation.

(7) Notify M-40 of any information it receives which raises a question about the fitness of a contractor employee.

(8) Take appropriate action when M-40 determines a contractor employee is unfit for access to DOT facilities, ITS, CNSI, and/or resources. Appropriate action may include excluding the contractor employee from working on any aspect of the DOT contract.

(9) Notify M-40 whenever a contractor employee has completed work under the contract or leaves his or her position with the contractor.

b. M-40 shall:

(1) Determine, in consultation with contracting officers, which contracts require a personnel security investigation of the contractor and/or contractor employees.

(2) Determine the types of investigation to be conducted on specific contractor employees.

(3) Assist contracting officers in developing appropriate language for inclusion in solicitations, contracts, and agreements.

(4) Receive and process forms to initiate required investigations on contractor employees.

(5) Adjudicate the results of personnel security investigations of contractor employees and determine fitness in consultation with contracting officer, contracting officers' representatives (CORs), and other offices on a need-to-know basis.

(6) Provide due process to contractor employees prior to taking any unfavorable action based on the results of an investigation. Due process shall consist of notifying the person of the specific reasons for the proposed action and affording the person an opportunity to respond.

(7) Notify the contracting officer in writing of any contractor employee found unfit for access to DOT facilities, ITS, CNSI, and/or resources and direct action to deny such access.

(8) Direct appropriate action to be taken whenever any information is received which raises a question about a contractor employee's fitness.

(9) Maintain records on contractor employee personnel security investigations and maintain personnel security files, as necessary, on contractor employees.

(10) Provide the contracting officer with all DOT security directives the contractor needs to fulfill security responsibilities under the contract.

7. Designating Position Risk Levels

a. Contractor employee positions shall be designated as Tier 1, Tier 2, or Tier 4. The Program Offices, Contracting Officer and M-40 shall work together to determine appropriate risk designation. M-40 shall have final approval authority over all designations. The policies specified in Chapter 3 shall apply in designating positions in terms of suitability and access to ITS. Program Offices must use the OPM's Position Designation System and Automated Tool for Position Designation of National Security and Public Trust Positions to ensure DOT designates positions uniformly and consistently. The tool is available on the OPM Web site at www.opm.gov/investigate. The organization shall also maintain documentation as to how the risk levels of contractor employee positions were determined.

b. Contractor employee positions may be designated in groups or by category rather than by individual position.

8. Investigative Requirements for Contractor Employees

a. Except as provided below, contractor employees having comparable exposure to DOT facilities, ITS, CNSI, and/or resources shall be subject to the same investigative requirements, based on the risk level of their positions, as DOT employees.

b. Specific requirements and exceptions are as follows:

(1) Low Risk positions

Except as specified below, the minimum investigative requirement for contractor employees in these positions is a Tier 1.

(2) Moderate Risk positions

All contractor employees in these positions shall be subject to a Tier 2 investigation.

(3) High Risk positions

All contractor employees in these positions shall be subject to a Tier 4 investigation.

(4) Temporary positions

Contractor employees in Low Risk positions that are intermittent, seasonal, per diem, or temporary, and who work on a DOT contract for less than 6 months in either a single assignment or a series of assignments, must undergo at least a fingerprint check and complete an OF 306. This requirement does not preclude investigating the person under the normal investigative requirements.

(5) Construction workers

Investigative requirements for construction workers will vary depending on the location and type of construction. In determining whether or not to conduct any investigation of these persons, M-40 should consider those factors and the extent of the contractor employees' access, particularly unescorted access, to DOT facilities, sensitive classified information, and resources. Many of these employees will be exempt as temporary personnel. However, longer-term construction personnel with such access shall have, at a minimum, a fingerprint check.

(6) Delivery personnel and repair technicians

These contractor employees are exempt from any investigative requirement even if they are working under a DOT contract for an extended period of time. However, depending on the extent of their access at a facility, they may require an escort if they have not been investigated.

(7) Contractor personnel requiring access to CNSI

When contractor employees require access to CNSI and the Department of Defense (DoD) has investigated them under the National Industrial Security Program, M-40 is not required to initiate any additional investigation. M-40 shall confirm the clearance of the contractor and that a DD 254 is properly completed.

c. The provisions of Chapter 8, Reciprocity and Standards for Using Previous Investigations, also apply to contractor employees.

9. **Initiating Investigations**

a. The COR has the primary responsibility for ensuring contractor employees complete in e-QIP all forms required for background investigations prior to the employees receiving access to DOT facilities, ITS, CNSI, and/or resources.

b. Specific forms are required to initiate investigations for Tier 1, Tier 2, and Tier 4 investigations:

(1) For Tier 1 investigations, the contractor employee shall be required to submit the FD-258, FBI Fingerprint Chart, OF 306, Declaration for Federal Employment, and via e-QIP, an SF 85, Questionnaire for Non-sensitive Positions.

(2) For Tier 2 and Tier 4 investigations, the contractor employee shall be required to submit the FD-258, FBI Fingerprint Chart, OF 306, Declaration for Federal Employment, and via e-QIP, an SF 85P, Questionnaire for Public Trust Positions.

(3) For any contractor employee position, M-40 requires submission of OF 306, Declaration for Federal Employment, or other form needed to comply with OPM requirements.

c. Because of the sensitive nature of the forms required for investigations and because of Privacy Act requirements, M-40 and the contracting officer should establish procedures for contractor employees to submit any hard-copy forms that might be required (e.g., release forms) directly to M-40 or to the contracting officer for forwarding to M-40. These procedures shall ensure an employee submits the forms directly to DOT in a sealed envelope and neither the employee's supervisor nor other company personnel have access.

d. Each DOT OA shall establish procedures to pay for investigations on contractor employees.

10. Adjudicating Investigations

a. M-40 shall adjudicate all reports of investigation on contractor employees to determine their fitness. In those cases where M-40 believes information developed during the course of an investigation might result in an unfavorable fitness determination, it shall consult with the contracting officer.

b. While adjudicating contractor employee investigations, M-40 shall apply the same standards and criteria used while adjudicating investigations on competitive service applicants and employees, as stated in 5 C.F.R. § 731.

c. Notwithstanding the following exception, before DOT denies a contractor employee access to its facilities, ITS, CNSI, and/or resources, because of information received as the result of investigation, M-40 shall provide the employee due process, which consists of notifying the contractor employee of the information being considered as the basis for denying that access and affording an opportunity to respond to the information prior to making a final determination. Exception - in some circumstances, with approval by the Director of Security (M-40), access can be suspended pending a review of information provided by the affected person. M-40 may provide due process either orally during an interview with the contractor employee, or in writing. In either case, M-40 shall clearly explain the unfavorable information and provide the employee the opportunity to respond. It shall then consider any information the employee has provided before making a final fitness determination. DOT is not required to give the employee any additional opportunity to respond to the decision.

d. When providing due process and adjudicating investigative results, M-40 shall communicate with a contractor employee directly rather than through a supervisor or other contractor official. No DOT employee shall disclose to a contractor, information contained in an investigation on a contractor employee or the specific reason(s) for any fitness determination. Contracting officers shall ensure contractors understand these procedures and the reasons for them.

e. In the case of an unfavorable fitness determination, M-40 shall notify the contracting officer in writing. The contracting officer shall then notify the contractor to remove the employee as otherwise objectionable from performance under the contract, or to take other action as M-40 directs.

> For example, M-40 may deny the person access to DOT facilities but may still allow the contractor employee to work on the DOT contract at another location.

11. Foreign Nationals as Contractor Employees

a. In general, foreign nationals (legally working in the U.S. and in U.S. Territories) may work as DOT contractor employees on unclassified contracts and may have access to DOT facilities and resources under agreements to which DOT is a party. In any situation where the DOT Secretarial Office or OA for which the contracted work is to be done, and/or M-40 determines it is in DOT's best interest to restrict access or work on a contract to United States citizens only, the appropriate contract or other agreement shall specify that restriction. In determining whether or not to apply this restriction in a given situation DOT personnel shall consider the nature and extent of

access. They should also ensure appropriate legal review of any contract clause applying this restriction.

b. The special considerations described below apply for credentialing of non-U.S. nationals.

(1) At U.S.-Based Locations and in U.S. Territories (Other than American Samoa and Commonwealth of the Northern Mariana Islands):

(a) Departments and agencies must verify employment authorization of new Federal employees with the Department of Homeland Security (DHS) in accordance with OMB Memorandum 07-21, Verifying the Employment Eligibility of Federal Employees.

(b) For individuals who are non-U.S. nationals in the United States or U.S. territory for 3 years or more a background investigation (i.e., NACI or equivalent) must be initiated after employment authorization is appropriately verified. Verification is made through E-Verify or immigration status is appropriately verified for those individuals not working for the Federal Government through the USCIS' Systematic Alien Verification for Entitlements (SAVE) system.

(c) For non-U.S. nationals in the U.S. or U.S. territory for less than 3 years, agencies may delay the background investigation until the individual has been in the U.S. or U.S. territory for 3 years. In such cases, an alternative facility access identity credential may be issued at the discretion of the relevant agency official as appropriate based on a risk determination. Before an alternative identity credential may be issued, the individual's employment authorization must be verified and an FBI fingerprint based criminal history must be completed If the agency decides to delay the background investigation, the agency must request an FBI Investigations Files (name check search), a name check against the Terrorist Screening Database, and a USCIS Check against SAVE.

(d) Agencies may also choose to include additional checks as appropriate. Furthermore, agencies may establish a Special Agreement Check (SAC) with OPM for the purpose of conducting the FBI fingerprint based criminal history check and other national agency checks on non-U.S. nationals.

(e) Verification of the legal status conducted through E-Verify or through the USCIS SAVE system must be submitted to the Office of Security, OST M-40

with the 1600.8 or in the Workforce Transformation Tracking System (WTTS).

(2) At Foreign Locations:

(a) Departments and agencies must initiate and ensure the completion of a background investigation before applying the credentialing standards. However, the type of background investigation may vary based on standing reciprocity treaties concerning identity assurance and information exchange that exist between the United States and its Allies or agency agreements with the host country. In most cases OPM will not be able to conduct a NACI, unless the non-U.S. national is or has been residing in the United States.

(b) The background investigation must be consistent with a NACI to the extent possible and include a fingerprint check against the FBI criminal history database, an FBI Investigations Files (name check search), and a name check against the Terrorist Screening Database. Agencies may also choose to include additional checks as appropriate.

(c) As in the United States, for those non-U.S. nationals where a NACI or equivalent cannot be performed, an alternative facility access identity credential may be issued at the discretion of the Department of State Chief of Mission Authority, Department of Defense Installation Commander, and/or other agency official as appropriate based on a risk determination.

(d) Whether at a U.S.-based or foreign location, reciprocity between agencies is not mandatory in the case of alternative identity credentials issued to non-U.S. nationals. Agencies may choose to honor such credentials from other agencies, but that is at their discretion.

12. Records on Contractor Employees

a. Consistent with DOT records retention policies, M-40 shall maintain a record of each investigation conducted on a contractor employee. M-40 may also maintain PSFs on contractor employees when there are reports of investigation or other records warranting retention. These records shall be maintained for as long as the employees are working on a DOT contract. After that time, M-40 shall maintain them for the same length of time as for separated DOT employees. These records will serve as the primary means by which M-40 can determine if a particular contractor employee has been investigated, which is especially important if the employee is assigned to work at DOT in the future or applies for DOT employment.

b. Personnel security records contain sensitive, highly privileged, and in some cases, sensitive information. All DOT personnel shall carefully protect these records in their handling, transmittal, storage, and release. The provisions of Chapter 2 of this Manual also apply to personnel security records on contractor employees.

c. Upon request, M-40 shall provide a contractor employee the opportunity to review any file that M-40 maintains about that contractor employee, to the extent required by the Privacy Act. The employee may also, in writing, authorize a representative to review it. When complying with a request for a file review, M-40 shall follow the same policies as those used in processing Privacy Act requests for files on DOT employees, as specified in Chapter 2.

Chapter VII

INITIAL ACCESS TO DOT FACILITIES, RESOURCES, AND INFORMATION TECHNOLOGY SYSTEMS

1. General

This chapter establishes minimum requirements for the onboarding process and is consistent/compliant with DOT Order 1631.1, Granting New Federal and Contractor Employees Access to Department of Transportation Facilities, Resources and Systems. It applies to new DOT Federal employees and contractor employees as defined in EO 12968. These employees, upon meeting the basic standards of suitability and fitness requirements for Entry-on-Duty (EOD), may be given access to DOT facilities, resources, sensitive information, and ITS.

2. Basic Requirements

a. No DOT organization may allow a new Federal or contractor employee to EOD or have access to any ITS (excluding those available to the general public) without authorization from M-40.

b. Before M-40 may concur with a new employee's or contractor employee's EOD or granting the individual access to an ITS, it must either:

(1) Confirm the prospective employee already has a completed background investigation meeting the requirements for his or her position; or

(2) Complete a preliminary review of documentation the prospective employee has submitted for any background investigation required and favorably adjudicate the results of a criminal history check.

3. Specific Requirements and Procedures

a. General

The following procedures are designed to minimize the risk that OST or the OAs may have with possibly having to remove newly hired Federal employees or contractor employees who are found to be unsuitable for employment after they have begun working at DOT. These procedures will ensure new Federal employees and new contractor employees will be eligible to receive identification cards and access ITS on their EOD date. At the same time, these procedures are designed to avoid imposing

unnecessary hiring delays and delays in contractor assignments as well as reduce additional costs.

b. Conditions for M-40 concurrence with prospective Federal employee or contractor employee EOD are described below.

(1) M-40 must either:

(a) Confirm the prospective Federal employee or contractor employee has a completed background investigation meeting the requirements for their position and find the investigation results to be satisfactory; or

(b) Complete a preliminary review of the documentation the prospective Federal employee or contractor employee has submitted for the required background investigation and favorably adjudicate the results of a criminal history check.

(2) Whenever an investigation is required, the prospective Federal employee or contractor employee must promptly provide information electronically through e-QIP, submit any other documentation required (e.g., release forms), and provide fingerprints for a criminal history check. M-40 will not provide concurrence for the individual to EOD until the prospective employee has submitted all required documentation and M-40 has completed a preliminary review.

(3) In cases where M-40 is able to verify the prospective Federal employee or contractor employee has a completed background investigation meeting the requirements for their position at DOT and no questionable suitability information exists nor an additional investigation is necessary, M-40 will provide concurrence for the individual to EOD.

c. Processing

For all prospective Federal employees and contractor employees, DOT Form 1600.8, Personnel Security Action Request and Notification, must be completed and signed by the Personnel Security Coordinator for the assigned organization in which the individual will be employed. The completed Form 1600.8 will be submitted through WTTS for Federal employees once this process is fully functional. The Personnel Security Coordinator (or other trained person) will contact the individual to begin the process to initiate an investigation or conduct the appropriate check to confirm an existing investigation.

(1) Federal Employees:

Whenever any preliminary review is required and when it is completed, M-40, in consultation with the servicing OAHR office, shall make a determination as to whether the individual appears to meet the basic suitability standards for employment. When there is no information raising suitability issues, M-40 will notify the employing organization's Personnel Security Coordinator that it concurs with the

individual's EOD. Once a favorable determination is made, the HR office may arrange a start date for the new employee.

(2) Contractor Employees:

M-40 will notify the appropriate COR, through the Personnel Security Coordinator, of concurrence or non-concurrence for EOD of a contractor employee.

d. Actions Required of DOT Secretarial Offices and Operating Administrations:

(1) The Personnel Security Coordinator or HR office for OST or an OA must provide the following to M-40 as soon as the organization has selected an individual for a position as a Federal employee and the individual has accepted a tentative offer:

(a) The completed DOT Form 1600.8;

(b) The Declaration for Federal Employment (OF 306);

(c) The e-QIP signature pages; and

(d) The applicant's resume.

The Personnel Security Coordinator must also send to M-40 these same completed forms as soon as it has identified an individual as a prospective contractor employee who will be working at a DOT facility or who requires access to sensitive information, ITS, or other DOT resources.

(2) HR offices and CORs, as applicable, shall work closely with M-40 in advance of a proposed EOD date. Personnel Security Coordinators should serve as the primary liaison among HR offices, hiring managers, contracting officials, prospective Federal/contractor employees, and M-40.

(3) When a Federal employee is transferring to DOT from another Federal agency and may already have a completed background investigation meeting the requirements for the employee's DOT position, the Personnel Security Coordinator or HR office shall use the Central Verification System (CVS) to verify this, and then notify M-40 as soon as possible in order to allow sufficient time to obtain information about the employee's previous investigation. If M-40 finds the employee does not have a completed investigation meeting the requirements for the DOT position, M-40 will instruct the Personnel Security Coordinator to initiate an investigation.

(4) When a prospective contractor employee already has a completed background investigation meeting the requirements for the individual's new DOT assignment, contracting officials shall notify M-40, through the Personnel Security Coordinator, as soon as possible in order to allow sufficient time to obtain information about the individual's previous investigation. If M-40 finds the individual does not have an

(5) investigation meeting the requirements for the work assignment at DOT, M-40 will instruct the Personnel Security Coordinator to initiate an investigation.

(6) DOT Secretarial Offices and OAs shall complete forms and follow the process listed in DOT Order 1631.1, Granting New Federal and Contractor Employees Access to Department of Transportation Facilities, Resources and Systems (Agency Access Order). The Order contains a list of the submissions required by M-40 to process a background investigation on a prospective Federal employee or contractor employee.

(7) Timely personnel security processing will occur when M-40 has received all required information, including electronic submissions, forms, and fingerprints. HR representatives, hiring managers, and contracting officials must stress to prospective Federal employees and contractor employees the importance of providing these items in an expeditious manner and responding promptly to any M-40 requests for additional information.

(8) M-40 cannot continuously monitor every case individually; therefore, it is imperative that HR offices, hiring managers, contracting officials, and Personnel Security Coordinators stay in contact with prospective Federal employees and contractor employees, as appropriate, to ensure they are completing forms, reporting for fingerprinting, and submitting information electronically as required. Failure to comply could result in onboarding delays.

(9) Contracting officials must ensure contracts requiring contractor employees to have access to DOT facilities, sensitive information, resources or ITS contain appropriate clauses to fully implement the provisions of this chapter. As contracts are awarded, DOT Secretarial Offices and OAs shall remind contractors that M-40 must favorably adjudicate the preliminary results of background investigations for their personnel, or confirm they already have completed investigations meeting the requirements of the positions staffed under the contract, before DOT will grant contractor personnel access to DOT facilities, sensitive information, resources, or ITS.

(10) Contractor employees who do not require regular access to a DOT facility and do not need access to sensitive information, ITS, or DOT resources normally do not require an investigation. If these persons visit a DOT facility occasionally, they should be treated as visitors and subject to any escort requirements in effect at the facilities they visit. However, any contractor employee who does need regular access to a facility is subject to investigation and should not be regularly treated as a visitor, even if escorted.

Chapter VIII

RECIPROCITY AND STANDARDS FOR USING PREVIOUS INVESTIGATIONS

1. **General**

The reciprocal recognition of suitability or fitness determinations is intended to simplify and streamline investigative and adjudicative processes where prior determinations are based on equivalent investigations and adjudicative criteria. Reciprocity limits the need to conduct a new fitness determination when an individual moves, without a break in employment, from a position in the Federal Government to an excepted service or contractor position, or from a contractor position to an excepted service position or another contractor employee position.

2. **Standards**

a. Some applicants for DOT employment and some newly hired employees, especially those persons transferring from other Government agencies, will have already been investigated by another Federal department or agency. In accordance with the guidelines specified in EO 13488, M-40 shall use these investigations to reduce the number of investigations which DOT requests from OPM or conducts itself, thereby reducing investigative costs and delays in waiting for investigations to be completed. The following standards for use of these investigations apply:

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

(2) Any investigation conducted by, or for, another Federal agency on a Federal employee/applicant that is of the same or higher risk and scope as the one required is sufficient to meet the investigative requirements if it was conducted within the past 5 years. If that investigation is unavailable, a new, appropriate investigation shall be completed. The investigation is obtained and reviewed in conjunction with pre-employment checks to make a suitability decision for employment in accordance with current adjudicative criteria.

(3) Any investigation conducted by, or for, another Federal agency on a Federal employee/applicant, the scope of which is less than that required for DOT employment, is upgraded to meet the investigative requirements of the position if the investigation was conducted within the past 5 years, or a new investigation shall be initiated.

b. Previously conducted background investigations shall not be duplicated when those investigations meet the scope and standards for the level of a security clearance required. M-40, as the servicing security organization responsible for granting clearances to civilian personnel, is responsible for determining whether such individuals have been previously cleared or investigated by the U.S. Government. Any previously granted security clearance which is based upon a current investigation of a scope that meets or exceeds that necessary for the new clearance shall provide the basis for issuance of a new clearance without further investigation or adjudication. A new clearance granted under this authority does not restart the clock for reinvestigations.

c. Previously conducted investigations and access adjudications shall be mutually and reciprocally accepted by all DOT organizations without requiring additional investigation. This applies unless there has been a break in the individual's Federal employment or military service in excess of 2 years or unless M-40 is aware of unfavorable information about the person that might affect a security adjudication that was unknown at the time of the previous investigation.

d. M-40 shall be alert to any information indicating the applicant may have had a previous investigation. This includes the review of the employment application; the SF-86, Questionnaire for National Security Positions; the SF-85P, Questionnaire for Public Trust Positions; and the SF-85, Questionnaire for Non-sensitive Positions. Such information would include:

   (1) Recent Federal employment.

   (2) Military service, including service with the National Guard or reserves.

   (3) Employment with a Government contractor where the person might have held a security clearance.

   (4) A claim by the person that he or she has had a previous investigation and/or a security clearance.

e. When a previous investigation is readily available, M-40 will review it prior to giving a human resources organization or employing office permission to employ the person in a sensitive (special-sensitive, critical-sensitive, or noncritical-sensitive) position, or before a human resources organization employs a person in a public trust (high risk or moderate risk) position. M-40 will obtain a copy of the investigation for the person's PSF.

f. If a previous investigation is not readily available, M-40 will obtain as much information as possible about the investigation before the person is employed in a sensitive or public trust position. Sources of this information can include a query of CVS, the agency which conducted the investigation, an employing agency security office, or the agency which granted the person a security clearance. M-40 will request a copy of the investigation and review it as soon as possible.

g. An investigation which another Federal agency conducted on a DOT applicant or employee, and which is of the same type and scope as the one required for the DOT position, is sufficient to meet the investigative requirements provided it was conducted within the past 5 years or the applicant or employee has had no break in service in excess of 2 years since the investigation was completed. Except where there is substantial information indicating an individual may not meet the suitability and/or security standards and criteria stated in Chapter 3, such an investigation shall be accepted by DOT. Any higher-level investigation than the one required for the position also meets the requirements.

h. An investigation conducted by a State or local government agency may provide useful information, particularly in determining whether or not to waive a pre-placement investigative requirement. However, such an investigation, regardless of how extensive it is, does not meet investigative requirements for Federal employment.

3. **Obtaining and Reviewing Previous Investigations**

a. Office of Personnel Management (OPM)

(1) OPM owns and operates the CVS in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 IRTPA), 50 U.S.C. § 3341(e). CVS collects and shares data necessary to make reciprocal determinations on existing security clearances, background investigations, and suitability, fitness, and HSPD-12, Personal Identity Verification (PIV), credentialing determinations.

(2) Agencies have the responsibility for practicing reciprocity and will consult CVS to determine if an existing investigation or applicable adjudication exists that can be reciprocally accepted. Agencies have the responsibility of providing data to CVS to enable reciprocity. This requires prompt reports of investigation and adjudication to OPM.

(3) To facilitate reciprocity, CVS shares adjudicative information reported to OPM. Federal Investigative Services revised the reporting template known as the INV

Form 79A "Report of Agency Adjudicative Action on OPM Personnel Investigations" to capture the adjudicative criteria used to make determinations on OPM investigations. The adjudicative information reported by agencies is viewable to adjudicators on the CVS "Adjudication Detail" screen.

b. Department of Defense (DoD)

(1) In January 2009, the Deputy Secretary of Defense directed the transfer of DoD enterprise-wide information technology systems associated with personnel security clearances from the Defense Security Service (DSS) to the Defense Manpower Data Center (DMDC).

(2) The applications that transferred from DSS to DMDC include:

a. The Joint Personnel Adjudication System (JPAS);

b. The Defense Central Index of Investigations (DCII);

c. The Secure Web Fingerprint Transmission (SWFT); and,

d. The Investigative Records Repository (IRR) also referred to as the "Improved" Investigative Records Repository (iIRR).

(3) The program management and operational responsibilities of these four transitioned applications now fall under the Personnel Security/Assurance (PSA) Division, which is a component of the Identity Management Directorate at DMDC.

(4) The DCII System is an automated central index that identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities. DCII is operated and maintained on behalf of the DoD components and office of the Under Secretary of Defense for Intelligence. Access to DCII is normally limited to the DoD and other Federal agencies that have adjudicative, investigative, and/or counterintelligence missions.

(5) Request for reciprocity of clearances with DoD should be directed to the Personnel Security Management Office for Industry (PSMO-I), formerly known as Defense Industrial Security Clearance Office, which has the mission of:

a. Determining the personnel clearance eligibility of employees for access to classified information, foreign or domestic.

b. Maintaining personnel clearance records and furnishing information to authorized activities.

c. Processing security assurances, clearances, and visits involving the United States and foreign countries.

d. Monitoring the contractor's continued eligibility in the NISP.

c. Federal Bureau of Investigation (FBI)

To request a check of the FBI's investigations index and a copy of any report of investigation the FBI might have, M-40 shall prepare an FBI record check request. This request will be faxed or mailed to:

U.S. Department of Justice
Federal Bureau of Investigation, Records Branch
Washington, DC 20535
FAX (540) 868-4996

d. Other Federal agencies

Other Federal agencies have authority, either by law or through agreement with OPM, to conduct their own investigations pursuant to EO 10450. If an applicant or employee has been employed by one of these agencies, or if there is an indication one of them conducted an investigation on the person, M-40 will contact that security office for a check of its files and to obtain a copy of any report the agency might have. If there is any indication a copy of an investigation might be on file, M-40 may request a copy as it would for an OPM investigation. OPM will furnish a copy of another agency's investigation if it has it on file and if it meets current OPM criteria for release.

4. **Exceptions to Reciprocity**

a. When a person who holds sufficient clearances and accesses from his home agency arrives at DOT, Table 1 below will be checked to confirm the clearances and accesses remain valid.
b. Unless any of the responses are "Yes," DOT may not:

- request the individual to complete a new security questionnaire;
- review existing background investigations for the individual;
- review existing security questionnaires for the individual; or
- initiate any new investigative checks.

FOR ACCESS TO COLLATERAL CLASSIFIED INFORMATION	Yes	No	NA
1. Is the existing clearance granted on an interim or temporary basis?			
2. Is the investigation upon which the existing clearance is based more than seven years old for TOP SECRET, ten years old for SECRET, and fifteen years old for CONFIDENTIAL?			
3. Is your activity (i.e., the gaining activity) aware (i.e., **already** in possession) of substantial information indicating that the standards of EO 12968 may not be satisfied?			
FOR SPECIAL ACCESSES (e.g., SCI and SAPs)	Yes	No	NA
4. Is the existing access eligibility determination based upon a waiver or deviation, or is access otherwise subject to conditions?			
5. If applicable, does the individual not satisfy a polygraph requirement imposed by the new program, as approved by the agency head or deputy? Under such circumstances, the completion of an entirely new security questionnaire is not authorized. Rather, only additional – not duplicative – investigative or adjudicative procedures will be completed.			
6. If applicable, does the individual not satisfy a requirement imposed by the new program that does not allow any non-U.S. immediate family, as approved by the agency head or deputy? Under such circumstances, the completion of an entirely new security questionnaire is not authorized. Rather, only additional – not duplicative – investigative or adjudicative procedures will be completed.			
7. If applicable and if approved by OMB, other than for questions 5 and 6 above, does the individual not satisfy an investigative and/or adjudicative criterion that is additional to the standards set forth in EO 12968? Under such circumstances, the completion of an entirely new security questionnaire is not authorized. Rather, only additional – not duplicative – investigative or adjudicative procedures will be completed.			

Table 1: Checklist of Valid Clearances and Accesses

Items 1, 2 and 4 through 6 above can be verified by querying OPM's CVS, DoD's JPAS, or the Intelligence Community's "Scattered Castles" database. If online access to the appropriate database, or if the record is otherwise incomplete, fax an "Inter-Agency Clearance Verification Request" to the appropriate agency.

Chapter IX

ROLE OF M-40 IN SUITABILITY OR FITNESS ADJUDICATION

1. Suitability

Suitability relates to the requirements for fitness or eligibility for employment and refers to identifiable character traits, reputation, trustworthiness, and past conduct that are sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate efficiency and effectiveness. The focus of suitability adjudication is on whether the employment or continued employment of an individual can reasonably be expected to promote the efficiency of the Federal Service.

2. Security Eligibility

Security relates to the requirements that an individual must be reliable, trustworthy, of good conduct and character, and completely loyal to the United States in order to occupy a specific sensitive position and to have access to classified information and sensitive, restricted facilities. A security determination focuses on the question of whether an individual is eligible for access to such information and facilities and is clearly consistent with the interests of national security.

a. Government workers in sensitive positions and/or requiring access or eligibility for access to classified material.

b. National Security authorities include: EO 10450; EO 12968; EO 13467; 5 C.F.R. § 732; and 5 U.S.C. § 7532.

c. The security determination is a discretionary agency responsibility made in addition to and subsequent to the suitability or fitness determination.

3. Fitness

Fitness refers to 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 in a position subject to suitability) or as a contractor employee.

a. Excepted service positions are covered by 5 C.F.R. § 302.

b. Contracts should specify investigative and adjudicative requirements for contract employees.

4. Security Determination

a. A security determination under EO 10450 and/or EO 12968, in the processing of an applicant for employment, is usually made subsequent to favorable suitability adjudication. The Personnel Suitability Adjudicator may favorably adjudicate a background investigation or information the applicant has provided and find the person suitable for employment in a specific sensitive position, but M-40, the servicing security organization, would separately determine whether or not the person should be eligible for access to classified information.

b. A security determination to establish eligibility for access to classified information may result in reassignment, suspension, or removal from a position, even if the servicing human resource organization has made a positive suitability determination. A security determination that an applicant or employee may not be granted a security clearance would prevent hire, promotion, or reassignment to a sensitive position.

5. Suitability Adjudication

a. DOT HR offices are responsible for suitability adjudication for both applicants for employment and employees. Employees not subject to suitability determinations under the provisions of 5 C.F.R. § 731 are subject to disciplinary and removal actions under other authorities. HR offices shall work with employing offices taking these actions. These positions include:

(1) Positions that are intermittent;

(2) Seasonal; and

(3) Per Diem or temporary, not to exceed an aggregate of 180 days per year in either a single continuous appointment or series of appointments.

b. Employment applications and related paperwork, such as an OF 306, Declaration for Federal Employment, may reveal information raising a question about an applicant's suitability for employment. HR shall follow OPM Suitability Adjudication training to resolve issues through Letters of Inquiry or Notice of Proposed Action. HR also has the option of requesting an additional investigation by OPM through a Reimbursable Suitability Investigation (RSI).

c. In many cases, suitability issues will not be evident until the required background investigation is completed or obtained by DOT, either while a person is still an applicant or after being hired. M-40 will receive all investigative reports from OPM and in some cases will receive reports of investigation completed by other agencies.

6. OPM

Upon request of OPM, DOT is required to report the final adjudicative action based on an OPM report of investigation or a file OPM furnishes in response to a check of its CVS.

Chapter X

SECURITY ADJUDICATION
GRANTING ELIGIBILITY FOR ACCESS TO CLASSIFED INFORMATION

1. Security Requirements - General

a. The standard which must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

b. The principal objective of the DOT personnel security adjudicative function is to ensure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior which could have an adverse effect to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

c. Establishing relevance is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility which could, if abused, have unacceptable consequences for the national security.

d. While equity demands optimal uniformity in evaluating individual cases, ensuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts and prior experience in similar cases. All information of record, both favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness, and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

2. Executive Orders

a. EO 10450, Security Requirements for Government Employment, requires an agency make a security determination as to whether the employment of a person in a sensitive position is clearly consistent with the interests of the national security.

b. EO 13526, Classified National Security Information, and EO 12968, Access to Classified Information, require a determination be made concerning whether the person is eligible for access to classified information.

3. OST Office of Security, Personnel Security (PerSec) Office, M-40

a. To ensure uniform application of the requirements of this manual and to ensure DOT personnel security determinations are effected consistent with existing statutes and Executive Orders, M-40 is designated the central adjudication office for DOT (with the exception of FAA). All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this manual shall be reviewed and evaluated by personnel security specialists specifically designated by the Associate Director of the M-40 Personnel Security Office.

b. M-40 is responsible for security adjudication for all employees and applicants for employment (with the exception of FAA) under its jurisdiction. However, it shall not adjudicate cases on its own manager or on any of its personnel directly responsible for administering the personnel security program.

c. M-40 is responsible for adjudicating all pertinent information and making these determinations. Chapter 11, Eligibility for Access to Classified Information, contains more specific criteria and procedures for granting access to classified information. Specific guidelines for determining access to classified information are contained in the Memorandum from the Assistant to the President for National Security Affairs, "Adjudicative Guidelines", dated December 29, 2005.

4. Evaluation of Personnel Security Information

a. The criteria and adjudicative policy to be used in applying the principles above are set forth in the "Adjudicative Guidelines" Memorandum referenced in 3.c. The ultimate consideration in making a favorable personnel security determination is whether such a determination is clearly consistent with the interests of national security and shall be an overall evaluation based on all available information. Such a determination shall include consideration of 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 pressure, coercion, exploitation, or duress; and

(9) The likelihood of continuation or recurrence.

b. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in the Memorandum from the Assistant to the President for National Security Affairs, "Adjudicative Guidelines", dated December 29, 2005. Adjudication policy for access to SCI is contained in Intelligence Community Directive number 704.

5. Special Cases

a. Cases which raise significant questions regarding a person's loyalty to the United States and cases where M-40 concludes a person has been coerced, influenced, or pressured to act contrary to the interests of the national security shall be referred as appropriate, to the Office of Inspector General and concurrently to the FBI.

b. During initial review of any report of investigation or of any information received which raises a security issue, M-40 shall:

(1) Determine if there are any material gaps in coverage of the individual's activities.

(2) Determine if there are any significant discrepancies between activities claimed on investigative request forms and those shown in the report or other information received.

(3) Decide if there is any questionable medical information requiring an opinion of a competent medical authority.

6. Case Adjudication

a. M-40 shall obtain additional information as needed to adjudicate the case. It may request OPM conduct an additional investigation if an OPM report appears to be inconclusive or incomplete, or that it conducts an RSI to resolve an issue in any previous investigation. M-40 may also:

(1) Initiate an inquiry to resolve any issues.

(2) Question an applicant or employee about discrepancies relating to applications or security forms, but it may not allow the person to amend such forms to eliminate discrepancies.

b. M-40 shall assess all issues in question (except loyalty cases) in terms of the sensitivity of the duties and responsibilities of the position and whether any conduct in question indicates employment of the person in a sensitive position and granting eligibility for access to classified information would pose a risk in terms of protecting the national security. Any conduct indicating the person, through individual or collective action or inaction, may impair the security interests of the United States demonstrates a national security risk. The standard and criteria to be used in this assessment are those stated in Chapter 3.

c. M-40 shall give particular attention to any indication of:

(1) Untrustworthiness;

(2) Lack of dependability;

(3) Potential for subornation or blackmail;

(4) Dishonesty;

(5) Loyalty;

(6) Disregard for the law or established authority.

If M-40 believes the granting of a security clearance is not clearly consistent with the interests of the national security, it shall deny the applicant or employee a security clearance following the procedures in Chapter 12. In the case of an employee who already has a clearance, the security organization shall immediately suspend the person's eligibility for access to classified information, if that has not already been done, following the procedures in Chapter 10. It shall then initiate the process for revocation of the clearance, following the procedures in Chapter 12.

d. In the interests of national security, M-40 shall expeditiously adjudicate all cases. The IRTPA mandates all agencies meet timeliness requirements for investigations and adjudications.

e. M-40 shall maintain a record of all security adjudications, to include copies of any forms returned to OPM that document the adjudication.

7. Adverse Security Action

a. When M-40 proposes an adverse security action, it shall maintain, at a minimum, an administrative due process file consisting of the documents mentioned in paragraph 6e and the following:

(1) Copies of all communications sent to the individual.

(2) Copies of all written challenges, replies, or documentation supplied by the individual, to include a written summary of any oral response.

(3) A copy of any report of investigation from OPM, another agency, or a DOT organization.

(4) Copies of any other documents related to the case.

8. Records Retention

a. Records retention shall be in accordance with the standards outlined in the National Archives and Records Administration General Records Schedule 18, Security and Protective Services Records.

(1) Personnel Security Clearance Files:

Defined - Personnel security clearance case files created under OPM procedures and regulations and related indexes shall be maintained by the personnel security office of the employing agency.

(a) These case files document the processing of investigations on Federal employees or applicants for Federal employment, whether or not a security clearance is granted, and other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government facilities or to sensitive data. These files include questionnaires, summaries of reports prepared by the investigating agency, and other records reflecting the processing of the investigation and the status of the clearance, exclusive of copies of investigative reports furnished by the investigating agency.

Case files shall be destroyed upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable. Reference - NC1-GRS-80-1 item 23a.

(b) Investigative reports and related documents furnished to agencies by investigative organizations for use in making security/suitability determinations shall be destroyed in accordance with the investigating agency instructions. Reference - NC1-GRS-80-1 item 23b.

(c) The index to the personnel security case files shall be destroyed with the related case file. Reference - NC1-GRS-80-1 item 23c.

Chapter XI

ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

1. General

The national interest requires certain information be maintained in confidence through a system of classifications in order to protect our citizens, our democratic institutions and our participation within the community of nations. The unauthorized disclosure of information, classified in the national interest, can cause irreparable damage to the national security and loss of human life. Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

a. Access authorizations are certifications granted by M-40 in accordance with provisions of:

(1) EO 13526, Classified National Security Information

(2) EO 12968, Access to Classified Information

Accordingly, persons are found to be sufficiently trustworthy to be granted eligibility for access to classified national security information at specified levels. These authorizations are generally called security clearances and granted on a need-to-know basis. M-40 may grant them for access to classified information at the Confidential, Secret, and Top Secret levels.

(1) "Confidential" shall be 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.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

b. Except as provided in Section 11, M-40 shall grant access only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicate loyalty to the United

States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. In granting eligibility for access to classified information, M-40 shall apply the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, guidelines which the President approved in December 2005 for use throughout the Executive Branch.

c. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States. Any doubt shall be resolved in favor of the national security.

d. In granting eligibility for access to classified information, M-40 shall not discriminate on the bases of race, color, religion, sex, national origin, disability, genetic information, age, protected activity or sexual orientation.

e. Employees shall not normally be granted access to classified information unless they have been determined to be eligible for access based upon a favorable adjudication of an appropriate investigation of their background, have a demonstrated need-to-know, and have signed an approved nondisclosure agreement. In very exceptional circumstances, where official functions must be performed prior to completion of the investigative and adjudicative processes, an interim clearance or temporary access may be granted. At any time during the period individuals are required to have access to classified information, they may be required to undergo a reinvestigation to ascertain whether they continue to meet the requirements for access to classified information.

f. Secretarial Offices and OAs shall notify M-40 whenever an employee is no longer required to have access to classified information.

g. Access authorizations shall be terminated when no longer required.

h. Especially tight controls are imposed in processing Top Secret access authorizations and requests for access to SCI. DOT does not have authority to grant access to SCI, but the Director of the Central Intelligence Agency may grant such access to a DOT employee when necessary for the employee to perform his or her duties.

2. Limitations and Restrictions on Access to Classified Information

a. The level of access approved for an employee shall be limited and shall relate directly to the level of classified information the employee has a need to access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

b. No one will be eligible for access to classified information merely because of Federal service, contracting, license, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of their title, rank, position, or affiliation.

c. The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the operational requirements. A security clearance shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access to classified information and such access can reasonably be prevented. Security clearances should not be issued to:

(1) Persons in non-sensitive positions.

(2) Persons whose regular duties do not require authorized access to classified information.

(3) Persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

(4) Persons whose duties do not require access to classified information.

(5) Persons who can be prevented from accessing classified information by being escorted by cleared personnel.

(6) Food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

(7) Maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

(8) Persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

(9) Perimeter security personnel who do not require access to classified information.

(10) Drivers and chauffeurs.

d. Eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

e. Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need to know that information.

3. Requesting a Security Clearance

a. EO 12968 requires an agency to limit the number of employees it determines are eligible for access to classified information to the minimum required for the conduct of agency functions. Supervisors and managers shall request security clearances for employees only when there is a demonstrated, foreseeable need for access.

b. M-40 shall grant a security clearance only with specific written justification and concurrence from the employee's supervisor or a manager. This request shall specify the reason a clearance is necessary, the level of classified information to which the employee will need access, and whether the employee has this documented in their position description.

c. When requesting an interim clearance, the supervisor or manager shall specify the reason the clearance should be granted before the expected completion date of the required investigation and the consequences of not waiting for the investigation to be completed.

4. Special Circumstances – Interim Eligibility

a. In exceptional circumstances where an employee must perform official functions requiring access to classified information prior to completion of the required investigation, M-40 may grant the employee interim eligibility for access to classified information pending completion of the investigation. EO 12968 refers to access under these circumstances as temporary eligibility for access; but this type of clearance is different from a "One-time" "temporary" clearance addressed in Section 6 of this Chapter. This type of access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of this access. This process shall not be used as a means to place an employee in a sensitive position without the required background investigation.

b. Interim eligibility for access shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted. Upon determining they are needed and justified, M-40 may grant interim clearances for access to Confidential, Secret, and Top Secret information.

c. Any one of the following may serve as the basis for M-40 to grant an interim Secret clearance:

Confirmation of a completed National Agency Check (NAC) which another Government agency used to grant the person a security clearance for employment or for a Government contractor provided that:

(1) Not more than 2 years have elapsed between the date the clearance was last in effect and the beginning date of the person's DOT employment; and

(2) The security organization has confirmed the clearance was not revoked for any reason raising a question about the person's fitness to hold a clearance.

d. M-40 shall not grant an interim clearance without reviewing the SF 86, completing a credit report, and initiating the required investigation.

e. As a matter of practice, M-40 rarely grants interim Top Secret clearances and does so only in exceptional cases. As much of the required investigation as possible shall be completed before this level of interim clearance is requested from M-40. An organization requesting M-40 to grant an interim Top Secret clearance shall include with its request copies of the SF 86 used to initiate the investigation, all available investigative information obtained to date, and any other pertinent information.

The minimum investigative requirements for an interim Top Secret clearance are as follows:

(1) For someone who has already been the subject of a current, favorable investigation, completion and review of the SF 86, including any applicable supporting documentation, and expedited submission of a request for a Tier 5 investigation.

(2) For someone who has not been the subject of a current favorable personnel security investigation of any kind, completion and review of the SF 86, including any applicable supporting documentation, and expedited submission of a request for a Tier 5 investigation. In addition, M-40 shall ensure completion and favorable review of relevant criminal history and investigative records checks at the Federal Bureau of Investigation, and checks of OPM's Central Verification System (CVS). The results of these checks may be obtained through an advance NAC report from OPM pending completion of the Tier 5 investigation. Whenever possible, M-40 should also conduct a credit check or obtain the results of one conducted by OPM.

f. M-40 may grant an interim clearance for a period of not more than 180 days. If the required investigation has not been completed at the end of that time, M-40, after checking on the status of the investigation and the information developed to date, may extend the interim clearance until the investigation and adjudication are complete. A final clearance supersedes an interim clearance.

g. Upon being granted an interim clearance, the employee shall complete and sign the SF 312, Classified Information Nondisclosure Agreement, and receive the appropriate briefing. M-40 shall also notify the employee in writing, as EO 12968 requires, that further access is expressly conditioned on the favorable completion of the investigation and adjudication of its results. M-40 shall immediately terminate an interim clearance if the investigative results do not warrant the granting of a final clearance.

5. Final Clearances

a. M-40 may grant a final clearance when the required investigation has been completed and adjudicated and all other pertinent official records have been reviewed and evaluated. M-40 may grant the clearance when the investigating agency or organization has provided a substantially complete investigation, even though a minor portion is still pending, if in the adjudicator's opinion the completed portion clearly supports a favorable adjudication and the pending information is unlikely to raise a material issue or help to resolve one.

b. The investigative requirements for final clearances are:

(1) Secret - Tier 3 investigation or higher level investigation with no subsequent break in service or access in excess of 2 years.

(2) Top Secret - Tier 5 investigation with no subsequent break in service or access in excess of 2 years. In using a combination of other investigations, the adjudicator must determine that together they provide investigative coverage equivalent to a Tier 5.

6. "One–Time" Access "Temporary" Clearances

Circumstances may arise where an urgent operational or contractual exigency exists for cleared DOT personnel to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for documented, compelling reasons in furtherance of the DOT mission, M-40 may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. The following procedures and conditions shall be followed for granting emergency one-time access to the next higher classification level.

a. Authorization for such one-time access shall be approved by a Senior Executive Service member prior to submission to M-40 for review and approval.

b. M-40 will review a current, signed SF 86 from the individual before granting a temporary clearance.

c. The recipient of the one-time access authorization must be a U.S. citizen, must possess a current DOT security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

d. Such access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

e. The employee to be afforded the higher level access shall have been continuously employed by a DOT Component or a cleared DOT contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees.

f. Pertinent local records for the employee concerned shall be reviewed with favorable results.

g. Fingerprint check and credit check need to be conducted and favorably reviewed.

h. Whenever possible, access shall be confined to a single instance or, at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of M-40 is required. If it is determined the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

i. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be made available under the general supervision of a properly cleared employee. The employee charged with providing such supervision is responsible for:

(1) recording the level of access actually reviewed,

(2) recording the dates the material is accessed, and

(3) retrieving daily the material accessed.

j. Access at the next higher level shall not be authorized for communications security (COMSEC), SCI, North Atlantic Treaty Organization (NATO), or foreign government information.

k. The exercise of this provision shall be used sparingly and repeat use within any 12-month period on behalf of the same individual is prohibited. M-40 shall maintain a record in the Personnel Security Tracking System containing the following data with respect to each such access approved.

l. When an individual is being granted a temporary clearance for access to another agency's classified information, that agency must concur before DOT grants the access. M-40 will take appropriate steps to ensure the other agency concurs with the release of its classified information to an employee with a temporary clearance.

7. Clearance Granting Procedures and Documentation

a. General

(1) The issuance of a national security clearance is a function distinct from that involving the granting of access to classified information. Moreover, the function of determining an individual's eligibility for participation with an SAP, their suitability for assignment to sensitive duties or to duties that require a trustworthiness determination, are also distinct from the granting of access to classified information.

(2) Clearance determinations are made on the merits of the individual case with respect to the employee's suitability for a security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of Chapter 12.

(3) Only M-40 is authorized to grant, deny or revoke personnel security clearances or special access authorizations (other than SCI). Any DOT manager may suspend access for cause when there is information raising a serious question as to the individual's ability or intent to protect classified information, provided the procedures are in compliance with Chapter 12 of this Manual.

(4) All managers and heads of DOT organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this Manual.

b. Basic Procedures

(1) M-40 will make all determinations regarding the granting of security clearances and shall document clearances that are granted. The documentation will include the level and date of clearance, the investigative basis and date of investigation, the sensitivity of the employee's position, and the date of the last update investigation, if applicable. M-40 will contact the employee directly and conduct a security briefing. The employee shall be required to sign the SF 312, Classified Information Nondisclosure Agreement. By signing the SF 312, the individual agrees not to disclose to any unauthorized person any classified information the employee has access to during the time he or she holds a security clearance and at all times thereafter.

(2) A person only needs to sign an SF 312 once regardless of how many times he or she is granted a clearance. M-40 will ensure the employee has received a briefing and has signed the SF 312, and shall then notify the employee's organization in writing—electronic notification is permissible—that he or she has been granted a clearance and will specify the level of clearance granted. M-40 will send the SF

312 to the servicing human resources organization for placement in the employee's eOPF.

(3) A personnel security clearance remains valid until:

a. The individual has separated from DOT employment,

b. The individual has no further official relationship with DOT or other Federal agencies,

c. Official action has been taken to deny, revoke or suspend the clearance or access, or

d. Regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of their duties.

If an individual resumes the original status of a. or b. above, and no single break in the individual's relationship with DOT exists greater than 24 months, and/or the need for regular access to classified information at or below the previous level recurs, then the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

c. Temporary and interim clearances

(1) An employee being granted an interim or temporary clearance is required to sign the SF 312 and receive a security briefing. M-40 will document the clearance in writing to the employee's organization.

(2) Whenever an employee has been granted an interim or temporary clearance, M-40 shall convey that fact to any other agency that considers affording the employee access to its information. M-40 should include this information on any visit request form containing clearance information that it sends to another agency.

d. Security briefings

(1) Security briefings shall be given by M-40 to all persons authorized access to classified information to ensure they fully understand the requirements and procedures for protecting it, the specific hazards that may be expected, what to do if a compromise occurs, and their continued obligations after their clearances are terminated.

(2) A person shall receive a security briefing from M-40 each time he or she is granted a security clearance, unless the employee has already received a briefing within the past year.

8. Security Education

a. Security education is an integral component of an effective security program. The effectiveness of an employee or contractor meeting their security responsibility is proportional to their understanding of the requirements. Thus, an integral part of the DOT security program is the training and education of individuals on their security responsibilities. Moreover, such training and education is essential to the efficient functioning of the DOT personnel security program.

b. M-40 will provide the initial security briefing to cleared employees when they are first granted access to classified information and will provide annual refresher training thereafter.

9. Security Performance Standard for Employees

a. DOT Manual 1640.4E, Classified National Information Security, an adjunct to DOT Order 1640.4E, prescribes the required performance standards for employees whose duties involve the creation, handling, or management of CNSI.

b. Secretarial Officers and Heads of Operating Administrations shall ensure that the performance standards of all employees and contractors whose duties significantly involve the creation, handling, or management of classified information include the management of classified information as a critical element to be evaluated in their ratings.

10. Terminating / Suspending Access Authorizations

a. Administrative termination

M-40 will administratively terminate an employee's security clearance whenever he or she is separated from DOT employment or when duty changes occur which eliminate the need for the clearance. When the latter situation exists, the employee's supervisor shall request termination of the clearance or reduction in the level of clearance, if appropriate. Clearance termination or reduction in level may require reassessment of the sensitivity level of the employee's position or re-designation of the position as non-sensitive.

b. Clearance suspension

(1) Suspension of a clearance, also known as administrative withholding, is appropriate when a significant question of security fitness arises. Suspension is warranted, for example, when the security organization receives information indicating possible gross misconduct, criminal conduct, substance abuse, or a serious breach of integrity.

(2) Clearance suspension is a temporary action and shall be in effect only while a question of security fitness is investigated, while other pertinent information is being obtained and evaluated, or while legal, administrative, or other action is pending that is expected to have a bearing on whether or not the employee can continue to hold a clearance.

(3) The suspension may remain in effect while an employee is participating in a rehabilitation program following determination of substance abuse; or in a rehabilitation program, counseling, or therapy resulting from legal action occurring outside of DOT. M-40 may reinstate the clearance whenever it believes this action is consistent with the interests of national security, even though the employee is still participating in a rehabilitation or similar program. However, M-40 is not required to do so when other DOT offices, such as a medical office, have determined the employee is fit for duty. M-40 will make every effort to complete all investigations expeditiously and obtain information necessary to make a final determination regarding an employee's clearance; and, when appropriate, shall reinstate a suspended clearance as soon as possible. When M-40 determines a clearance should be revoked, it shall promptly begin the procedures outlined in Chapter 12.

(4) When suspending clearances, M-40 will ensure adherence to the clearance suspension procedures specified in Chapter 12.

(5) M-40 will coordinate a clearance suspension with the employee's supervisor. While it is not necessary to inform the employing organization in detail of the reason for a suspension, M-40 will notify the office in writing that the clearance has been suspended and shall ensure the employee is notified. As stated in Chapter 12, a clearance suspension exceeding 10 days requires written notice to the employee.

c. Security Debriefings

All persons vacating a sensitive position must sign the termination portion of an SF 312 or other approved DOT termination form, which constitutes a security debriefing. The official conducting the debriefing shall sign the form as a witness. The completed form shall be returned to M-40, which shall retain it for at least 1 year. This process is not required when an employee transfers to another sensitive position or when a clearance is suspended, but only when employment with a DOT organization ends, a temporary clearance expires, or the individual permanently transfers to non-sensitive duties.

11. Special Access Authorizations

a. General

It is the policy of DOT to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding

established requirements are authorized only when mandated by other authority. For example, there are Special Access Programs originating at the national or international level that require personnel security investigations (PSIs) and procedures of a special nature. These programs and the special investigative requirements imposed by them are described in this section. A Special Access Program is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to Section 4-1 of EO 12958.

b. Department of Energy (DOE)

DOE issues security clearances for access to DOE Restricted Data under the provisions of the Atomic Energy Act of 1954, as amended. DOE Restricted Data relate to the design, manufacture, and use of atomic weapons; the production of special nuclear material; and energy production. Restricted Data are assigned classification levels of Confidential, Secret, and Top Secret similar to the levels of other national security information classified under the provisions of EO 13526, Classified National Security Information.

(1) M-40 has the responsibility to obtain and control the clearances for all DOT organizations.

(2) When a DOT employee needs access to Restricted Data, the employee's management shall request M-40 to arrange for this access. M-40 will request and obtain from the employee any forms DOE requires and follow DOE procedures in processing the request.

(3) The background investigation and reinvestigation requirements for a DOE "Q" clearance are the same as those for a Top Secret clearance. The requirements for DOE "L" clearances are the same as those for Secret and Confidential clearances.

(4) The decision to grant or deny a DOE clearance is solely a DOE responsibility, and denial of a clearance is not subject to review or appeal by DOT. DOE is responsible for affording an employee all due process rights as prescribed by EO 13526 and EO 12968. However, when DOE denies a clearance for a DOT employee, M-40 will review any information that DOE used in making its decision that was not available when M-40 granted the employee's current DOT security clearance. It shall then determine whether or not the employee's continued access to classified information is clearly consistent with the interests of national security.

(5) When DOE grants a Restricted Data clearance, M-40 will notify both the employee and the employee's organization. It is contrary to DOE regulations to provide the employee with written notification of a DOE clearance; therefore, M-40 will provide this notification orally. M-40 will also ensure the employee receives all briefings required by DOE.

(6) M-40 will arrange for termination of a DOE clearance when employees no longer have a need for this clearance to perform their official DOT duties. It shall ensure the employee is debriefed according to DOE procedures.

c. North Atlantic Treaty Organization (NATO)

Access by DOT personnel to NATO-classified information requires special authorization. The Central United States Registry (CUSR) has granted applicable authority to the Maritime Administration's (MARAD) Office of Management and Administration. The MARAD Security Officer is the DOT official responsible for performing requirements concerning NATO access and information. Policy related to NATO information is contained in DOT Order 1642.2/MAO 280-4.

(1) NATO information and material will be protected at the same level as U.S. Classified National Security Information but at an enhanced security level that provides compartmentalization.

(2) A request for authorization for access to NATO classified information shall be initiated by an employee's supervisor or other management official who can attest to the official need. The request shall specify the level of NATO information to which the employee will need access. This information shall be forwarded to the MARAD Security Officer for action. Individuals will be granted access to NATO information and material once:

(a) The individual completes initial NATO specific training to ensure a complete understanding of NATO requirements;

(b) The individual is indoctrinated into NATO by signing the briefing/debriefing acknowledgement form and if;

(c) The individual has a need to know, position requirement, justification, and appropriate security clearance.

(3) A security clearance issued under the provisions of this chapter is a prerequisite for authorizing access to NATO information at the corresponding level. Upon determining an employee may be granted access to NATO information, the MARAD Security Officer will issue a NATO access authorization specifying the level of access and shall notify the employee's office.

(4) When the employee ceases to be employed in a position requiring access to NATO classified information the servicing security organization shall debrief the employee regarding his or her continued responsibility to safeguard the information.

12. Security Clearances and Authorizations for Non-United States Citizens

a. Only U.S. citizens are eligible for a security clearance. Therefore, every effort shall be made to ensure non-U.S. citizens are not employed in duties that may require access to classified information. However, when there are compelling reasons to grant access to classified information to an immigrant or a foreign national in furtherance of a DOT mission, such individuals may be granted a "limited access authorization" (LAA) under the following conditions:

(1) The LAAs will be limited to the Secret and Confidential level only; LAAs for Top Secret are prohibited.

(2) Access to classified information is not inconsistent with that determined releasable by designated disclosure authorities.

(3) Access to classified information must be limited to information relating to a specific program or project.

(4) Favorable completion of a background investigation. Such an authorization may be approved only if the prior 10 years of the person's life can be appropriately investigated. Individuals granted LAAs under the foregoing provisions shall be the subject of a 5-year periodic reinvestigation.

(5) Security clearances previously issued to immigrants will be reissued as LAAs. Immigrants who are eligible for U.S. citizenship and have not tried to become naturalized within 12 months of eligibility will not be considered for an LAA.

(6) The limited access authorization determination shall be made only by the Director of M-40 and may not be further delegated.

(7) The LAAs will be limited to persons who have a special skill or technical expertise essential to the national security that is not available from U.S. personnel. An LAA request will clearly describe the nature of the classified information involved and state the level of classification. The requesting office will clearly show the person's services are of such unique quality and character as to be unobtainable elsewhere; and if his or her services are not obtained, the work cannot proceed or will be seriously impaired to the extent that national security interests will be affected.

(8) LAAs will not be granted to secretarial or clerical personnel or to others who perform routine administrative duties.

(9) Non-citizens shall not be eligible for access to any higher level of classified information than the U.S. Government has determined may be releasable to the country of which the person is currently a citizen.

b. M-40 shall adjudicate the completed investigation and determine whether or not to grant the requested authorization. In granting an LAA, M-40 shall specify both the level and the type or category of classified information to which the non-citizen may have access.

c. In each case of granting a limited access authorization, a record shall be maintained as to:

(1) The identity (including current citizenship) of the individual to whom the limited access authorization is granted, and shall include name and date and place of birth;

(2) Date and type of most recent investigation to include the identity of the investigating agency;

(3) The nature of the specific program material(s) to which access is authorized (delineated as precisely as possible);

(4) The classification level to which access is authorized;

(5) The compelling reasons for granting access to the materials cited in paragraph (3) above; and

(6) Status of the individual (that is, immigrant or foreign national).

CHAPTER XII

ADVERSE SECURITY ACTIONS

1. General

a. This chapter prescribes procedures which DOT personnel shall follow upon receipt of information about an employee or applicant, which may result in an adverse security action. Such actions may include denial, suspension, or revocation of a security clearance for their eligibility for access to classified information.

b. Upon receipt of information that raises questions concerning the personnel security fitness of an individual, M-40 shall immediately assess the security factors involved and shall take suitable action to ensure national security interests are protected. In taking such action, M-40 shall consider such factors as the conclusiveness and seriousness of the information developed, the employee's access to classified information, and the opportunity the position affords the employee to commit acts contrary to national security interests.

c. M-40 may suspend, revoke, or deny a security clearance. The FAA may establish its own procedures for processing adverse security actions, separate from those in this chapter, provided it receives approval from M-40 and appropriate legal counsel, and the FAA procedures are consistent with the provisions of Section 5.2 of EO 12968. Any such procedures shall ensure an individual whose security clearance is being denied or revoked is provided the rights and opportunities stated in Section 5.2 of EO 12968. These opportunities include that of appearing personally and presenting relevant documents, materials, and information at some point in the process before an adjudicative or other authority other than the investigating entity.

d. All individuals whose clearances are denied or revoked, regardless of which DOT organization takes the action, have the right to appeal the denial or revocation to the Personnel Security Review Board (PSRB).

e. The Secretary of Transportation may also exercise authority granted in 5 U.S.C. §7532 to suspend without pay, and then remove, a DOT employee when the Secretary considers the action necessary in the interests of national security.

2. Security Clearance Suspension, Denial or Revocation

a. Suspension

If a decision is made to suspend a security clearance temporarily pending an investigation to determine if revocation of the clearance is warranted and the suspension exceeds 10 days, M-40 will notify the employee in writing that it has

suspended the clearance and provide justification on the suspension to the extent consistent with the interests of national security.

b. Post Suspension

After the security clearance is suspended, but prior to a determination on whether to reinstate or revoke it, the employee's management may, in its sole discretion: restrict the employee to non-sensitive duties of the position, temporarily reassign the employee to a non-sensitive position with the same grade and pay, or place the employee on administrative leave with pay.

c. Denial or Revocation

(1) If M-40 decides to pursue the denial or revocation of a security clearance, it shall notify the individual in writing, to the extent consistent with the interests of national security, that the clearance is being denied or revoked and provide the employee the justification for the action. The explanation for the decision shall be as comprehensive and detailed as permitted by the national security interests of the United States and applicable laws. M-40 shall also notify the individual in writing that:

(a) The individual has 30 days from the date of the notification to submit a written response to M-40 with any supporting documentation and/or to request the opportunity to appear personally before the adjudicative authority.

(b) The individual may request an extension of the response time but must do so in writing to M-40. The granting of any extension is subject M-40's discretion.

(c) The individual has the right to be represented by counsel or other representative at his or her own expense and to request any documents or records of verbal reports upon which the decision is based.

(d) The individual has the right to request from the investigating agency the entire investigative file for any investigation on which the decision is based.

(e) If no timely response is received, the denial or revocation shall be final.

(2) If the employee or applicant submits a timely response, that response and any supporting documentation shall be considered before making a final decision. If the individual asks to appear in person to respond to the denial or revocation decision, the Departmental element whose action is the subject of appeal will be responsible for travel expenses resulting from the appellant's personal appearance.

(3) The appearance shall be before an adjudicative authority other than the investigating entity, and M-40 will allow the individual to present any documents, materials, or other information as part of the response. All such evidence shall be

considered before making a final decision. M-40 will make a written summary or recording of any such personal appearance and place it in the individual's personnel security file. The final decision shall be in writing and, in the case of a denial or revocation, M-40 shall notify the individual that:

(a) He or she may appeal the decision to the PSRB chaired by the Director, Office of Security (M-40).

(b) The review request must be in writing and must be submitted to M-40 within 30 days from the date of the final decision.

d. Final Appeal

(1) Section 5.2(a)(6) of EO 12968 provides each person whose security clearance has been denied or revoked an opportunity to appeal in writing to a high-level panel appointed by the agency head. The Assistant Secretary for Administration has chartered the PSRB to fulfill this requirement.

(2) Whenever any element of the Department has made a final determination denying a person a security clearance for access to classified information or revoking an existing security clearance, that employee (appellant) may appeal the decision to the PSRB by writing to the Chairperson of the Board (Chair), the Director, Office of Security, M-40. All final determinations shall be in accordance with the provisions of EO 12968 and are subject to the review required by Presidential Policy Directive-19 (PPD-19), Protecting Whistleblowers with Access to Classified Information.

(3) The appellant must submit the appeal in writing within 30 calendar days after receiving formal notification of the determination denying or revoking the security clearance.

(4) Once a request has been made for the Board, the Director of Security must respond to appellant acknowledging receipt of request for the Board.

(5) The Chair shall determine whether the matter is ripe for appeal and whether the deadline for filing an appeal has been met. If the matter is not ripe for appeal, the Chair shall return the appeal to the appellant with a written explanation. If the deadline for submitting an appeal has passed, the Chair shall so advise the appellant, in writing, and shall return the appeal to the appellant. The Chair shall also advise the appellant that he or she may petition for a waiver of the deadline.

(6) If the appellant petitions for a waiver of the deadline, and if the Chair concludes the appellant has presented sufficient reason why he/she could not, with due diligence, have met the deadline, the Chair shall accept the appeal as timely filed. If the Chair concludes the appellant could have met the deadline but did not, the appeal shall be rejected. The decision of the Chair under this paragraph is final.

(7) The Board shall be composed of five members, at the minimum grade of GS-15 or equivalent, any three of whom (to include one who is familiar with personnel security adjudicative guidelines) shall constitute a quorum for official action. In accordance with EO 12968, two members of the Board shall be from outside the security field.

(8) The Board acts on behalf of the Secretary, except in any case in which the Secretary personally elects to make the final decision on an appeal. The Board has the authority to direct the granting of a clearance that M-40 or FAA has denied, and to direct the reinstatement of a revoked clearance as if it had never been revoked. Board decisions shall be in writing.

(9) The Board shall be chaired by the Director of M-40, as appointed by the Assistant Secretary for Administration (M-1) and may, with the approval of M-1, establish its own operating procedures.

(10) An appeal to the Board does not stay the decision being appealed. However, no adverse personnel action based on the denial or revocation of a clearance shall be proposed or taken against the affected person prior to the expiration of the 30-day period in which he or she may appeal the denial or revocation and until any appeal is decided by the Board.

e. Whistleblower Reprisals

(1) In accordance with PPD-19, retaliation that affects eligibility for access to classified national security information is prohibited.

(2) Any officer or employee of an executive branch agency who has authority to take, direct others to take, recommend, or approve any action affecting an employee's eligibility for access to classified national security information shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, any action affecting an employee's eligibility for access to classified national security information as a reprisal for a protected disclosure.

(3) The Department will not tolerate whistleblower reprisal. Any employee who believes he/she is the target of reprisal due to his/her whistleblower actions, may, at any time, report this concern to the DOT Office of Inspector General (OIG), the U.S. Office of Special Counsel (OSC), and appropriate management officials.

(4) If an employee appeals a clearance decision and alleges the revocation or denial of their clearance is a reprisal for whistleblowing, prior to consideration of the appeal by the PSRB, the allegation of whistleblower reprisal in violation of PPD-19 shall be reviewed by the DOT OIG. The DOT OIG may initiate its own investigation expeditiously or review the fully developed record from DOT's established administrative procedures for review of security clearance determinations.

(5) Upon a finding by the DOT OIG that there is no violation of the whistleblower provisions as specified in PPD-19, the PSRB shall proceed with its review of the appeal.

(6) Upon a finding by the DOT OIG that an action affecting eligibility for access to classified national security information violated whistleblower protections as defined in PPD-19, the DOT OIG may recommend that the Department reconsider the employee's eligibility for access to classified national security information and take other corrective actions to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred.

(7) An employee who has exhausted the applicable review process required by Section B of PPD-19 may request an external review by the Inspector General of the Intelligence Community. This review shall be in accordance with the guidelines contained in PPD-19 and should be completed within 180 days.

(8) If an employee alleging reprisal due to whistleblower activities chooses to file an appeal with the OSC, the DOT Office of General Counsel (C) shall be designated as the Departmental Liaison responding to any requests from the OSC for matters involving OST. The Chief Counsel's Office of the relevant OA shall be designated as the Departmental Liaison responding to any requests from the OSC for matters involving an OA. The Director, Office of Security, shall await a conclusion from the OSC appeal process prior to accepting the employee's appeal for review by the PSRB.

f. Post Denial or Revocation

(1) After the procedures outlined in the PSRB Charter have been completed and a security clearance has been revoked, M-40 will provide the servicing human resources organization and/or the employing organization office all information necessary to take appropriate action under applicable personnel authority and regulations. Such action may include removing the employee or permanently reassigning the employee to a non-sensitive position.

(2) After the procedures outlined in the PSRB have been completed and a security clearance has been denied:

(a) If the individual denied a clearance is an applicant for appointment to a position for which a clearance is required, the person shall not be appointed to that position.

(b) If the individual denied a clearance is an employee occupying a non-sensitive position that has been selected for a position requiring a clearance, appointment or reassignment to that position shall not be made.

3. Employment of Individuals Previously Separated for Security Reasons

No person who has been separated from employment with any department or agency of the U.S. Government under any Federal security program (such as 5 U.S.C. §§ 7531-33, EO 9835, or EO 10450) may be employed in DOT without prior approval of the Secretary and determination by the servicing human resources organization that the factors leading to the separation are not currently disqualifying for DOT employment. When employment of such a person is proposed, M-40 will obtain complete information regarding the basis for the separation, ensure appropriate investigation of the person's subsequent activities, ascertain whether the human resources organization has determined the person is eligible for DOT employment, and obtain any other information the Secretary needs to decide whether or not the person's employment is clearly consistent with the interests of national security. If additional investigation is required, M-40 will make such request from OPM.

CHAPTER XIII

FOREIGN ASSIGNMENTS AND TRAVEL

1. General

Special safeguards are required to protect the national interest and national security information when DOT personnel and representatives are given foreign assignments or perform official foreign travel. For this purpose, a "foreign" location means outside the 50 States, the District of Columbia, Puerto Rico, or any of the United States possessions, territories, or trust territories. The investigative requirements and security precautions specified in this chapter apply to employees on foreign assignments or travel. DOT personnel assigned official travel in a foreign country must exercise good judgment at all times to ensure they do nothing contrary to the interests of the United States or DOT. Officials authorizing the travel are responsible for ensuring each traveler possesses the good character and reliability needed for the assignment.

2. Investigative and Clearance Requirements

a. Foreign assignments

(1) A DOT employee serving in a foreign duty location will normally be assigned to the U.S. diplomatic or consular mission in the country of residence. To comply with Department of State (DOS) regulations, all employees assigned to a mission through permanent change of station must hold at least a Secret clearance.

(2) All foreign positions shall be designated at least noncritical sensitive. Personnel elected for these positions shall have a completed and favorably adjudicated investigation commensurate with their assignment prior to reporting to their foreign location.

(3) When an employee is being assigned to a foreign duty location, M-40 will transmit the security clearance data to the appropriate DOS regional security officer (RSO) or post security officer (PSO). M-40 may do so either by electronic message directly to the RSO or PSO or by providing the data to the Bureau of Diplomatic Security, Department of State, for transmission to the post.

b. Personal service contract (PSC) personnel

U.S. citizens who are family members of U.S. personnel stationed in foreign countries, and who are technically PSC employees under arrangements made through DOS, are not required to hold security clearances if their employment will not require them to have access to classified information or to sensitive areas at locations which

receive, process, or store classified or other foreign policy or operationally sensitive information or material. A Tier 1 Investigation is the minimum required investigation for these positions. M-40 is responsible for granting any security clearances necessary for persons in these positions.

c. Temporary duty (TDY)

(1) If an employee is to be on TDY intermittently or continuously to a foreign location for more than 120 days in a calendar year, a completed Tier 3 Investigation is required prior to beginning the travel.

(2) For all other TDY assignments, there are no special investigative requirements other than those applicable to the risk or sensitivity level of the employee's position.

(3) There is no requirement that an employee on TDY to a foreign location have a security clearance. While there is no specific clearance requirement to visit DOT offices located in foreign countries, provided access to classified information is not required, an employee requiring access to an office located in an embassy or embassy annex must be escorted if he or she does not have a favorably adjudicated Tier 3 Investigation granting eligibility for access to classified information at the Secret level.

(4) When an employee is scheduled for TDY to a foreign location, the organization where the employee works should determine whether or not a clearance will be required for the work the employee will be doing and/or to avoid major inconvenience due to lack of unescorted access to particular Government agency offices. In making this determination, the office should consider such factors as the nature of work to be performed; the extent, nature, and location of contacts with DOT and other Government officials; and the length of the TDY. In many cases, not being allowed unescorted access for one visit to an office or embassy in a foreign location will cause an employee no significant inconvenience.

(5) When an office determines that clearance information should be provided to DOS for an employee scheduled for TDY, it shall contact M-40 as far in advance of the trip as possible. DOS requires that the level of clearance be stated in the travel message and on the travel authorization. However, no such information shall appear on any message or travel authorization without coordination with M-40.

(6) If an employee scheduled for TDY needs a security clearance and does not have one, the operating office shall complete form DOT F 1600.8 and submit this to M-40 requesting a temporary clearance. The request shall state the period of time for which the clearance is needed, the location(s) to be visited, and specifically why the clearance is necessary.

(7) M-40 will transmit clearance data for employees going on TDY, as necessary, as stated in Section 2, Investigative and Clearance Requirements, paragraph a. (3) above.

d. International conferences

(1) Head of a delegation

Any DOT employee selected to head a delegation from the United States to an international conference on other than a one-time basis shall be subject to a minimum Tier 3 Investigation.

(2) Nominee as DOT representative at an international conference

Nomination to represent DOT at an international conference is subject to completion of a Tier 1 or higher level investigation. This investigation has normally been conducted on Federal employees but not necessarily on technical advisors or other representatives from industry. If an advisor from industry is selected to help represent DOT at an international conference, the DOT office arranging for the advisor's services shall contact M-40 at least 3 weeks prior to the date the delegation is scheduled to depart. M-40 will determine if a Tier 1 Investigation has been conducted on the industry representative, as may be the case, for example, if the person holds a Government security clearance or is a military reservist. If a Tier 1 Investigation has not been completed, M-40 will initiate in e-QIP for the person to complete the investigative forms. The employing office will ensure the forms are expeditiously completed and returned to M-40, which shall then process the Tier 1 Investigation. A Tier 1 Investigation for this purpose need not include a completed fingerprint check prior to the delegation's departure.

e. Special requirements

Visits to some activities at foreign locations require special security authorizations or clearances. For example, to attend a meeting at NATO headquarters in Brussels, Belgium, NATO requires a person to have a NATO clearance. An office arranging for a DOT employee to visit NATO headquarters or a similar activity shall ensure in advance that it coordinates with M-40 for any special clearance(s) required. A request for a NATO clearance will be made with the MARAD Security Officer. Requesting offices should ask about clearance requirements when making visit arrangements and provide its request to M-40 and/or MARAD at least 3 weeks in advance of the visit to allow time for processing.

APPENDIX 1

DEFINITIONS

Access: In general, the ability to enter and/or pass through an area or a facility, or the ability or authority to obtain information or monetary or material resources. As related to classified national security information - the ability, authority, and/or opportunity to obtain knowledge of such information.

Access authorization: Certification a person is currently authorized to have access to classified national security information at specific levels.

Appointing/Approving Official: The individual delegated the authority to effect appointments, reassignments, promotions, separations, or similar personnel actions regarding DOT employees, contractors or applicants.

Automated Record Checks (ARC): A method for requesting, collecting, and validating electronically accessible and adjudicated relevant data using the most efficient and cost-effective technology and means available.

Background Investigation (BI): Any personnel investigation conducted to meet personnel security program requirements. An investigation consisting of a National Agency Check (NAC), credit search, personal interviews of subject and sources, written inquiries, and record searches covering specific areas of a person's background during the most recent 5 years, and additional record searches during the most recent 7 years.

Central Verification System (CVS): OPM's online computer database of investigations and clearances. CVS is designated as the primary tool for facilitating reciprocal decisions, as required by Executive Orders, regulations and policies.

Classified National Security Information (CNSI): Official information or material that requires protection in the interest of national security and is classified for such purpose by appropriate classification authority in accordance with the provisions of Executive Order 12968, Classified National Security Information.

Cohabitant: An individual with whom the subject lives, other than a spouse, child, or other relative (mother, father, brother, sister, in-laws, etc.), with whom a bond of affection, influence, obligation, or a spouse-like relationship exists.

Contract: As defined in Federal Acquisition Regulation 2.101, a mutually binding legal relationship that obligates the seller to furnish supplies or services (including construction) and the buyer to pay for them. This includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing.

Continuous Evaluation (CE): Review of the background of an individual at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility.

Contracting Officer (CO): As defined in Federal Acquisition Regulation 2.101, a person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer.

Contracting Officer Representative (COR): Contracting officer representatives (COR) are qualified individuals appointed by the Contracting Officer (CO) to assist in the technical monitoring or administration of a contract.

Contractor Employee: A person hired by a contractor as an employee or subcontractor to perform tasks under a DOT contract. This term includes any consultant to DOT who is not a Federal employee.

Covered Positions: As defined in 5 C.F.R. § 731, means a position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service.

Counterintelligence (CI): Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

DOT Employee: Any person employed directly by DOT. "Employee" (defined in EO 12968) means a person, other than the President and Vice President, employed by, detailed to or assigned to an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

Electronic Official Personnel Folder (eOPF): The eOPF is an electronic version of the paper OPF and a system for accessing the electronic folder online. The eOPF system combines document management with workflow capabilities. The eOPF allows each employee to have an electronic personnel folder instead of a paper folder.

Electronic Questionnaires for Investigations Processing (e-QIP): e-QIP is a Web-based automated system designed to facilitate the processing of standard investigative forms used when conducting background investigations for Federal security, suitability, fitness and credentialing purposes. e-QIP allows users to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency.

Employment Reference: An individual with direct knowledge of a subject's character and conduct in the workplace, such as a supervisor, coworker, or subordinate.

Expandable Focused Investigation (EFI): Tailored investigative leads conducted to develop and resolve identified issues and explore the potential for other pertinent issues sufficient to make an informed decision when an eApplication, investigation, or continuous evaluation flags potential issues.

Enhanced Subject Interview (ESI): An in-depth interview between a trained and certified investigator and the subject to develop a full understanding of the subject's background as a required part of an investigation and to offer the subject an opportunity to explain, clarify, refute, or mitigate issues or discrepant information. The ESI shall explore the presence or absence of all potentially disqualifying conditions and mitigating factors.

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.

Foreign National: An individual who is not a citizen of the United States.

Homeland Security Presidential Directive 12 (HSPD-12): Mandates a standard for secure and reliable forms of identification for personnel requiring physical or logical access to Federal facilities or computer systems.

Immigrant: An individual (alien) who is lawfully admitted to the United States under an immigration visa for permanent residence.

Interim Access Authorization: An authorization for access to classified information granted pending completion of the required investigation.

Investigative Record: The official record of all data obtained on the subject from Trusted Information Providers, suitability and/or security applications and questionnaires, and any investigative activity conducted under these standards.

Investigative Service Provider (ISP): A Federal agency authorized to conduct investigations utilizing Federal staff and/or contractor personnel.

Limited Access Authorization (LAA): A certification a person is authorized to have access only to certain specified classified information which has been carefully screened by security officials for its release to that person.

Local Agency Check (LAC): A check/review of records at a State or local law enforcement agency.

Logical and Physical Access: Access other than occasional or intermittent access to Federally controlled facilities or information systems.

Minimum Background Investigation (MBI): An investigation consisting of a National Agency Check and Inquiries (NACI), a credit search, a face-to-face personal interview between the investigator and the subject and telephone inquiries to follow up on written inquiries not returned.

National Agency Check (NAC): An investigation consisting of searches of the following files: Security/Suitability Investigations Index (SII), Defense Central Index of investigations (DCII), the Federal Bureau of Investigation's (FBI) Identification Division, and the FBI's Records Management Division.

National Agency Check and Inquiries (NACI): The NACI is the basic and minimum investigation required on all new Federal employees. It consists of a NAC with written inquiries and searches of records covering specific areas of a person's background during the most recent 5 years.

National Agency Check with Local Agency Check and Credit (NACLC): This investigation is composed of a NAC plus credit search and checks at local law enforcement agencies where the subject has lived, worked, or attended school within the last 5 years, and if applicable, the appropriate agency for any identified arrests.

National Security: The protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs, from overt and covert attack, against or from espionage, sabotage, and subversion, and any and all illegal acts designed to weaken or destroy the United States.

National Security Position: Positions designated "noncritical-sensitive," "critical-sensitive," and "special-sensitive" involving Government activities concerned with the protection of the national security.

Need-to-Know: A determination made by an authorized holder of classified information that a prospective recipient requires access to, knowledge of, or possession of specific classified information to perform or assist in a lawful and authorized U.S. Government function or program.

Operating Administrations (OAs): The component agencies that constitute the operational arm of DOT, each with its own management and organizational structure.

Periodic Reinvestigation (PRI): An investigation updating a previous investigation and consisting of an NAC, credit search, personal interview of the subject, and selected record searches.

Personnel Security: The standards and procedures used to determine and document that the employment or retention in employment of an individual will promote the efficiency of the service and is clearly consistent with the interests of the national security.

Personnel Security Adjudicator: An individual in the servicing security organization who conducts security adjudications.

Personnel Security Coordinator: A specifically appointed individual within a DOT Secretarial Office or Operating Administration who is the liaison between the applicant/employee/contractor completing the security forms and M-40.

Position Designation: The assessment of the potential for adverse impact on the integrity and efficiency of the service, and/or the assessment of the degree to which, by the nature of the position, the occupant could bring about a material adverse effect on the national security.

Position Risk Level: The designation of a position based on its public trust responsibilities and attributes as they relate to the efficiency of the service.

Position Sensitivity: The designation of a national security position based on its relative importance to national security.

Proprietary Information: In trade secret law, information in which the owner has a protectable interest. As specifically defined in the Federal Acquisition Regulation (48 C.F.R. § 3.104-4), it means information contained in a bid or proposal or otherwise submitted to the Government by a competing contractor in response to the conduct of a particular Federal agency procurement, or in an unsolicited proposal, that has been marked by the contractor as proprietary information in accordance with applicable law and regulation.

Public Trust Position: A position which has the potential for action or inaction by an incumbent to affect the integrity, efficiency, or effectiveness of assigned Government activities. Public trust positions are designated as Moderate Risk or High Risk.

Reasonable Accommodation: Any change to a job, the work environment, or the way things are usually done that allows an individual with a disability to apply for a job, perform job functions, or enjoy equal access to benefits available to other individuals in the workplace.

Reimbursable Suitability Investigation (RSI): A customized investigation conducted by the Office of Personnel Management (OPM) to resolve issues that surfaced during or after a standard personnel security investigation.

Reinvestigation: An investigation conducted to update a previously completed background investigation on a person occupying a public trust position, a position requiring access to classified information, or occupying a sensitive position, to determine whether that individual continues to meet the requirements for the position.

Scope: The time period to be covered and the sources of information to be contacted during the prescribed course of a personnel security investigation.

Security Adjudication: The determination as to whether the employment or continued employment of an individual, and the person's access to classified information, if necessary, can reasonably be expected to be clearly consistent with the interests of national security.

Security Eligibility: A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

Security Executive Agent: As defined in EO 13467, the Director of National Intelligence shall serve as the Security Executive Agent.

Security/Suitability Investigations Index (SII): OPM's index of investigations conducted by OPM and by other agencies as reported to OPM.

Sensitive Position: Any position so designated by the head of any department or agency in accordance with Section 3(b) of Executive Order 10450, as amended, or its successor provision.

Servicing Security Organization (SSO): OST Office of Security (M-40) is the designated organizational office responsible for providing security services to a particular DOT administration or office.

Suitability: Identifiable character traits and past conduct which are sufficient to determine whether or not a given individual is likely to carry out the duties of a Federal job with appropriate efficiency and effectiveness.

Suitability Adjudication: The process of determining a person's suitability for Federal employment in a particular position.

Suitability Executive Agent: As defined in EO 13467, the Director of the Office of Personnel Management shall serve as the Suitability Executive Agent.

Temporary Clearance: An authorization for access to classified information granted for a limited period of time.

Trusted Information Provider (TIP): An authorized individual working for or on behalf of the Federal Government, other than for the ISP, who, consistent with the investigative requirements at each tier, corroborates and/or verifies subject data, regarding date and place of birth, citizenship, and education records. These individuals may include Federal Government and contractor employees or military personnel working in human resources or security offices or in equivalent organizations.

Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.

Appendix II

ACRONYMS

APL – Acquisition Policy Letter

ARC – Automated Records Check

BI – Background Investigation

CE – Continuous Evaluation

C.F.R. – Code of Federal Regulations

CI – Counterintelligence

CNSI - Classified National Security Information

CO – Contracting Officer

COR – Contracting Officer Representative

CS – Critical-Sensitive

CUSR – Central United States Registry

CVS – Central Verification System

DCID – Defense Community Intelligence Directive

DCII – Defense Central Index of Investigations

DMDC – Defense Management Data Center

DOD – Department of Defense

DOE – Department of Energy

DOJ – Department of Justice

DOS – Department of State

DOT – Department of Transportation

DSS – Defense Security Service

EFI – Expandable Focused investigation

EO – Executive Order

EOD – Entry on Duty

eOPF – Electronic Official Personnel Folder

e-QIP - Electronic Questionnaires for Investigations Processing

ESI – Enhanced Subject Interview

FAA – Federal Aviation Administration

FBI – Federal Bureau of Investigation

HR – Human Resources

HSPD - Homeland Security Presidential Directive

ICD – Intelligence Community Directive

iIRR – "Improved" Investigative Records Repository

IRR – Investigative Records Repository

IRTPA – The Intelligence Reform and Terrorism Prevention Act

ISP – Investigative Service Provider

ITS – Information Technology System

JPAS – Joint Personnel Adjudication System

LAA – Limited Access Authorization

MARAD – Maritime Administration

MBI – Minimum Background Investigation

NAC – National Agency Check

NACI – National Agency Check and Inquiries

NACLC - National Agency Check with Local Agency Check and Credit

NATO – North Atlantic Treaty Organization

NCS – Noncritical-Sensitive

NISP – National Industrial Security Program

OA – Operating Administrations

OAHR – Operating Administration Human Resources

OF – Optional Form

OIG – Office of Inspector General

OMB – Office of Management and Budget

OPM – Office of Personnel Management

OSC – Office of Special Counsel

OST – Office of the Secretary of Transportation

PIV – Personal Identity Verification

PPD – Presidential Policy Directive

PRI – Periodic Reinvestigation

PSA – Personnel Security Assurance

PSFs – Personnel Security File

PSI – Personnel Security Investigation

PSMO-I – Personnel Security Management Office for Industry

PSO – Post Security Officer

PSRB – Personnel Security Review Board

RSI – Reimbursable Suitability Investigation

RSO – Regional Security Officer

SAP – Special Access Program

SCI – Sensitive Compartmented Information

SES – Senior Executive Service

SF – Standard Form

SII – Security/Suitability Investigations Index

SS – Special-Sensitive

SSO – Servicing Security Organization

SWFT – Secure Web Fingerprint Transmission

TIP – Trusted Information Provider

U.S.C. – United States Code

USCIS – United States Citizenship and Immigration Service

WTTS – Workforce Transformation Tracking System