**U.S. DEPARTMENT OF TRANSPORTATION**
FEDERAL AVIATION ADMINISTRATION

**ORDER 1600.1F**

National Policy

Effective date:
11/04/2021

**SUBJ:** Personnel Security Program

This directive establishes policy and assigns responsibilities for the Federal Aviation Administration's (FAA) Personnel Security Program and for implementing the program in accordance with applicable law.

As the FAA, our mission is to provide the safest, most efficient aerospace system in the world. Our ability to do this depends on the adequacy, reliability, and security of our facilities, automated systems, information, and resources. The objectives of the policies outlined in this order are to prevent the FAA from employing, retaining, or providing access to its facilities, information, or resources to any individual who poses a threat to national security, the safety of the traveling public, or to the safety, security, and integrity of the Agency. By following the policies set forth in this order, we ensure the people who work for the FAA are properly vetted, thus mitigating risks to the FAA and the U.S. aviation system.

Each Assistant Administrator and Associate Administrator, the Chief Counsel, the Chief Operating Officer of the Air Traffic Organization, and each director, manager, and FAA employee must comply with applicable provisions of this order.

Steve Dickson
Administrator

# Table of Contents

## Table of Contents (Continued)

## Table of Contents (Continued)

## Table of Contents (Continued)

# Chapter 1. General Information

**1. Purpose of this Order.** U.S. Department of Transportation (DOT) Order 1630.2, Personnel Security Management, delegates to the Federal Aviation Administration (FAA) the authority to administer its own personnel security program, including the authority to grant security clearances for access to classified national security information (also known as CNSI or classified information). The FAA program must implement the policies of DOT Order 1630.2 and the associated DOT Personnel Security Management Manual (PSMM). Subject to the 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 the DOT PSMM, provided they are sufficient to meet the requirements contained in DOT Order 1630.2. FAA Order 1600.1 establishes personnel security standards, criteria, and procedures for the FAA, consistent with applicable law, Executive Orders (EO), and Government-wide regulations governing the Personnel Security Program. The objective of the Personnel Security Program is to provide the highest possible degree of assurance that the employment, retention, or continued access to classified information of persons working for or on behalf of the FAA will promote the safety, security, and efficiency of the National Airspace System and safeguard national security.

**2. Audience.** This order applies to all FAA employees, contractor employees, and other persons, hereinafter referred to as non-employees, who by agreement with the FAA, have access to FAA facilities, systems, sensitive unclassified information (SUI), resources, and/or classified national security information (CNSI) similar to the access that FAA employees and contractor employees have.

**3. Where Can I Find This Order?** You can find this order on the Directives Management System website: https://employees.faa.gov/tools_resources/orders_notices.

**4. Cancellation.** Upon publication, this order cancels and incorporates information previously contained within the following:

**a.** FAA Order 1600.1E, Personnel Security Program, dated July 25, 2005.

**b.** FAA Order 1600.72A, Contractor and Industrial Security Program, dated December 28, 2005.

**5. Related Publications and References.** Appendix A lists publications and references related to this order.

**6. Definitions.** Appendix B lists definitions used in this order.

**7. Acronyms.** Appendix C lists acronyms used in this order.

**8. Authority to Change this Order.** The Associate Administrator, Security and Hazardous Materials Safety (ASH-1), is authorized to issue changes to this order as necessary to carry out

and manage the Personnel Security Program. ASH-1 must coordinate all changes with the Office of the Secretary of Transportation, Office of Security, M-40.

**9. Explanation of Changes.** This order:

**a.** Removes references to canceled Executive Orders, FAA Orders, and policies, as well as obsolete forms.

**b.** Combines policy from the canceled Contractor and Industrial Security Program Order, FAA Order 1600.72, with this order.

**c.** Updates office titles and routing symbols for the ASH organization and other FAA organizations.

**d.** Updates personnel security policy to include current Federal Investigative Standards, implementation of investigative tiers, changes to background investigation naming conventions, and new reciprocity guidance.

**e.** Updates personnel security file maintenance requirements, to include the change from a paper format to an electronic format.

**f.** Removes the requirement for lines of business and staff offices to have a designated Personnel Security Coordinator.

**g.** Updates procedures for determining position risk and sensitivity levels.

**h.** Combines related chapters and eliminates obsolete chapters.

**i.** Delegates' authority to Office of Personnel Security (AXP) Division Managers to approve certain waivers for persons entering non-critical sensitive and critical sensitive positions.

**j.** Removes specific processing procedures and places them in a standard operating procedure (SOP) manual for internal use by ASH personnel.

**10. Background.** The FAA strives to provide the safest, most efficient aerospace system in the world. To accomplish its mission, the FAA relies on and uses classified national security information as well as unclassified information. As such, it is crucial that the Agency have a robust personnel security program that seeks to provide the highest possible degree of assurance that the FAA will not employ, retain, or allow access to classified information by any individual who poses a threat to the safety, security, or integrity of the Agency; the safety of the traveling public; or, national security. Proper position designation is the foundation of an effective and consistent personnel security program. Background investigations must be commensurate with the risk or sensitivity level of the corresponding positions and must allow the Agency to assess whether a candidate can be trusted with access to FAA facilities, systems, SUI, resources, and/or CNSI. Sound and timely adjudication of background investigations by properly trained Personnel Security Specialists are key to an effective personnel security program. Additionally, adherence to the requirements and standards described in this order is critical to ensuring the

FAA does not grant individuals logical or physical access to FAA facilities, systems, SUI, resources, or CNSI until they meet all applicable personnel security requirements.

**11. Exceptions to Requirements and Standards.** To the extent permitted by applicable law, ASH-1 has the authority to approve exceptions to the requirements and standards outlined in this order.

**12. Scope of This Order.** All employees, contractor employees, and non-employees must comply with the provisions of this order.

**13. Overarching Principles.** The FAA will:

**a.** Not employ or retain a person in employment unless a determination is made that the person's employment or retention will promote the efficiency of the civil service.

**b.** Not employ or retain a person in a position requiring access to classified information unless a determination is made that such employment or retention is clearly consistent with the interests of national security.

**c.** Grant a person eligibility for access to classified information (i.e., a security clearance) only when facts and circumstances indicate that access to classified information is clearly consistent with the national security interests of the U.S. Resolve any doubt concerning eligibility in favor of national security.

**d.** Ensure that all employees responsible for making suitability and security determinations complete formal adjudicative training, in compliance with the Office of the Director of National Intelligence (ODNI) and Office of Personnel Management (OPM) National Training Standards (NTS), within 12 months of entering on duty.

**e.** Not grant access to classified information to anyone unless the required background investigation is completed and favorably adjudicated; the person has a need for access to classified information in order to perform his or her official duties, and the person has signed an approved classified information nondisclosure agreement. In exceptional circumstances, AXP may grant access to classified information to persons whose required investigations are not completed, consistent with government-wide requirements for granting interim or temporary access.

**f.** Afford fair, impartial, and equitable treatment to all FAA applicants, employees, contractor employees, and non-employees through consistent application of personnel security standards, criteria, and procedures consistent with applicable law. FAA will not discriminate on the basis of race, color, sex, national origin, religion, age, disability, marital status, pregnancy, sexual orientation, gender identity, genetic information, or any other protected activity/class in any personnel security actions, including the granting of access to classified information, or use the denial of access to classified information as a substitute for an appropriate adverse suitability determination or disciplinary action.

**g.** Provide all applicants, employees, contractor employees, and non-employees due process, under applicable law and policies, by affording them the opportunity to explain or refute

any unfavorable information before using the information as a basis for finding someone unsuitable for employment or ineligible for a security clearance.

**h.** Not employ any person removed for national security reasons from employment with any U.S. government department or agency without the Secretary of Transportation's prior approval.

**i.** Disclose investigative and personnel security records only to the extent permitted under this order; the Privacy Act of 1974, as amended Privacy Act; the Freedom of Information Act (FOIA); FAA Order 1270.1, Freedom of Information Act Program; FAA Order 1370.121, FAA Information Security and Privacy Program & Policy; and any other applicable orders or directives that implement the Privacy Act and FOIA.

# Chapter 2. Roles and Responsibilities

## 1. FAA Office of the Administrator, Lines of Business (LOB), and Staff Offices (SOs).

**a.** The Administrator is responsible for ensuring that the FAA maintains a Personnel Security Program consistent with applicable law and government-wide policy.

**b.** Management at all levels is responsible for their respective organizations' compliance with and implementation of this order and for communicating the contents of this order effectively within their respective organizations.

**c.** Throughout this order, references to LOB/SOs include the Office of the Administrator, unless otherwise specified.

## 2. Associate Administrator for Security and Hazardous Materials Safety, ASH-1.

**a.** Develops, implements, and manages the FAA's Personnel Security Program on behalf of the Administrator, including but not limited to establishing FAA personnel security requirements and policies.

**b.** Provides executive direction and oversight to ASH personnel responsible for the Personnel Security Program.

**c.** Obtains and effectively uses resources needed to conduct an effective Personnel Security Program.

**d.** Denies or revokes security clearances of persons whose access to classified information is not consistent with the interests of national security.

**e.** Coordinates with affected LOB and SOs and issues changes to this order, as necessary, to meet changing security needs.

## 3. Director, Office of Personnel Security, AXP-1.

**a.** Implements the Personnel Security Program for the FAA on behalf of ASH-1.

**b.** Evaluate the effectiveness of the Personnel Security Program and make or recommend changes in policies and procedures.

**c.** Ensures all Personnel Security Specialists (PSSs) receive appropriate training to comply with the applicable ODNI and OPM NTS.

**d.** Provides information, guidance, and direction, as appropriate, throughout the FAA on all personnel security matters. Develops and issues internal AXP policy and SOPs for PSSs.

**e.** Assists the Office of Acquisition Policy and Oversight (AAP) in developing appropriate personnel security clauses for inclusion in solicitations, contracts, purchase orders (PO), lease agreements, and other similar agreements.

**f.** Collaborates with AAP to ensure guidance and resources for contracting officers and contracting officer representatives, complies with this order.

**g.** Recommends revocation or denial of security clearances, as appropriate, to ASH-1 when a person's access to classified information would not be consistent with the interests of national security.

**h.** Grants or denies residency waiver requests for foreign nationals.

**i.** Serves as the FAA liaison with other Government agencies on personnel security matters.

**j.** Issues policy updates and clarifications affecting the implementation of this order, in coordination with ASH-1 and interested LOB and SOs, as appropriate.

**4. Managers, Personnel Security Division, East, AXP-400 and West, AXP-500.**

**a.** Ensure compliance with personnel security and suitability investigative requirements.

**b.** Ensure all PSSs receive training in compliance with the NTS.

**c.** Ensure all employees, contractor employees, and non-employees undergo the appropriate background investigation and, if applicable, periodic reinvestigation, as required by Federal Investigative Standards.

**d.** Check investigation databases prior to initiating investigations to validate the need for an investigation and exercise reciprocity, as appropriate.

**e.** Provide assistance and resources throughout their area of responsibility on designating position risk and sensitivity levels.

**f.** Ensure that position risk and sensitivity levels are properly determined and are accurate for all positions within their area of responsibility.

**g.** Adjudicate the results of background investigations in accordance with suitability standards and criteria set forth in Title 5, Code of Federal Regulations (CFR), Part 731, and applicable adjudicative guidelines.

**h.** Evaluate background investigations against government-wide Quality Assessment Standards and record assessments in the Quality Assessment Reporting Tool, as required by the Security Executive Agent. The Director of National Intelligence is the Security Executive Agent.

**i.** Provide a due process to all applicants, employees, contractor employees, and non-employees during the adjudication process prior to taking any unfavorable action.

**j.** Refer applicant and employee adjudications, determined to be potentially unsuitable, to the Office of Human Resource Management (AHR) for a final suitability determination.

**k.** Adjudicate security issues, grant security clearances, and, as necessary, suspend clearances and recommend revocation and denial of security clearances.

**l.** Notify appropriate LOB/SO and AHR whenever an applicant or employee has had their security clearance denied or revoked and provide all information needed to take appropriate action.

**m.** Ensure that employees who hold security clearances complete required initial and recurrent training.

**n.** Process visit clearance requests and verify security clearances as necessary.

**o.** Notify the responsible AAQ Contracting Officer (CO) or delegated Contracting Officer's Representative (COR) in writing when an interim suitability determination is made on a contractor employee.

**p.** Notify the responsible AAQ CO, or delegated COR, in writing of any contractor employee found unsuitable for access to FAA facilities, systems, SUI, CNSI, and/or resources, and direct action to deny such access.

**q.** Provide advice, guidance, and direction, as appropriate, throughout their area of responsibility on all personnel security matters.

**r.** Advise all LOB/SOs of all changes in policy, procedures, and costs of background investigations.

**s.** Periodically evaluate Personnel Security Program in their division to ensure that it is operating effectively and efficiently.

**5. Manager, Personnel Security Business and Analytics Division, AXP-300.**

**a.** Provide guidance to LOB/SOs and AAQ, when requested, on which solicitations, contracts, POs, lease agreements, and other similar agreements should require an investigation of contractor employees.

**b.** Review solicitations, contracts, POs, lease agreements, and other similar agreements that will require contractor employees to have a background investigation to ensure the appropriate security clauses are included.

**c.** Review Position Designation forms, in conjunction with the Statement of Work (SOW), to ensure position risk/sensitivity level designations are correct and appropriate and approve or disapprove accordingly.

**d.** Coordinate all solicitations, contracts, POs, lease agreements, and other similar agreements that require contractor employees to have access to CNSI with the Information Safeguards Division, AXF-200, to ensure compliance with Department of Defense National Industrial Security Program Operating Manual (NISPOM) requirements.

**6. Manager, Personnel Security Policy and Programs Division, AXP-100.**

**a.** Provides advice and guidance to AXP divisions on all personnel security matters.

**b.** Develops policy, SOPs, and other resources to assist AXP divisions with implementing the personnel security program.

**c.** Evaluates referrals from AXP divisions recommending security clearance denial or revocation, and provides due process for accepted referrals.

**d.** Recommends revocation or denial of security clearances, as appropriate, to ASH-1 when a person's access to classified information would not be consistent with the interests of national security.

**e.** Conducts program evaluations of AXP divisions to determine if processes comply with SOPs, Agency policy, and applicable law.

**7. Office of Human Resource Management, AHR.**

**a.** Include appropriate information about investigative and/or personnel security clearance requirements that are a condition of employment in all vacancy announcements.

**b.** Enter applicants who have accepted a tentative offer of employment into the Investigation Tracking System (ITS) and upload all documents required for security processing.

**c.** Verify that, prior to processing a personnel action to place an individual in any position, the responsible AXP office has determined that the individual meets applicable pre-placement investigative requirements or has received an appropriate waiver.

**d.** Maintain and update, as necessary, position description records to reflect approved position risk and sensitivity level designations accurately.

**e.** Make final suitability determinations on all cases referred by AXP as potentially disqualifying. Notify AXP of final suitability determinations.

**f.** Notify AXP of any employment action resulting from a clearance revocation or denial (ex. removal, reassignment to a non-sensitive position, non-selection, etc.).

**g.** Upload required personnel security records into electronic Official Personnel Folders.

**8. FAA Managers.**

**a.** Familiarize personnel under their supervision with applicable personnel security standards, criteria, procedures, and oversee their compliance.

**b.** Include background investigation and/or security clearance requirements that are conditions of employment in vacancy announcements.

**c.** Confirm with AHR, before placing or making any commitment to place a person in any position, that the individual meets applicable pre-placement investigative requirements or has received an appropriate waiver.

**d.** Identify and report to the responsible AXP office any deviation from personnel security standards, criteria, or procedures.

**e.** Ensure that employees under their supervision complete required investigative forms and cooperate with personnel security investigations.

**f.** Require employees under their supervision who hold security clearances to comply with annual training requirements for access to CNSI.

**g.** Properly designate all positions in their respective organizations and coordinate the risk level or sensitivity designation, as applicable, with the responsible AXP office on all newly established or revised positions.

**h.** Coordinate with AHR and the responsible AXP office when a position's duties change to require access to CNSI and re-designate the position at the appropriate sensitivity level.

**i.** Include the approved position designation and any requirement for access to classified information in position descriptions.

**j.** Determine the need for a security clearance for any foreign temporary duty assignment, and coordinate with the responsible personnel security office on any assignment determined to require a temporary security clearance.

**k.** Advise the responsible AXP office of any conduct or activity by an employee, contractor employee, or non-employee that calls into question their suitability for federal employment or eligibility to hold a security clearance, as applicable. Appendix D lists conduct and activities that pose suitability concerns. The National Security Adjudicative Guidelines provide the security clearance eligibility concerns and is available by link in Appendix A.

**9. FAA Employees, Contractors and Non-Employees.**

**a.** Comply with all applicable requirements of this order.

**b.** Comply with all applicable investigation and reinvestigation requirements, including submitting fingerprints and completing investigative forms upon request and within established deadlines, unless AXP grants an extension.

**c.** Familiarize themselves with pertinent security requirements pertaining to their assigned duties, and with the standards of conduct required of all employees. Recognize and avoid personal behavior that could render them ineligible for continued assignment in their position.

**d.** Promptly report all violations of security requirements to their personnel security office.

**e.** Comply with all applicable international travel security briefing requirements when traveling abroad for either official or unofficial business, as required by FAA Order 1600.61, International Travel Security Program.

**10. FAA Employee Security Clearance Holders.**

**a.** Comply with annual training requirements for access to CNSI.

**b.** Comply with Security Executive Agent Directive (SEAD) 3 reporting requirements, outlined in Chapter 7 of this order. These include planned or actual involvement in certain activities, including foreign travel, foreign contacts, foreign activities, media contacts, arrests, financial anomalies, alcohol-or drug-related treatment, and foreign national associates. Additional requirements include reporting any information that raises doubts as to whether another security clearance holder's continued national security eligibility is clearly consistent with the interests of national security.

**c.** Protect classified information from unauthorized disclosure, in accordance with FAA Order 1600.2, Classified National Security Information.

**11. Acquisitions & Contracting (AAQ) Contracting Officers (COs) unless delegated.**

**a.** Send all procurement actions that will require a contractor to have physical or logical access to FAA facilities, systems, SUI, resources, and/or CNSI to the responsible AXP office for review during the pre-award stage.

**b.** Ensure that all procurement actions determined by the LOB/SO to have security requirements contain the appropriate security clauses.

**c.** Provide a copy of the award to the responsible AXP office whenever a contract, PO, lease agreement, or other similar agreement requires investigation of any contractor and/or contractor employees.

**d.** Ensure that all contracts requiring access to CNSI by a contractor and/or contractor employees:

**(1)** Conform to the requirements in the NISPOM;

**(2)** Include a Contract Security Classification Specification (Department of Defense (DD) Form 254);

**(3)** Include the security clause relating to classified contracts; and,

**(4)** Identify the tasks to be performed requiring access to CNSI in the contract SOW.

**e.** Notify the personnel security office whenever there is a change in the status of a contract, PO, lease agreement, or other similar agreement, having a security requirement (e.g., modified, terminated, replaced, or defaulted).

**f.** Maintain a listing of all contractor employees working on-site for each contract and coordinate with the responsible AXP office to ensure accuracy.

**g.** Notify the responsible AXP office whenever a contractor employee resigns, transfers to another location, is terminated, completes work under the contract, or his/her employment status otherwise changes within 24 hours of becoming aware of the information.

**h.** Notify the responsible AXP office of any information received, which raises a question about the fitness of a contractor employee within 24 hours of becoming aware of the information.

**i.** Assist AXP in obtaining compliance with security requirements by enforcing the security clauses in the contract, PO, lease agreement, or other similar agreement.

**j.** Notify the relevant COR and LOB/SO of all contracts that call for escorting of contractor employees and oversee compliance with proper escort procedures.

**k.** Forward Position Designation forms to the responsible AXP office for review and approval, prior to any contractor employee beginning work on an FAA contract, and retain a copy.

**l.** Remove from the contract within 24 hours, any contractor employee determined by AXP to be unsuitable, and notify AXP upon completion.

**m.** Do not permit a contractor employee to begin work on an FAA contract until the responsible AXP office confirms that interim or final suitability has been granted to the individual.

**12. Contracting Officer Representatives (CORs)**

**a.** Determine position risk and sensitivity levels for contractor employee positions using the OPM Position Designation Automated Tool (PDT) and submit to the responsible personnel security office for review and approval prior to any contractor employee beginning work on the contract.

**b.** Do not permit a contractor employee to begin work on an FAA contract until the responsible AXP office has notified the CO/COR that interim or final suitability has been granted to the individual.

**c.** Maintain a listing of all contractor employees working on-site for each contract and coordinate with the personnel security office to ensure accuracy.

**d.** Monitor contractors' compliance with security requirements. Ensure contractors' performance of requirements is in agreement with provisions contained in the applicable security clauses.

**e.** Notify the responsible AXP office whenever a contractor employee resigns, is terminated, is transferred to another location, has completed work under the contract, or his/her employment status otherwise changes, within 24 hours of becoming aware of the information.

**f.** Notify the responsible AXP office of any information received, which raises a question about the fitness of a contractor employee, within 24 hours of becoming aware of the information.

**g.** Ensure contractor employees are properly escorted when required under the relevant contract.

## Chapter 3. Designating Position Sensitivity and Risk Levels for Federal Positions

**1. Position Sensitivity and Risk Level Designation.** All FAA positions receive a risk level designation, based on the potential for adverse impact to the efficiency and integrity of the service. Positions that require access to CNSI also receive a sensitivity designation based on the degree of potential damage to national security.

OPM's PDT provides a systematic, dependable, and uniform way of making position sensitivity and risk level designations. The PDT is used to assess the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the federal service, should misconduct of an incumbent occur. This establishes the risk level of that position. This assessment also determines if a position's duties and responsibilities present the potential for position incumbents to bring about a material adverse effect on national security, and the degree of that potential effect, which establishes the sensitivity level of a position. The results of this assessment determine the level of investigation required for a position.

**a. Low Risk**. Positions that involve duties and responsibilities of limited relation to the FAA mission, and have the potential of limited impact on the efficiency and integrity of the service. Positions with access to critical areas of National Airspace System operational facilities, critical systems, or critical information should not be designated as Low Risk.

**b. Moderate Risk**. Public trust positions with the potential for moderate to serious impact. They involve duties of considerable importance to the Agency or program mission with significant program responsibilities and delivery of customer services to the public.

**c. High Risk.** Public trust positions with the potential for exceptionally serious impact involving duties especially critical to the FAA or a program mission with a broad scope of policy or program authority.

**d. Non-critical Sensitive.** Sensitive positions with the potential for causing significant or serious damage to national security. Position requires eligibility for access to Secret or Confidential CNSI.

**e. Critical Sensitive.** Sensitive positions with the potential for causing exceptionally grave damage to national security. Position requires eligibility for access to Top Secret CNSI.

**f. Special Sensitive.** Sensitive positions with the potential to cause inestimable damage to national security. Position requires eligibility for access to Sensitive Compartmented Information (SCI), other intelligence-related Special Sensitive information, or involvement in Top Secret Special Access Programs (SAPs).

**2. Responsibility for Position Sensitivity and Risk Level Designations.** LOB/SOs are responsible for determining the correct position sensitivity and risk level designations for each position within their respective organizations prior to submitting position descriptions to AHR for requested personnel actions. AHR and LOB/SOs must coordinate all position designations for new position descriptions with their responsible personnel security office to ensure uniform

designations for positions common in more than one region. AXP has the right and responsibility to challenge any position sensitivity or risk level designations made by AHR and the LOB/SO that appear to be incorrectly designated.

Individuals with position designation responsibilities must use the PDT to make position designations. The PDT is available at https://pdt.nbis.mil/. OPM offers training on the use of the PDT when requested.

**3. Official Record of Position Risk and Sensitivity Designation.** AHR is responsible for maintaining a record of each position's sensitivity and risk level designation. The record may be maintained electronically, in lieu of retaining a hard copy. If a position sensitivity and risk level designation record already exists for a position, it is not necessary to produce another one every time a person is placed into the position (i.e., the position sensitivity and risk level designation is completed for the *position*, not for each person placed into that position).

## Chapter 4. Personnel Security Investigation Requirements

**1. Introduction**. Federal Investigative Standards (FIS) have been established by the Director of the Office of Personnel Management, which is the designated Suitability Executive Agent (SuitEA), and the Office of the Director of National Intelligence, which is the designated Security Executive Agent (SecEA). These investigative standards apply to background investigations used 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.

The FAA will not establish additional investigative requirements that exceed these standards without the approval of the Suitability and Security Executive Agents. The Executive Agents ensure that any approvals to establish additional requirements are limited to circumstances in which additional requirements are necessary to address significant needs unique to the agency involved or to protect national security, and ensure that investigations conducted under the standards remain aligned to the extent possible.

**2. Types of Background Investigations and Investigative Requirements.** The type of background investigation required is determined by the position's risk or sensitivity level, and the security clearance, if any, required for a position. The PSS is responsible for initiating the appropriate investigation in accordance with the FIS, as outlined by the SuitEA and SecEA. There are five investigative tiers, and each successively higher level of investigation builds upon, but does not duplicate, the levels below it.

**a. Tier 1 Investigation.** 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 Homeland Security Presidential Directive (HSPD) 12, using Standard Form (SF) 85, or its successor form.

**b. Tier 2 Investigation.** Investigations conducted to this standard are for non-sensitive positions designated as moderate risk public trust, using SF-85P, or its successor form.

**(1) Tier 2 Reinvestigation.** A person occupying a Tier 2 position must be reinvestigated at least once every five years and when certain events occur, subject to implementing guidance.

**c. Tier 3 Investigation.** Investigations conducted to this standard are for positions designated as non-critical sensitive, and/or requiring eligibility for L access (used in the Department of Energy (DOE)) or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information, using SF-86, or any successor form. (A security clearance cannot be granted on the basis of any investigation conducted based on a SF-85P.)

**(1) Tier 3 Reinvestigation.** A person occupying a Tier 3 position is subject to reinvestigation at least every five years and when certain events occur, subject to implementing guidance.

**d. Tier 4 Investigation.** Investigations conducted to this standard are for non-sensitive positions designated as high-risk public trust positions, using SF-85P, or its successor form. (A security clearance cannot be granted on the basis of any investigation conducted based on a SF-85P.)

**(1) Tier 4 Reinvestigation.** A person occupying a Tier 4 position is subject to reinvestigation at least every five years and when certain events occur, subject to implementing guidance.

**e. Tier 5 Investigation.** Investigations conducted to this standard are for positions designated as critical sensitive, special sensitive, and/or requiring eligibility for Q access (used by the DOE) or access to Top Secret or SCI, using SF-86, or any successor form.

**(1) Tier 5 Reinvestigation.** A person occupying a Tier 5 position is subject to reinvestigation at least every five years and, when certain events occur, subject to implementing guidance.

**f. Continuous Evaluation.** Pursuant to guidance prescribed by the SecEA, subjects may be reevaluated on a random or continuous basis between investigative cycles.

**3. Basic Investigative Requirements.**

**a. Special Sensitive Position.** A person occupying a special sensitive position must have a completed and favorably adjudicated Tier 5 investigation, or meet the applicable requirements of Section 5 of this chapter, prior to being placed in the special sensitive position. A completed and favorably adjudicated Tier 5 investigation is required before a Top Secret clearance can be granted, and before the subject can be considered for SCI access.

**b. Critical Sensitive Position.** A person occupying a critical sensitive position must have a completed and favorably adjudicated Tier 5 investigation, or meet the applicable requirements of Section 5 or Section 6 of this chapter, prior to being placed in the critical sensitive position. A completed and favorably adjudicated Tier 5 investigation is required before a final Top Secret clearance can be granted.

**c. Non-critical Sensitive Position.** A person occupying a non-critical sensitive position must have a completed and favorably adjudicated Tier 3 investigation, or meet the applicable requirements of Section 5 or Section 6 of this chapter, prior to being placed in the non-critical sensitive position. A completed and favorably adjudicated Tier 3 investigation is required before a final Secret clearance can be granted.

**d. High Risk.** A person occupying a high-risk position must have a completed and favorably adjudicated Tier 4 investigation, or meet the requirements of Section 5 of this chapter, or receive a favorable interim suitability determination from the processing personnel security office, prior to being placed in the high-risk position.

**e. Moderate Risk.** A person occupying a moderate-risk position must have a completed and favorably adjudicated Tier 2 investigation, or meet the requirements of Section 5 of this chapter, or receive a favorable interim suitability determination from the processing personnel security office, prior to being placed in the moderate-risk position.

**f. Low Risk.** A person occupying a low-risk position must have a completed and favorably adjudicated Tier 1 investigation, or meet the requirements of Section 5 of this chapter, or receive a favorable interim suitability determination from the processing personnel security office, prior to being placed in the low-risk position.

**4. Investigative Methodology.** Investigative coverage obtained by FAA's Investigation Service Provider (ISP) will follow the investigative methodology established in the Federal Investigative Standards (FIS). The FIS outline the requirements for subject interviews, the use of automation, the use of Trusted Information Providers, and other standards. The FIS also outlines the specific requirements for an Expandable Focused Investigation (EFI), based on derogatory information or discrepancies. The EFI model is subject to change, based on direction by the Suitability or Security Executive Agents. The FAA may request additional investigation from its ISP for any information necessary to resolve issues in order to render an adjudicative decision.

**5. Reciprocity.** Except as otherwise permitted by applicable Security Executive Agent directives, the FAA will exercise reciprocity by accepting existing background investigations meeting reciprocity requirements, in lieu of initiating new investigations.

Reciprocity is required when the investigation is within scope, was favorably adjudicated, there has been no break in service over 24 months, and no new derogatory information is known.

Reciprocity is not required when the new position requires a higher level investigation than previously conducted; there is new information that calls into question the subject's suitability for federal employment, eligibility for a sensitive position, eligibility for access to classified information, or fitness; and/or the individual's investigative record shows conduct that is incompatible with the core duties of the new position.

PSSs will conduct appropriate checks of indices and databases to validate whether there is an existing investigation that meets or exceeds the investigative requirement of the sought position. If reciprocity requirements are not met, a new investigation will be conducted in accordance with this chapter.

**6. Waivers for Sensitive Positions.**

**a. General**. AXP may approve persons to occupy sensitive positions before the investigation and adjudication processes are completed. These temporary eligibility approvals, also known as waivers, may be issued during exceptional circumstances when official functions must be performed, including meeting mission readiness requirements. The Office of the Secretary of Transportation's, Office of Security, M-40, has delegated authority to AXP-1 to grant waivers for persons entering non-critical sensitive and critical sensitive positions. AXP-1 has further delegated this authority to the AXP Division Managers. Waiver requests will be processed in accordance with Security Executive Agent Directive 8, Temporary Eligibility.

**b. Waiver Request**. To request approval for an employee to be placed in a sensitive position before the completion of the investigation and adjudication processes, a LOB/SO must submit a written waiver request to their responsible personnel security office containing the following information:

**(1)** The nature of the waiver being requested (e.g., a waiver to allow appointment, reassignment, detail, or promotion, etc.);

**(2)** The position's title, grade, location, position sensitivity level, and security clearance level, if the position requires a security clearance;

**(3)** An explanation of the exceptional circumstances justifying placement in a sensitive position before the completion of the investigation and adjudication processes; and,

**(4)** Either a statement that the employee will not have access to CNSI until the investigation is completed and the personnel security office has granted a security clearance; ***or*** a request for a temporary clearance for the employee, if needed, while the appropriate investigation and adjudication are pending.

The personnel security office will review the waiver request, request the completion of investigative forms by the employee, confirm citizenship has been verified, review completed forms, and conduct indices check required under SEAD 8, to determine whether or not the waiver will be granted. Any doubts about the subject's eligibility to occupy a national security position will be resolved in favor of national security, and the waiver request will be denied. AXP may rescind a waiver approval if disqualifying information is received at any time during the waiver period. Waiver approvals remain valid until the exceptional circumstances have abated, the temporary eligibility is terminated, or final eligibility is granted. Temporary eligibility must not exceed one year unless approved by AXP-1.

Derogatory information that may cause a waiver request to be denied includes information that raises doubts about the subject's judgment, trustworthiness, or reliability, in accordance with applicable security adjudicative guidelines.

**c. Exceptions**. Due to the volume of sensitive Air Traffic Control Specialist positions hired each year, a blanket waiver has been approved; therefore individual written waiver requests are not required for appointment into these positions. LOB/SOs may contact AXP if they wish to request a blanket waiver in connection with mass hiring efforts. Approval of such a request is at the discretion of AXP-1.

**7. Exceptions to Investigative Requirements.**

**a. Exempt Positions.** Certain low-risk positions are exempt from the investigative requirements. This exemption should not be viewed as a prohibition from processing the subject under the normal investigative requirements. These positions may include, but are not limited to:

**(1)** Contractor employees exempted under Chapter 8, Section 6(c);

**(2)** Non-employees exempted under Chapter 8, Section 7(b); and,

**(3)** Positions located outside the U.S. that are occupied by persons who are not U.S. citizens.

**b. Details and Other Temporary Assignments of 180 days or less.**

**(1)** Details and Other Temporary Assignments into Public Trust Positions. Employees who do not meet the investigative requirements of a higher level public trust position, may be approved by the personnel security office to detail or be temporarily assigned, for 180 calendar days or less, into the position upon favorable review of the person's previous investigation, Personnel Security File, and a newly completed electronic Questionnaires for Investigations Processing (e-QIP) security questionnaire.

**(2)** Details and Temporary Assignments into Non-Critical and Critical Sensitive Positions.

(a) If the detail/temporary assignment in question will not require access to CNSI, despite the position normally requiring access to CNSI, the LOB/SO must submit a written waiver request, as outlined in Section 6 of this chapter, and include a statement that the employee will not have access to CNSI during the detail/temporary assignment. The detail/temporary assignment may be approved by the personnel security office upon a favorable review of the subject's previous investigation, Personnel Security File, and a newly completed electronic Questionnaire for Investigations Processing (e-QIP) security questionnaire.

(b) If access to CNSI is required in the detailed/temporary position, the LOB/SO must submit a written waiver request, as outlined in Section 6 of this chapter, and include a request for a temporary clearance for the employee. The employee must meet the normal investigative requirements of the position, or meet the requirements for a temporary clearance, as outlined in Chapter 7 of this order.

**(3)** Details and Temporary Assignments into Special Sensitive Positions.

(a) Employees must already have a minimum of a Top Secret clearance granted based on a favorably adjudicated Tier 5 investigation, or equivalent, in order to be considered for a detail or temporary assignment into a Special Sensitive position.

(b) All details and temporary assignments into Special Sensitive positions require the prior approval of the manager of the Special Operations and Law Enforcement Support Division, AXE-300.

**(4)** Extensions. The normal investigative requirements must be met for any detail/temporary assignment that is extended beyond 180 calendar days.

**c. Details and Temporary Assignments in excess of 180 days**. Details and temporary assignments in excess of 180 calendar days are subject to the normal investigative requirements of the position, as outlined in Section 3 of this chapter.

# Chapter 5. Personnel Security Records

## 1. Personnel Security Files (PSFs).

**a.** AXP must establish PSFs for all applicants, employees, contractor employees, and non-employees, and maintain PSFs electronically in ITS, or any successor database. Records maintained in ITS are covered under the Privacy Act system of records notice published in the Federal Register, DOT/FAA 815, and Investigative Record System.

**b. PSF contents.** The responsible personnel security office must keep the following records in the PSF:

**(1)** All documents and forms submitted in connection with background investigations, including but not limited to:

(a) e-QIP questionnaires (e.g., SF-85, SF-85P, SF-86);

(b) Disclosure and Authorization Pertaining to Consumer Reports, DOT Form 1631;

(c) Declaration for Federal Employment, Optional Form 306 (OF-306), if needed; and,

(d) Resume, if needed.

**(2)** Pertinent correspondence (formal and informal) between the personnel security office and the applicant, employee, contractor employee, or non-employee related to their background investigation and/or issue resolution. Do not upload exchanges concerning access issues, fingerprinting locations, and other related matters.

**(3)** Pertinent correspondence between the personnel security office and AHR, Office of Aerospace Medicine (AAM), AAQ, other FAA LOB/SOs, ISPs, or other government agencies, related to the personnel security of the applicant, employee, contractor employee, or non-employee.

**(4)** Forms and documents related to the adjudication of background investigations.

**(5)** Reports of investigation (ROIs) completed by FAA's ISP, and/or other agencies.

**(6)** ROIs completed by FAA's Internal Investigations Division, AXI-100.

**(7)** Memoranda are documenting waivers and temporary and interim security clearances.

**(8)** Classified Information Nondisclosure Agreement (SF-312) and all documents relating to the granting, termination, suspension, or revocation of security clearances.

**(9)** A record of all PSF disclosures to persons outside the FAA.

**2. Personnel Security File Retention.** AXP will maintain and destroy PSFs of separated employees, contractor employees, non-employees, and inactive applicants in accordance with established records management policy and retention schedules found in the National Archives and Records Administration (NARA).

**3. Protection of Personnel Security Records.** Personnel security records contain sensitive and Personally Identifiable Information (PII) that must be protected from unauthorized access and disclosure. All PSSs must:

**a.** Control investigative information received from a confidential source in accordance with the restrictions that the investigating agency has placed on it. Such restrictions normally preclude divulging investigative information to the subject of the investigation, or anyone else, without a need to know.

**b.** Control medical information included as part of an investigation to ensure that the information is disseminated only to personnel who need it for security or suitability adjudication. Such information must only be released to LOB/SO managers through AAM officials, who will interpret the medical information for management officials who have a need to know.

**c.** Protect ROI, files, or other records that contain CNSI, as required by Executive Order 13526, Classified National Security Information; the applicable NARA regulations in 32 C.F.R. Part 2001 and 2004; FAA Order 1600.2; and other applicable law. Classified information received in connection with an employee's, contractor employee's, non-employee's' or applicant's background investigation must not be uploaded into ITS. In these instances, a remark must be entered into the ITS record indicating:

**(1)** There is classified information contained in a file that is stored in a safe, or

**(2)** Classified information was received from another government agency that did not impact the adjudication, and has been destroyed.

**d.** Protect, transmit, store, and destroy all personnel security records as required by FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI), FAA Order 1370.121, and other applicable laws.

**(1)** PSFs are considered SUI. Individual documents and records do not need to be marked as SUI, as long as they reside in ITS. Records handled outside of ITS, must be marked as the appropriate category of SUI.

**(2)** When emailing documents reproduced from a PSF, documents must be marked as the appropriate category of SUI and sent encrypted.

**(3)** When documents reproduced from a PSF are not under the physical custody or the control of an authorized person, they must be stored in a lockable container, such as a file cabinet or desk, or in a locked space.

**(4)** When documents reproduced from a PSF are no longer needed, they must be destroyed in a manner that makes them unreadable, indecipherable, and unrecoverable. SUI may

not be placed in office trash bins or recycling containers. At a minimum, SUI must be destroyed in a crosscut shredder or by commercial destruction services obtained by the FAA, unless the specific type of SUI involved requires a different method of destruction.

**4. Individual Access to a PSF.** PSSs must grant an applicant, employee, contractor employee, non-employee, or their designated representative, access to their PSF upon request, in accordance with the Privacy Act and FAA Order 1370.121. Individuals must designate any representatives in writing. When complying with a request for a PSF, the PSS must:

**a.** Evaluate any request for access under both the FOIA and the Privacy Act, regardless of which the requester cites, and determine which statute, in the specific circumstances at hand, provides greater access.

**b.** Examine the file for any third-party reports. If the PSF contains a report from another agency, remove the report before providing the PSF for release. If such a report is removed, the response must advise the requester that the original PSF contains a report completed by another agency, the FAA is not authorized to release it directly to them, and they can contact the investigating agency directly in order to request a copy. Defense Counterintelligence and Security Agency (DCSA) reports can be released to a subject for the specific purpose of providing Procedural Rights or Administrative Due Process. Release of any records for these purposes is limited in scope to only those records specifically relied upon. This is considered a re-disclosure. Re-disclosure to a subject should be coordinated with the DCSA FOIA/Privacy Act office, to ensure that any re-disclosure does not violate statutory restrictions.

**c.** If the PSF contains an FAA Report of Investigation (ROI), the request must be referred to the Office of Investigations (AXI) for determination and release of the ROI.

**d.** Information that would identify a confidential source, PII of a third party, and information about an ongoing investigation is exempt from release under the Privacy Act, and must be removed before releasing.

**e.** Releasable PSF contents can be sent to the requester through email or U.S. mail utilizing protective transmittal measures outlined in FAA Order 1600.75.

**f.** Annotate the request and disclosure in the PSF. Individuals do not need to sign an acknowledgment when reviewing investigative information pertaining to them.

**5. Other Disclosures of Personnel Security Records.**

**a.** A PSS can share personnel security records, including DCSA ROI to authorized FAA officials who have a need to know for a specific purpose under EO 13467 as amended, to the extent permitted by applicable law and policy. Authorized purposes include but are not limited to:

- Adjudications and related hearings and appeals
- Continuous evaluation
- Insider threat programs

- Inspector general functions
- Counterintelligence

Prior to disclosing a DCSA report, the PSS must review the report to identify any information that is subject to limitations on its distribution internally within the FAA, under the Privacy Act or other applicable law or policy. Limitations that may be relevant include, but are not limited to:

- Classified material
- Other government agency data and reports
- Financial information protected by either the Fair Credit Reporting Act (e.g., a Credit Report) or the Right to Financial Privacy Act
- Law Enforcement/Criminal History Record Information limited by 5 USC 9101(d)
- Fingerprint Name Check Only results
- Information from the Financial Crimes Enforcement Network
- IRS Tax Information collected with a 4506-T release potentially limited by 26 USC 6103

Any questions about the release of items in the report are to be directed to DCSA's FOIA office. All FAA recipients must carefully protect any information released to them from personnel security records in accordance with all applicable law and policy.

**b.** Any external request for records must be evaluated under both the FOIA and Privacy Act regardless of the law cited, to determine which statute, in the specific circumstances presented, provides greater access.

**c.** The information must not be released to a third party, unless the first party to whom a record pertains signs a statement granting permission to release the specific information requested. If such permission is granted, the release authority document must be uploaded to the PSF.

**d.** If the first party to whom a record pertains does not grant permission to release their records, the procedures for responding to the third-party request under FAA Order 1270.1, and the FOIA Procedural Manual are to be followed.

**e.** Requests for information concerning deceased persons are to be processed under the provisions of the FOIA.

**6. Agreements to Release Personnel Security Records.** Without the concurrence of ASH-1, no FAA employee may enter into any agreement requiring the FAA or any FAA organization to release any information from personnel security records. This includes ROI completed by other Federal agencies.

## Chapter 6. Personnel Suitability Standards, Criteria, and Adjudication

**1. Background.** The 1996 DOT Appropriations Act, Public Law 104-50, directed the FAA to develop and implement a new personnel management system that addresses the unique demands on the Agency's workforce, and provides for greater flexibility in the hiring, training, compensation, and location of personnel. As a result of this law, the FAA became an excepted service agency. This law exempted the FAA from most of the personnel provisions in Title 5 USC, except for those specifically identified in the law. The FAA remains covered by Chapter 73 of Title 5, U.S.C., relating to suitability, security, and conduct, but is exempt from the Title 5 provisions relating to suitability investigations adjudication. The FAA developed its own program for investigating and adjudicating the suitability of FAA applicants and appointees, largely following the practices set forth by OPM. Pursuant to its appointment and employment authority, the FAA requires individuals applying for FAA employment to undergo an investigation to establish their suitability or fitness for employment.

**2. Suitability and Fitness Distinction.** *Suitability* refers to identifiable character traits and past and present conduct that are sufficient in determining whether a person is likely or unlikely to be able to carry out the duties of a Federal job in the competitive service with appropriate efficiency and effectiveness. The focus of suitability is on whether the employment, or continued employment, of an individual, can reasonably be expected to promote the efficiency of the Federal service. It is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

*Fitness* is the level of character and conduct determined necessary for an individual to perform work for, or on behalf of, a Federal agency as an employee, or a contractor employee, in the excepted service. Fitness determination means 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 an employee, or a contractor employee, in the excepted service.

Although the FAA, as an excepted service agency, is exempt from the provisions in Title 5 relating to suitability investigations adjudication, the Agency has developed its own program largely adopting the same adjudication guidelines and procedures set forth by OPM. As such, the term *suitability* has often been used in the FAA when referring to fitness and fitness determinations. To remain consistent with Human Resources Personnel Manual EMP 1.24, Suitability, and the Human Resources Suitability Handbook, and to avoid any confusion with medical fitness determinations, the FAA will use the term suitability throughout this Order to encompass the concepts of both suitability and fitness, as described above.

**3. Responsibilities.** AXP and AHR are both involved in the suitability adjudication process for FAA employees and applicants. AXP conducts suitability adjudications on all background investigations, and refers cases containing potentially disqualifying suitability issues to AHR. AHR has the authority and responsibility to make final suitability determinations on FAA employees and applicants.

AXP is responsible for making final suitability determinations on contractor employees and non-employees.

**4. Applicability.** All applicants, probationary employees, contractor employees, and non-employees, are subject to a suitability determination. Non-probationary employees are not subject to suitability determinations; however, these employees are subject to disciplinary and adverse personnel actions in accordance with the Standards of Conduct and other applicable Agency policies. Derogatory issues that surface during background investigations of non-probationary employees will be handled in accordance with Section 9(b) of this chapter. Employees in sensitive positions are also subject to security adjudication determinations, in accordance with Chapter 7 of this order.

**5. Suitability Adjudicative Standard and Criteria.** The objective of the suitability adjudicator is to establish a reasonable expectation that the employment or continued employment of the person would protect the integrity or promote the efficiency of the service. When there is a reasonable expectation a person's employment would not protect the integrity or promote the efficiency of the service, the person must be found unsuitable. This expectation is established when an adverse nexus, or direct connection, can be shown between the character or conduct in question, and the integrity of a competitive examination or appointment; the integrity of the competitive examining system; or the person's capacity and fitness for employment in covered positions. Refer to Appendix D for suitability factors and additional considerations to apply when making suitability determinations.

**6. Employee Applicant Suitability Screening Process.**

**a.** The suitability screening process begins after an applicant completes an OF-306. This normally occurs after the LOB/SO and AHR have determined that the applicant is eligible and best qualified for the position, but before a firm offer letter is issued. The OF-306 is used to identify potentially disqualifying issues. AHR has the responsibility to review the OF-306 to identify potentially disqualifying issues, before passing the case to the personnel security office for security processing.

**b.** The PSS begins the security review process once s/he receives all documents needed for security processing from AHR. The PSS will review the OF-306, for completeness, accuracy, and potential suitability issues. The PSS will first check the Central Verification System to determine whether the applicant has a completed background investigation, sufficient for the position that meets the reciprocity requirements outlined in Chapter 4 of this order.

**c.** If there is no prior investigation, the PSS will contact the applicant with instructions for completing investigative requirements, including the completion of a background investigation security questionnaire, submission of fingerprints, and the completion of a credit report release, if required for the position. The PSS will review the fingerprint check results, security questionnaire, and credit report, if required for the position, to determine whether the applicant can be placed into the position prior to the completion of all investigative requirements. This is referred to as an interim suitability determination.

**d.** If there are potential disqualifying suitability issues that cannot be satisfactorily mitigated, the PSS will advise AHR that the applicant is denied interim suitability, and cannot be placed into the position at this time. AHR, in consultation with the hiring LOB/SO, will advise the PSS if they still wish to consider the applicant. If the applicant is still to be considered, the

PSS will initiate the required investigation. A final suitability determination will be made when the completed investigation is received and adjudicated. If the completed investigation is favorably adjudicated, the applicant can be placed in the position. If the completed investigation cannot be favorably adjudicated, the case will be referred to AHR for a final suitability determination.

**e.** Pending criminal charges of a nature that could be potentially disqualifying cannot be adjudicated until there is a court disposition. The PSS must still afford the applicant an opportunity to refute the information, to protect against cases of mistaken identity, or erroneous information. If the applicant confirms that they are under pending criminal charges of a nature that could be potentially disqualifying, the applicant will be denied interim suitability.

**f.** In many cases, potentially disqualifying suitability issues are not evident until the required background investigation is completed, either while a person is still an applicant or after entering on duty. In such cases, the processing personnel security office will adjudicate the completed background investigation, as outlined in Section 7 below, and will refer these cases to AHR for a final suitability determination, as outlined in Section 8 below.

**7. Suitability Adjudication Process.**

**a.** All trained adjudicators from AXP and AHR must be thoroughly familiar with current laws, regulations, and criteria pertaining to suitability adjudication. Adjudicators should possess mature judgment, discretion, reliability, good analytical ability, strong writing skills, and objectivity.

**b.** The PSS must adhere to the suitability factors and criteria found in Appendix D when performing suitability adjudications.

**c.** The PSS must give applicants and employees an opportunity to explain, refute, or deny any unfavorable information obtained as the result of an investigation before taking any unfavorable action based on that information. This includes denying a benefit to which they would otherwise be entitled. This practice, known as due process, provides the subject the opportunity to present mitigating information that may be unknown to adjudicating officials, and also prevents the FAA from making errors that might otherwise result from mistakes in identity or erroneous information.

**d.** A PSS must adjudicate cases promptly in the interests of the FAA and the person involved. Adjudications should be completed within the timeframes established by the Suitability Executive Agent.

**e.** In accordance with standard operating procedures, all suitability adjudications will be documented with a written summary of all issues. The summary must include a rationale supporting the PSS's recommendation that the person's employment, or continued employment, would or would not promote the efficiency of the service. The final adjudicative action must be promptly recorded in ITS and reported to the ISP.

**8. Suitability Referrals.** AXP must refer any unfavorable suitability recommendations for employees or applicants to AHR for a final suitability determination. They must provide all documentation to AHR for their use in making the final suitability determination.

**9. Coordinating Personnel Security Information.** In accordance with applicable Systems of Records privacy protections:

**a.** FAA managers from all LOB/SOs must provide to their personnel security office any information they receive concerning employees under their supervision, or applicants for positions that would be under their supervision, which may affect their suitability for employment. The personnel security office will refer any potentially disqualifying suitability issues to the AHR Central Adjudications Office for a final suitability determination, if the employee is still in their probationary period.

**b.** Derogatory information received by the personnel security office on non-probationary employees through reinvestigations, Post-Appointment Arrest Notifications, notifications from the Office of Investigations, self-reporting, peer-reporting in accordance with SEAD 3 requirements, or any other source, may be referred to the AHR Labor and Employee Relations (LER) office for action for possible violations under the FAA Standards of Conduct. The personnel security office must provide the LER office with all investigative reports and other information necessary to enable officials to take appropriate action.

**c.** The personnel security office must forward to the responsible AAM office any information raising a question about a person's physical or mental fitness to perform a particular job, including information on drug and alcohol-related issues.

# Chapter 7. Security Clearance

## 1. Personnel Security Eligibility Standards and Criteria.

**a. Eligibility Standard.** AXP is responsible for making determinations of eligibility for access to CNSI. AXP must ensure that the granting of access to any person is clearly consistent with the national security interests of the U.S. AXP must assess past and present conduct and consider whether the granting of access conforms to this standard. Conduct relating to any of the criteria listed below is grounds for denying or revoking access to classified information if the conduct indicates the person would pose a risk of damage to national security. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by trained adjudicative personnel. Any doubt must be resolved in favor of national security.

**b. Criteria.** EO 12968 states that, with limited exceptions, "eligibility for access to classified information shall be granted only to persons who are U.S. citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the U.S., the 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." Eligibility for a security clearance will be determined based on current adjudicative guidelines.

**c. Restrictions.**

**(1)** In granting access to classified information, there must not be any discrimination against any person on the basis of race, color, sex, national origin, religion, age, disability, marital status, pregnancy, sexual orientation, gender identity, genetic information, or any other protected activity/class.

**(2)** No negative inference regarding an individual's eligibility for a security clearance may be drawn solely on the basis of their having received mental health counseling. Such counseling can be a positive factor in making eligibility determinations. However, a history of receiving mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the applicable security standards and criteria are satisfied, and mental health may be considered when it directly relates to those standards and criteria.

**2. Requesting a Security Clearance.** A manager in a LOB or SO requests a security clearance for an employee when the employee is in a position designated as non-critical sensitive, critical sensitive, or special sensitive; needs access to CNSI or classified systems, and the employee has a need to know. An employee cannot submit a request for a security clearance on their own behalf. Eligibility for access to classified information must 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 access to classified information may reasonably be prevented. Only when a manager demonstrates that a current employee has a foreseeable need

for access to classified information may the manager request a security clearance for an employee. The manager must justify this need as part of the request for clearance. The automated PDT must be used to ensure the change in duties supports a security clearance, as outlined in this chapter. The LOB/SO will submit the request to the responsible personnel security office via AHR. The level of security clearance that a person needs depends on the classification level of the information that the person needs to access (e.g., Top Secret or Secret).

**3. Security Adjudication.**

**a. Adjudicative Procedures and Guidelines.** The personnel security office will follow current National Security Adjudicative Guidelines, when determining eligibility for access to classified information. The ultimate consideration in making a personnel security eligibility determination is whether such a determination is clearly consistent with the interests of national security, and must be an overall evaluation based on all available information and the whole person concept. In addition, the personnel security office will adjudicate each background investigation within the timelines established by the SecEA, and will ensure that the employee meets the conditions listed below prior to granting a security clearance:

**(1)** U.S. Citizenship;

**(2)** Favorably adjudicated background investigation at the appropriate level;

**(3)** No open ROI or pending adverse action;

**(4)** Completed CNSI training; and,

**(5)** Signed SF-312.

**b. Due Process.** In the event that potentially disqualifying information is discovered during the course of the investigation, the personnel security office must give applicants and employees an opportunity to explain, refute, or deny this information before making an ineligibility determination. This includes denying a benefit to which the applicant or employee would otherwise be entitled. This practice, known as due process, provides the applicant or employee the opportunity to present mitigating information that may be unknown to adjudicating officials, and also prevents the FAA from making errors that might otherwise result from mistakes in identity or erroneous information.

**c. Referral of Counterintelligence Concerns to AXI-300.** The personnel security office must refer cases to the Advanced Threat Analysis & Mitigation Division, AXI-300, when they believe that a person has been coerced, influenced, or pressured to act contrary to the interests of national security; when significant questions are raised regarding a person's loyalty to the U.S; or when other counterintelligence concerns are identified.

**d. Special Access Authorizations.** Authorization for special categories of classified information, such as SCI and information related to SAP requires additional security review outside the scope of this Order. SCI access authorizations are processed under FAA Order 1600.76, Sensitive Compartmented Information (SCI) Program Management, and SAP access

authorizations in accordance with the access requirements established by the responsible SAP authority. For all requests for special access authorizations, the LOB/SO will:

**(1)** Work with AHR to have the position designation updated to reflect Special Sensitive; and,

**(2)** Submit a request for a special access authorization to AXP.

The personnel security office will:

**(1)** Ensure the position designation as Special Sensitive;

**(2)** Ensure the employee has a Top Secret clearance; and,

**(3)** Process the request and manage all aspects of the special access authorization.

**4. Temporary and One-Time Clearances.** Unless a manager provides adequate written justification that exceptional circumstances exist, the personnel security office must wait until the background investigation is complete and favorably adjudicated before granting a security clearance.

**a. Temporary Clearances.** In accordance with SEAD 8, Temporary Eligibility, interim access to classified information may be approved during exceptional circumstances when official functions must be performed, including meeting mission readiness requirements, before the completion of the investigation and adjudication processes.

**(1) Secret.** Temporary (i.e., interim) secret clearance requirements include the following:

- Written request from the LOB/SO with acceptable justification explaining the exceptional circumstances;
- Favorable review of a completed SF-86, Questionnaire for National Security Positions;
- Citizenship verification;
- Favorable review of credit report;
- Favorable review of a Federal Bureau of Investigation (FBI) fingerprint check;
- Initiation of the required background investigation; and
- Employee has completed CNSI training and signed an SF-312.

The personnel security office may not grant an interim Secret clearance if the review reveals unresolved derogatory information. Temporary security clearances are only valid within the FAA, unless another agency's personnel security office chooses to accept them based upon its own risk assessment, and may be terminated at any time if disqualifying information is received. Temporary Secret clearances must not be granted for more than one year, unless approved by AXP-1 or designee, and are only valid until the exceptional circumstances have abated, the access is terminated, or a final clearance is granted.

**(2) Top Secret.** Only the OST Office of Security, M-40, may grant a Temporary (i.e., interim) Top Secret clearance, and may do so only in exceptional cases. The personnel security office must forward all requests for interim Top Secret clearances to AXP-100. AXP-100 will forward the request to M-40, and notify the referring personnel security office of M-40's decision. Temporary Top Security clearance requirements include:

- Written request from the LOB/SO with acceptable justification explaining the exceptional circumstances;
- Favorable review of a completed SF-86, Questionnaire for National Security positions;
- Initiation of the required background investigation;
- Citizenship verification;
- Favorable review of a credit report; and
- Favorable review of a fingerprint check, FBI name check, and a National Crime Information Center check.

Temporary security clearances are only valid within the FAA unless another agency's personnel security office chooses to accept them based upon its own risk assessment, and may be terminated at any time if disqualifying information is received. Temporary Top Secret clearances must not be granted for more than one year, unless approved by M-40, and are only valid until the exceptional circumstances have abated, the access is terminated, or a final clearance has been granted.

**b. One-Time Clearances.** During exceptional circumstances, one-time access to classified information may be approved when it is determined to be in the national security interest. In accordance with DOT policy, which is more restrictive than SEAD 8, one-time clearances are limited to current security clearance holders only, and the access required is limited to classified information one level higher than the current clearance (i.e., there are no one-time clearances to the Secret level within DOT). One-time access is limited to individuals whose expertise offers specialized and important benefits and value to the U.S government or to individuals to whom access to classified information needs to be provided in the interest of national security. In addition, one-time access is limited to specific, identifiable classified information and is limited to information necessary to fulfill the national security requirement. LOB/SOs providing access to specific, identifiable classified information to individuals with one-time clearances must maintain appropriate records of such disclosures.

**(1) Request Requirements.** A written request from the LOB/SO, approved at the SES level, includes a statement of compelling need that addresses:

- The unique qualifications of the individual(s) and/or the unique circumstances that require divulging classified information;
- The expected benefit to the U.S. government and national security;
- The expected nature, extent, and level of access to classified information; and,
- Dates for which access is required.

Only M-40 may grant one-time access to the Top Secret level and does so only in exceptional cases. All requests for one-time Top Secret clearances must be sent to AXP-100. AXP-100 will forward the request to M-40, and notify the referring personnel security office of M-40's decision. One-time access approvals are only valid within the FAA unless another agency's personnel security office chooses to accept them based upon its own risk assessment, and may be terminated at any time without appeal. One-time access must be limited to the period needed to accomplish the national security requirement, may range from one to 30 calendar days, and maybe extended to 90 days with written approval from M-40.

**5. Suspension of a Security Clearance.** Whenever the personnel security office receives information that indicates an employee's access to CNSI may not be clearly consistent with the interests of national security, the personnel security office will suspend the employee's clearance until the matter is resolved and the employee's record is reevaluated for eligibility. Each decision to suspend requires the PSS to use their judgment on a case-by-case basis, using the Adjudicative Guidelines. Certain types of incidents require the immediate suspension of an employee's clearance until a reevaluation has been completed. By their nature, these types of incidents indicate that continued access to CNSI may not be clearly consistent with the interests of national security. These include, but are not limited to, the following:

- Positive test for an illegal drug, or admitted drug misuse while holding a security clearance;
- Any arrest while holding a security clearance that has the potential to impact eligibility to hold a national security position;
- Misconduct investigation having a nexus to national security;
- Failure to complete reinvestigation forms despite sufficient follow-up, including managerial notification;
- Failure to complete the training requirements of FAA Order 1600.2 (i.e., annual CNSI training) despite sufficient follow-up, including managerial notification; and,
- Any other incident that indicates the continued holding of a security clearance is not consistent with the interests of national security.

**a. Clearance Suspension Memorandum.** When a decision is made to suspend the employee's security clearance, the personnel security office will send a Clearance Suspension Memorandum to the employee through the employee's manager. This is done to ensure the employee's manager is aware of the clearance suspension. The Clearance Suspension Memorandum advises the employee and their manager that the suspension will remain in effect until further notice and that the suspension does not constitute an adverse action. The employee and the employee's manager must sign and date the Clearance Suspension Memorandum and return it to the PSS. The PSS will update all relevant databases to reflect the suspension.

**b. Letter of Inquiry (LOI).** If needed to resolve outstanding issues, the personnel security office will issue a LOI regarding the potentially disqualifying information. The employee has 15 calendar days from the date of the LOI to provide any mitigating information (e.g., court documents, financial records, etc.). (The personnel security office understands that some individuals may need more than 15 calendar days to acquire the necessary information and, if

they choose, seek legal counsel from their personal attorney. At least one extension of an additional 15 calendar days will be granted, if requested. Additional extensions will be considered upon request.) In some cases, prior to sending a LOI, the personnel security office may opt to have a supplemental investigation by the ISP, or an FAA internal investigation conducted to address the issue.

**c. Clearance Reinstatement.** A clearance suspension does not necessarily result in a revocation action; however, an employee's clearance will be reinstated only when the issues for which the clearance was suspended are resolved (e.g., allegations are disproved, the court process is completed, issues have been mitigated). If the employee is able to resolve the issue(s) for which their clearance was suspended, the personnel security office will reinstate the clearance. If appropriate, the PSS may also issue an Advisory Letter, which advises the employee that, while their clearance is being reinstated, the receipt of derogatory information in the future may lead to reconsideration of this determination up to or including revocation of their clearance.

**d. Conditional Clearance Memorandum.** The personnel security office also has the option of issuing a Conditional Clearance Memorandum to the employee prior to reinstating their clearance, if the issue(s) for which their clearance was suspended does not rise to the level of warranting a clearance revocation, per the Adjudicative Guidelines. A Conditional Clearance Memorandum informs the employee that the issues have been mitigated, at that time, but that receipt of derogatory information in the future may lead to a clearance revocation. The Conditional Clearance Memorandum includes specific conditions that an employee must meet in order to maintain their clearance and may include regular follow-up with AXP.

**6. Denial or Revocation of a Security Clearance.** A person must meet, and continue to meet, eligibility standards for access to classified information to obtain initial eligibility, and maintain continued eligibility, for access to classified information. Whenever information is received that indicates a person's access to classified information may not be consistent with the interests of national security, the personnel security office will evaluate the information against the Adjudicative Guidelines to determine initial or continued eligibility. The authority to deny or revoke a security clearance lies with ASH-1.

**a. Process to Deny or Revoke a Security Clearance**.

**(1) Clearance Suspension.** As soon as the personnel security office becomes aware of derogatory information that may require revocation of the security clearance, the personnel security office will suspend the security clearance, as described in Section 5(a) above. The personnel security office cannot move forward with a revocation action if the security clearance has not been suspended.

**(2) Letter of Inquiry (LOI).** In most cases the personnel security office will issue the subject a LOI regarding the incident or activity that raises concerns, as described in Section 5(b) above.

**(3) Recommendation and AXP-100 Determination.** If the personnel security office recommends a denial or revocation, they will forward their recommendation and all supporting

documentation to AXP-100 for review and concurrence. AXP-100, or designee, will review the information and assess the soundness of the proposed denial or revocation.

**(4) Notice of Intent to Deny or Revoke.** If AXP-100 concurs in the proposed denial or revocation, they will send a Notice of Intent to Deny or Revoke to the subject, informing them of the intention to deny or revoke, and identifying the specific issues of concern. The Notice of Intent is signed by ASH-1, and advises the subject that they have:

(a) 30 calendar days from the date of the Notice to submit a written response to ASH-1, with any supporting documentation, and that they may also request the opportunity to appear in person;

(b) The right to be represented by counsel, or other representative, at their own expense;

(c) The right to request any documents or records upon which the decision is based; and,

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

**(5) Subject Response.** AXP considers all timely responses and any supporting documentation submitted before recommending a final decision. If the subject fails to mitigate the issues, or does not respond to the Notice of Intent to Deny or Revoke within the required timeframe, the denial or revocation becomes final. AXP will inform the subject of this decision via a Notice of Final Determination to Deny or Revoke Security Clearance.

**(6) Notice of Final Determination to Deny or Revoke.** The Notice of Final Determination letter will provide the subject with an explanation for the denial or revocation and inform them of their right to appeal the decision in accordance with this order and 49 C.F.R. Part 8. AXP sends the Notice of Final Determination letter to ASH-1 for consideration and, if ASH-1 concurs with the denial or revocation of the security clearance, for the signature of the letter.

**b. Post Denial or Revocation.** Following the denial or revocation of a security clearance, the referring personnel security office enters the determination into the Personnel Investigations Processing System/Clearance Verification System and ITS to reflect the final decision.

**(1)** Appeal to the Department of Transportation.

(a) The DOT Personnel Security Review Board. EO 12968, Section 5.2(a)(6), provides every applicant or employee whose security clearance is denied or revoked an opportunity to appeal in writing to a high-level panel appointed by the relevant agency (i.e., DOT, in the case of FAA applicants and employees). The Secretary of Transportation chartered the Personnel Security Review Board (the Board) to fulfill this requirement. The Board adjudicates final appeals originating in any DOT organization regarding decisions to deny or revoke access to classified information. The Board's membership is described in 49 C.F.R. § 8.25 and in DOT Order 1630.2, which also sets forth the procedures of the Board.

(b) Status During Appeal. An appeal to the Board does not halt the decision that is being appealed. However, no adverse personnel action based on the denial or revocation of a security clearance can be proposed or taken against the subject prior to the expiration of the 30-day period in which the subject can appeal the denial or revocation and until any appeal is decided by the Board.

**(2) Informing interested parties**. If the Board upholds FAA's decision, or the subject does not file an appeal within the appeal period, the responsible personnel security office will make appropriate notifications. For existing employees, the employee's manager will be notified that the employee can no longer occupy a sensitive position. It is the responsibility of the LOB/SO and AHR LER to ensure that the employee is removed or, if appropriate, permanently reassigned to a position within FAA that does not require a security clearance (i.e., a public trust position). For applicants, the responsible personnel security office will notify AHR that the applicant cannot be placed into a sensitive position. AXP will provide AHR, and the LOB/SO, all information necessary to take appropriate action. AHR must inform AXP of any action resulting from the clearance revocation or denial (ex. removal, reassignment to a non-sensitive position, non-selection, etc.).

**(3) SF-312 Debrief Acknowledgment.** The personnel security office, in coordination with the employee's manager, must ensure that the employee signs the Debrief Acknowledgment section of the SF-312. The manager must witness the employee's signature and return the SF-312 to the personnel security office.

**c. Subsequent Applications for Clearance.** If ASH denies or revokes a security clearance, it is general practice that ASH will not consider a new application for a security clearance from that person for a minimum of 12 months after the date of the final denial or revocation. At that time, the person must provide evidence that the issues for which the security clearance was denied or revoked no longer exist before the request will be taken under consideration.

**7. 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 may be employed at FAA without prior approval of the Secretary of Transportation, and determination by the servicing human resources organization that the factors leading to the separation are not currently disqualifying for FAA employment. When employment of such a person is proposed, the responsible personnel security office, must:

**a.** Obtain complete information regarding the basis for separation;

**b.** Ensure appropriate investigation of the person's subsequent activities;

**c.** Ascertain whether AHR has determined that the person is suitable for FAA employment;

**d.** Obtain any other information the Secretary of Transportation needs to decide whether or not the person's employment is consistent with the interests of national security; and,

**e.** Forward this information to M-40 for approval by the Secretary. The Secretary's approval authority has not been re-delegated.

**8. Administrative Withdrawal of a Security Clearance.** An administrative withdrawal is not an adverse action. It has no negative implications for the employee. The personnel security office administratively withdraws a clearance when an employee no longer needs it due to a change in duties or responsibilities, expiration of a temporary clearance, transfers to a non-sensitive (public trust) position, or separates from the Agency. It is the responsibility of the LOB/SO to inform the personnel security office, through AHR, when an employee no longer needs clearance for one of the listed reasons. Upon receipt of this information, the personnel security office will update all pertinent databases, and will contact the employee to sign the Debrief Acknowledgment section of the SF-312.

**9. Administrative Downgrade of a Security Clearance.** The personnel security office administratively downgrades a clearance when an employee no longer needs the higher level clearance (e.g., Top Secret) but still requires a lower level clearance (e.g., Secret) due to a change in duties or responsibilities or transfer to a less sensitive position. An administrative downgrade is not an adverse action. The personnel security office will notify the employee when the downgrade occurs.

**10. Responsibilities for Security Clearance Holders and Those Occupying Sensitive Positions.**

**a.** Properly handle and protect CNSI.

**b.** Complete annual CNSI training. Failure to complete the training by the given due date may result in re-evaluation of eligibility to occupy a sensitive position and suspension of the clearance, if applicable.

**11. Reporting Requirements for Clearance Holders and Those Occupying Sensitive Positions.**

**a.** All individuals with access to CNSI, or who occupy a sensitive position, are subject to reporting requirements outlined in Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access Classified Information or Who Hold a Sensitive Position.

**b.** Individuals with Access to Secret Information, or holding a Non-Critical Sensitive Position, are required to report the following:

**(1)** Unofficial foreign travel;

**(2)** Unofficial contact with a known or suspected foreign intelligence entity;

**(3)** Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact, or any contact with a foreign national that involves the exchange of personal information. (This reporting requirement is based on the nature of the relationship, regardless of how or where the foreign national contact was made or how the relationship is maintained [i.e., via personal contact, telephonic, postal system, Internet, etc.]. The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement listed. Following initial reporting, updates regarding continuing

unofficial association with known foreign nationals are required only if and when there is a significant change in the nature of the contact.)

**(4)** Application for and receipt of foreign citizenship;

**(5)** Application for, possession of, or use of a foreign passport or identity card for travel;

**(6)** Attempts by any person at elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure, regardless of means;

**(7)** Media contacts, other than for official purposes, where the media seeks access to classified information, or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported;

**(8)** Arrests;

**(9)** Bankruptcy or over 120 days delinquent on any debt; or

**(10)** Alcohol and drug-related treatment.

**c.** Individuals with Access to Top Secret Information, or Holding a Critical or Special Sensitive Position, are required to report the following:

**(1)** Unofficial foreign travel;

**(2)** Unofficial contact with a known or suspected foreign intelligence entity;

**(3)** Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact, or any contact with a foreign national that involves the exchange of personal information. (This reporting requirement is based on the nature of the relationship, regardless of how or where the foreign national contact was made or how the relationship is maintained [i.e., via personal contact, telephonic, postal system, Internet, etc.]. The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement listed. Following initial reporting, updates regarding continuing unofficial association with known foreign nationals are required only if and when there is a significant change in the nature of the contact.)

**(4)** Direct involvement in foreign business;

**(5)** Foreign bank accounts;

**(6)** Ownership of foreign property;

**(7)** Application for and receipt of foreign citizenship;

**(8)** Application for, possession of, or use of a foreign passport or identity card for travel;

**(9)** Voting in a foreign election;

**(10)** Adoption of non-U.S. citizen children;

**(11)** Attempts by any person at elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information, or other information specifically prohibited by law from disclosure, regardless of means;

**(12)** Media contacts, other than for official purposes, where the media seeks access to classified information, or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported;

**(13)** Arrests;

**(14)** Financial Anomalies: Including, but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater, such as an inheritance, winnings, or similar financial gain;

**(15)** Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days;

**(16)** Cohabitant(s);

**(17)** Marriage; or

**(18)** Alcohol and drug-related treatment.

**d. Reportable Actions by Others.** Individuals covered under SEAD 3 also have a responsibility to report the following activities of other individuals covered under SEAD 3:

**(1)** An unwillingness to comply with rules and regulations or to cooperate with security requirements;

**(2)** Unexplained affluence or excessive indebtedness;

**(3)** Illegal use or misuse of drugs or drug activity;

**(4)** Alcohol abuse;

**(5)** Apparent or suspected mental health issues where there is reason to believe it may impact the employee's ability to protect classified information, or other information specifically prohibited by law from disclosure;

**(6)** Criminal conduct;

**(7)** Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security; or

**(8)** Misuse of U.S. Government property or information systems.

**e. Reporting Method.** All unclassified reporting is accomplished through the online SEAD 3 Reporting Tool. Please contact 9-ASH-AXP-SEAD3@faa.gov for further guidance if a classified report is necessary.

**f. Resources.** The SEAD 3 directive, frequently asked questions, a listing of all reportable issues, and the online SEAD 3 Reporting Tool are all available on the MyFAA SEAD 3 webpage.

**12. Classified Visit Control (Security Clearance Verification)**

**a. Classified Visits by FAA Employees.** If an FAA employee needs to have their security clearance certified to conduct business with another government agency or government contractor facility, the employee must submit DOT Form 1630.5 Visit Clearance, in advance of the visit, to their personnel security office. Upon receipt of the request, the personnel security office will forward certification of the employee's clearance to the point of contact for the location to be visited. Security clearance verifications contain PII and must be handled and transmitted in accordance with FAA Order 1600.75 and FAA Order 1370.121. The clearance should never be passed directly to the employee; it must go from the personnel security office directly to the receiving agency's security office.

**b. Classified Visits to FAA by Personnel of Other Agencies.** A visitor to the FAA must arrange for their employing agency or contractor facility to certify their security clearance to the FAA personnel security office before visiting for a classified meeting.

**c. Classified Visits by FAA Contractors.** FAA contractor employees who are providing support on classified contracts are granted a security clearance by the DCSA. The contractor notifies the personnel security office when a contractor employee holds a security clearance. The certification for contractor employee security clearances comes from the contractor on their letterhead. The certification can be used for no more than one year from the date of the letter to enable FAA to certify contractor employee security clearances when required in support of Agency business. This information must be updated once a year from the contractor to the personnel security office.

**d. North Atlantic Treaty Organization (NATO) Visits by FAA Employees.** Access by FAA personnel to NATO-classified information requires special authorization. The Central U.S. Registry 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-classified information is contained in DOT Order 1642.2/MAO 280-4.

**(1)** NATO information and material must be protected at the same level as the corresponding level of U.S. CNSI, but with enhanced security measures that provide compartmentalization.

**(2)** A request for authorization for access to NATO-classified information must be initiated by an employee's manager, or other management official, who can attest to the official

need. The request must specify the level of NATO information to which the employee will need access. NATO uses the terms 'NATO Secret' and 'Cosmic Top Secret' to classify their clearance levels. The employee must have a collateral clearance of either Secret or Top Secret in order to obtain a NATO Secret or Cosmic Top Secret, respectively. If an FAA employee has never attended a NATO function, they will need to be NATO indoctrinated, per the NATO Security Regulation Requirements. The responsible personnel security office must have the subject read the NATO Security Briefing, complete the NATO Briefing Certificate, and return the certificate to the personnel security office.

**(3)** The personnel security office will forward the completed NATO briefing certificate to the MARAD Security Officer for issuance of a NATO access authorization specifying the level of access. MARAD will communicate the level of access approved to the Department of State's (DOS) Security Office.

## Chapter 8. Personnel Security for Contractor Employees and Non-Employees

**1. General.** This chapter provides policy and procedures for the Personnel Security Program as it relates to FAA contractor employees and non-employees. It applies to contractor employees who have access to FAA facilities, systems, SUI, resources, and/or CNSI, and other persons, referred to as non-employees, who have similar access by agreement with the FAA (e.g., consultants, military liaisons, credit union workers, childcare center employees).

**2. Background.** Many contractor employees and non-employees support the FAA mission. Based on their FAA affiliation, the extent of their responsibilities, and the risk levels of the positions they occupy, FAA investigates contractor employees and non-employees who have such access by agreement with an FAA LOB/SO, to determine their suitability for access to FAA facilities, systems, resources, SUI, and/or CNSI, as applicable.

**3. Policy.**

**a.** Except as stated in this chapter, personnel security program requirements and procedures applicable to FAA employees also apply to contractor employees and non-employees who have comparable access to the Agency's facilities, systems, SUI, CNSI, and/or resources. References to an employee's supervisor will be construed as referring to the COR in the case of a contractor employee, unless otherwise specified elsewhere in this order.

**b.** FAA requires background investigations on all contractor employees and non-employees, unless they are exempted in accordance with Section 6(c) of this chapter, as determined by the Federal Investigative Standards and the position's risk level. These investigations will serve as the basis for a suitability determination.

**c.** FAA will not allow a person to work under a contract unless they have been granted a favorable interim or final suitability determination.

**d.** Trained PSSs will adjudicate contractor employee and non-employee background investigations using procedures established by 5 CFR Part 731.

**e.** Contractor employees are expected to maintain high standards of conduct. Receipt of derogatory information during a contractor employee's work on an FAA contract may result in the contractor employee being found unsuitable to continue work on the contract, and removal from the contract.

**f.** No contractor employee, or applicant for contractor employment, will be denied access to FAA facilities, systems, SUI, CNSI, or resources, or removed from an FAA contract, because of information revealed in a background investigation, or during the period of performance of the contract, unless they have been given an opportunity to respond to any information used as a basis for such action. EXCEPTION – if the contractor employee's continued access to FAA facilities, systems, SUI, CNSI or resources, poses a threat to the safety or security of the FAA or its employees, with approval by an AXP manager, access can be suspended, pending the completion of an inquiry.

**g.** No contractor employee, who is not a U.S. citizen, can work or provide services or goods under FAA contracts within the U.S., unless they have resided in the U.S. for three years, except if they are exempt from the investigative requirements in Section 9(d), or a waiver of this requirement is requested and approved by AXP-1 (or designee), prior to contract award, or prior to the individual beginning work.

**h.** Contracts requiring contractor employees to have access to CNSI will be prepared and processed according to the procedures of NISPOM and FAA Order 1600.2.

**4. Procurement Reviews.**

**a.** COs must ensure that all solicitations, contracts, purchase orders, lease agreements, and similar agreements that will require a contractor employee to have physical or logical access to FAA facilities, systems, SUI, resources, and/or CNSI, are sent to the PSS during the pre-award stage. The SOW and PDTs must be included in the package for PSS review. Procurement actions with no investigative requirement do not need to be sent to the PSS for review.

**b.** The PSS must review all procurement actions in a timely manner. The PSS must ensure PDTs have been properly completed and designations are correct and appropriate and that a PDT has been completed for each labor category included in the contract. The PSS must consider the extent of access contractor employees will have to CNSI, SUI, FAA systems, FAA resources, and FAA facilities when determining whether the position designation indicated is appropriate for the contract. If the PSS does not agree that the designation is appropriate for the position described, the PDT will not be approved. The PSS must advise the preparer of this determination and the reason for the determination. The LOB/SO can either resubmit the PDT to show an appropriate designation, or provide additional justification for the position designation sought.

**c.** The PSS must also ensure that the solicitation package contains all required security clauses, and that the clauses are the most current version. To ensure security clauses are accurate and up-to-date, access the contract clause page at https://fast.faa.gov/contractclauses.cfm.

**d.** The PSS must contact and coordinate with the Information Safeguards Division, AXF-200, upon notification that a contract or other agreement may require access to CNSI.

**e.** The PSS must return a written record of the review results to the CO and document all review actions in the Contractor Security File.

**f.** The AAQ component must ensure that all amendments, modifications, revisions, and renewals of existing contracts, purchase orders, lease agreements, and other agreements are sent to the personnel security office for review. This requirement does not apply to contracts, POs, and agreements with no security requirements, or to changes that do not affect the security posture of the contract or agreement. For changes that do affect the security posture, the AAQ component must also submit new PDTs if any positions are affected by the change.

**g.** The AAQ component must notify the PSS of all expired contracts or contracts that were renewed under a new contract number.

**5. Designating Position Risk Levels.**

**a.** The LOB/SOs must coordinate with the CO to determine the appropriate risk designation for all contractor positions requiring access to FAA facilities, systems, SUI, resources, and/or CNSI. LOB/SOs must use OPM's Position Designation System and PDT to ensure positions are designated uniformly and consistently. The tool is available at https://www.dcsa.mil/is/pdspdt/. The LOB/SO must also maintain documentation as to how the risk levels of contractor employee positions were determined. Contract companies are not authorized to complete the PD Tool.

**b.** LOB/SOs and COs do not need to provide a PDT for contracts, POs, lease agreements, etc., that do not have a background investigation requirement.

**c.** The PSS is responsible for reviewing and approving all position designations. If the PSS determines that the information provided on the PDT is not accurate or appropriate for the position described, the form will not be approved. The PSS must advise the preparer of this determination and the reason for the determination. The LOB/SO can either resubmit the PDT to show an appropriate designation has been made, or provide additional justification for the risk/sensitivity level sought.

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

**6. Investigative Requirements and Exceptions for Contractor Employees.**

**a.** Except as provided in (c) below, contractor employees are subject to the same investigative requirements, based on the risk/sensitivity level of their position, as FAA employees, which are outlined in Chapter 4, Personnel Security Investigative Requirements. The minimum background investigation for a contractor employee is a Tier 1 investigation.

**(1) Contractor employees requiring access to CNSI.** Contractor employees who require access to CNSI are investigated by the Department of Defense under the National Industrial Security Program. These individuals are not required to undergo additional investigation by the FAA.

**b.** Reciprocity policies, outlined in Chapter 4, Section 5, also apply to contractor employees.

**c.** Certain contractor positions are exempt from the investigative requirements. Contractor employees exempt from investigative requirements must not have access to classified information or restricted areas or be issued a Personal Identity Verification (PIV) card. For badging options, please see FAA Order 1600.78, PIV Card and Other Identification Cards. Exempt positions include:

**(1) Contractor employees with no access.** Contractor employees who have no access to FAA facilities, CNSI, SUI, systems, or resources, have no investigative requirement. This includes contractor employees under full escort.

**(2) Construction workers.** Construction workers doing work on new construction for a non-commissioned FAA facility are not required to undergo an investigation, unless the construction is co-located within an existing FAA facility.

**(3) Delivery personnel and repair technicians.** Contractor employees in this category are exempt from any investigative requirement, even if they are working under an FAA contract for an extended period of time. However, they have to comply with facility visitor procedures, as described in FAA Order 1600.69, Facility Security Management Program.

**d.** No contractor employee with an investigative requirement can begin working on a contract, unless the contractor employee has been granted interim or final suitability by the personnel security office.

**7. Investigative Requirements and Exceptions for Non-Employees.**

**a.** Persons who are neither FAA employees nor contractor employees, but have access to FAA facilities, systems, SUI, CNSI, or resources, will be investigated at the same level as an employee or contractor employee with similar access. These non-employees include, but are not limited to, consultants, military liaisons, credit union workers, and interns. For badging options, please see FAA Order 1600.78.

**b.** Non-employees whose physical access can be restricted to a specific area of a facility, and who do not need logical access to FAA systems, are exempt from the normal investigative requirement. However, this exception does not preclude an investigation of the person under the normal investigative requirement to allow for unrestricted physical access. These individuals include, but are not limited to, childcare parents, carpoolers, concessionaires, and fitness center employees. At a minimum, exempted non-employees must have a favorably adjudicated Special Agreement Check (SAC). Exempted non-employees will be subject to a new SAC every three years. Non-employees exempt from investigative requirements must not have access to classified information, SUI, restricted areas, FAA systems, or be issued a PIV card. For badging options, please see FAA Order 1600.78.

**8. Additional Investigative Requirements for Childcare Workers.**

**a. Requirements**. Childcare workers hired or contracted by the federal government are subject to the investigative requirements of 34 U.S.C. § 20351. Under the provisions of this law, childcare workers must undergo a background investigation based on an FBI fingerprint check and checks of each State's criminal history records for which an employee lists a current or former residence. Under 34 U.S.C. § 20351(c), any conviction for a sex crime, an offense involving a child victim, or a drug felony, may be grounds for denying employment or for dismissal of a childcare worker. In the case of an incident in which an individual has been charged with one of those offenses, when the charge has not yet been disposed of, the childcare worker may be suspended from having any contact with children while on the job until the case is resolved. Conviction of a crime other than a sex crime may be considered if it bears on an individual's fitness to have responsibility for the safety and well-being of children.

**b. Applicability.** The provisions of this section apply to any persons working or applying to work, in an FAA-sponsored childcare center, or who provide childcare services to persons under the age of 18 as part of any FAA-sponsored activity.

**c. Policy.**

**(1)** All childcare workers require a Tier 1 investigation with State Criminal History Repository extra coverage indicated in the investigation request.

**(2)** The PSS will provide the childcare worker applicant with a supplemental questionnaire regarding the disqualifying offenses outlined in Section 8(a) above, prior to making an interim suitability determination.

**(3)** No childcare worker may begin work until they have been granted interim suitability by the personnel security office.

**(4)** Childcare workers who are granted interim suitability to begin work must also be under continuous supervision, pending the completion of their background investigation.

**(5)** PSSs will provide Interim Suitability Determination notifications in writing to the National Child Development Program Manager, AHF-300, and will include instructions regarding the need for continuous supervision. PSSs will also send a Final Suitability Determination notification in all cases once the investigation has been completed and adjudicated, and the childcare worker is no longer required to work under continuous supervision.

**(6)** PSSs must afford a childcare worker applicant due process by providing them an opportunity to address any unfavorable information.

**(7)** PSSs will adjudicate childcare worker investigations using the same suitability standards and criteria used for FAA applicant, employee, and contractor employee investigations.

**(8)** PSSs will not disclose to the childcare director, or any official of a private entity, the specific reasons for any suitability determination.

**(9)** Childcare workers cannot appeal a suitability determination.

**9. Adjudicating Investigations.**

**a.** The provisions of Chapter 6, Personnel Suitability Standards, Criteria, and Adjudication, also apply to contractor employee and non-employee adjudications.

**b.** Before FAA denies a contractor employee or non-employee access to its facilities, systems, resources, SUI, and/or CNSI because of information received as the result of an investigation, or during the period of performance of the contract, the PSS must provide the contractor employee or non-employee due process. This consists of notifying the contractor employee or non-employee of the information being considered, and affording an opportunity to

respond to the information, prior to making a final determination. (EXCEPTION – upon written request from a Labor and Employee Relations Manager or from a Threat Assessment Team, access may be suspended, pending the completion of the inquiry.) The contractor employee or non-employee will be notified in writing of the derogatory issues. The PSS will explain the unfavorable information, provide the contractor employee or non-employee an opportunity to respond, and consider any information provided in response, before making a final suitability determination. Contractor employees and non-employees cannot appeal a suitability determination.

**c.** When providing due process and adjudicating investigative results, the PSS must communicate directly with the individual contractor employee or non-employee. The PSS must not disclose to the contractor employee's employer, or FAA contracting or management officials, the information contained in an investigation on an individual contractor employee, or the specific reason(s) for any suitability determination, unless authorized by law.

**10. Foreign Nationals as Contractor Employees and Non-Employees.**

**a. Investigative Requirements at US Locations.** Foreign nationals legally authorized to work in the U.S. may work as FAA contractor employees on unclassified contracts, and may have access to FAA facilities, systems, and resources, and, if they meet the applicable access requirements, and SUI. The following conditions apply:

**(1)** The immigration status of the individual must be verified through the Department of Homeland Security Systematic Alien Verification for Entitlements system, or any successor system.

**(2)** The individual has resided within the U.S. for a minimum of the last three years, or a waiver for this requirement has been requested and approved by AXP-1.

**(3)** The appropriate background investigation, based on the position's risk level, can be accomplished.

**(4)** All investigative requirements for an interim or final suitability determination have been completed and favorably adjudicated.

**b. Investigative Requirements at Foreign Locations**.

**(1)** Foreign nationals not residing in the U.S., but working for a foreign entity and supporting FAA contracts outside the U.S., are exempt from the investigative requirements of Section 11(a) of this chapter that apply to U.S. locations, unless they have access to FAA facilities, systems, resources, and/or SUI. If they do have any of the foregoing types of access, the PSS must initiate a Tier 1 investigation, if possible. In most cases, the ISP will not be able to conduct a Tier 1 investigation, unless the foreign national is, or has been, residing in the U.S. If a Tier 1 investigation cannot be conducted, the PSS may honor an equivalent background investigation, if it includes a fingerprint check against the FBI criminal history database, an FBI name check, and a name check against the Terrorist Screening database. Additional checks may be conducted, as appropriate. If a Tier 1 investigation cannot be conducted and an equivalent

background investigation cannot be verified, then the sponsoring FAA LOB/SO must ensure that the foreign national is escorted at all times.

**(2)** Foreign nationals working as contractor employees at FAA locations overseas are exempt from the requirement to have resided in the U.S. for at least the last three years.

**c. Procedures for Requesting a Residency Waiver.** A LOB/SO or CO, in consultation with the PSS, can submit a written request for waiver of the three-year residency requirement to AXP-2, through their personnel security office. The request must contain:

**(1)** A detailed justification of the reason for the waiver request;

**(2)** A copy of a completed PDT for the position;

**(3)** The name, date of birth, place of birth, and country of citizenship of the individual under consideration;

**(4)** Any supporting residency status documentation;

**(5)** Identity of the LOB/SO, organization, or office by routing symbol and title, the physical location(s) where the individual will be working, and the extent of time he or she will be at that location; and

**(6)** Name of contractor and contract number, if applicable.

**(7)** AXP-2, or his or her designee, will advise the responsible personnel security office or PSS whether the waiver has been approved. The PSS will notify the LOB/SO or CO, as soon as practical, of the decision.

**d. Restrictions.** In any situation where the LOB/SO or AXP determines that it is in FAA's best interest to restrict access or work under a contract to U.S. citizens only, the appropriate contract or other agreement must contain a clause specifying that restriction. In determining whether or not to apply this restriction, the CO and LOB/SO, in consultation with AXP, must consider the nature and extent of access necessary to perform the contract, particularly in regard to SUI. They must also ensure appropriate legal review of any contract applying this restriction by the Office of the Chief Counsel's Acquisitions and Fiscal Law Division, AGC-500.

**e. Export Control.** Working with, giving information to, or training a foreign national, even if the activity occurs in the U.S., could be considered an export (also known as a deemed export), and is subject to export control requirements. Certain exports, such as hardware, software, or information involving encryption technology, primary radar, GPS technology, maintenance hardware and/or services, and commercial space technology, are more tightly controlled. Potential transactions and disclosures must be legally reviewed to determine whether they are eligible for export. See FAA Order 1240.13, FAA Export Control Compliance, the Department of Commerce's Export Administration Regulations, the Department of State's International Traffic in Arms Regulations, and the Department of the Treasury's Office of Foreign Assets Control's regulations for possible restrictions. Consult with FAA's Office of the Chief Counsel, Acquisition and Fiscal Law Division, AGC-500, for legal review and advice.

**11. Classified Contracts.**

**a.** All contracts requiring access to CNSI must be processed in compliance with the National Industrial Security Program (NISP), per EO 12829 and 32 CFR Part 2004. The NISP classified contracting process ensures only properly cleared contractor entities and contractor employees can conduct classified work for the FAA under contract.

**b.** FAA Order 1600.2 contains requirements and procedures for processing classified contracts.

**c.** The Information Safeguards Division, AXF-200, provides oversight of classified contract activities throughout all contract phases. The PSS must coordinate with AXF-200 upon being notified by a CO that a contract may require access to CNSI.

**d.** Classified contracts must:

**(1)** Be prepared in accordance with the requirements in the NISPOM and FAA Order 1600.2;

**(2)** Include a completed Contract Security Classification Specification (DD Form 254), approved in writing by the manager of the Information Safeguards Division, AXF-200, or designee, and the CO;

**(3)** Include the appropriate security clause relating to classified contracts; and

**(4)** Identify the tasks to be performed requiring access to CNSI in the contract SOW.

**e.** The CO must also submit to their personnel security office for review a PDT, identifying the position sensitivity levels for each position, or labor category, for the classified contract.

**f.** Any contractor, or prospective contractor, requiring access to CNSI must have a valid Facility Clearance issued by the DCSA. The responsible CO must obtain verification in writing from AXF-200, or designee, that the contractor possesses a valid Facility Clearance prior to disclosing any CNSI at any stage of the contracting process.

**g.** FAA does not initiate background investigations for contractor employees on classified contracts, i.e., contracts requiring access to CNSI for their performance. Background investigations for contractor employees requiring access to CNSI are processed by the contractor through DCSA. Upon award, the contractor's Facility Security Officer must submit to the personnel security office a Visit Access Request (VAR), containing security clearance information, for each contractor employee who will be working on the classified contract. Upon receipt of the VAR, the PSS will confirm the security clearance information through centralized databases before authorizing the contractor to begin work on the contract. The PSS must update ITS with the investigation information and upload the VAR into the contractor's record. The PSS is not required to initiate any additional investigation. However, if the PSS cannot confirm that the contractor has met the investigative requirement for a PIV card, then the PSS must initiate an additional investigation.

**h.** The contractor must submit to the personnel security office new VARs annually, or when changes occur to contractor employee personnel security clearances.

**i.** Background investigations for contractor employees on classified contracts who will not have access to CNSI will be processed by the personnel security office.

**12. Records.** The personnel security office that reviewed the contract must establish a Contract Security File (CSF) for each contract that has a security requirement. The CSF will contain the PDTs, SOWs, security clauses, and modifications that affect the security posture of the contract, and any other significant documents relating to the contract.

Personnel Security Files for each contractor employee will be established and maintained in accordance with Chapter 5.

## Chapter 9. Limited Access Authorizations for Non-United States Citizens

**1. General.** Non-U.S. citizens are not eligible for FAA security clearances. When there are compelling reasons to grant access to classified information to a non-U.S. citizen in furtherance of a FAA mission, such individuals may be granted a limited access authorization (LAA) by the DOT Office of Security, M-40, under the following conditions:

**a.** The LAA determination must be made only by the Director, Office of Security, M-40, Office of the Secretary, and may not be further delegated.

**b.** The LAA will be limited to the Secret and Confidential level only; LAAs for Top Secret are prohibited.

**c.** Any access to classified information by non-U.S. citizens may only be permitted in accordance with applicable law, including 32 C.F.R. Part 2001, and policies. In particular, please refer to 32 C.F.R. § 2001.55, which specifically addresses foreign disclosure of classified information.

**d.** Access to classified information by non-U.S. citizens must be limited to information relating to a specific program or project.

**e.** Favorable completion of a background investigation. Such an authorization may be approved only if the prior ten years of the person's life can be appropriately investigated. Individuals granted LAAs under the foregoing provisions are subject periodic reinvestigations or continuous vetting, as applicable.

**f.** Security clearances previously issued to immigrants who have not become naturalized U.S. citizens will be reissued as LAAs, except as otherwise provided in this order. Immigrants who are eligible for U.S. citizenship, and have not applied for naturalization within 12 months of eligibility, will not be considered for an LAA.

**g.** The LAAs will be limited to persons who have a special skill or technical expertise essential to national security that is not available from U.S. citizen personnel. The request must clearly describe the nature of the classified information involved and state the level of classification. The requesting office must clearly show that 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.

**h.** LAAs will not be granted to secretarial or clerical personnel, or to others who perform routine administrative duties.

**i.** Non-U.S. citizens are not eligible for access to any higher level of classified information than the U.S. government has determined may be released to the government of the country of which the person is currently a citizen.

**2. Procedures for Limited Access Authorizations.** Personnel security offices must forward any LAA requests received to M-40 for processing. All persons granted LAAs by M-40 will be subject to the same security training, briefing, and debriefing requirements as security clearance holders.

**3. Approval for Visits by Foreign Nationals Cleared by Other Agencies.** No FAA office will accept security clearances, or LAAs or similar authorizations, for foreign nationals granted by other U.S. government departments or agencies for visits, conferences, or other purposes, without prior approval from M-40. The office involved must present justification to, and request approval from, M-40, through their local personnel security office.

# Chapter 10. Foreign Assignments and Travel

**1. General.** Special safeguards are required to protect national security when FAA employees, contractor employees, or non-employees are given foreign assignments, or perform official foreign travel. (Note: Only FAA employees receive foreign assignments.) For this purpose, a foreign location means outside the 50 states, the District of Columbia, and any of the United States' possessions and territories. The investigative requirements and security precautions specified in this chapter apply to all employees, contractors, or non-employees on foreign assignments or travel. FAA employees assigned to, or FAA employees, contractor employees, or non-employees on official travel in, a foreign country must exercise good judgment at all times to ensure that they do nothing contrary to the interests of the U.S. or the FAA. Officials authorizing the travel are responsible for ensuring that each traveler possesses the good character and reliability needed for the assignment.

**2. Investigative Requirements.**

**a. Foreign Assignments.**

**(1)** An FAA employee serving in a foreign duty location is assigned to the U.S. diplomatic or consular mission in the country of residence. To comply with DOS regulations, all employees assigned to a U.S. diplomatic or consular mission through a permanent change of station must hold at least a Secret clearance.

**(2)** All foreign assignment positions must be designated at least non-critical sensitive. Personnel selected for these positions must have a completed and favorably adjudicated investigation, commensurate with their assignment, prior to reporting to their foreign duty location.

**(3)** The personnel security office will transmit the security clearance data to the appropriate DOS regional security officer or post security officer when an employee is being assigned to a foreign duty location. They can do this either by electronic message directly to the regional or post security officer, or by providing the data to the Bureau of Diplomatic Security, DOS.

**b. Personal Service Agreement (PSA) Personnel.** U.S. citizens who are family members of U.S. personnel stationed in foreign countries and who are PSA employees under arrangements made through DOS are not required to hold a security clearance if their employment will not require them to have access to CNSI, or to sensitive areas at locations that receive, process, or store classified, other foreign policy, or operationally sensitive information or material. The personnel security office is responsible for granting any security clearance necessary for PSA personnel requiring access to classified information or sensitive areas. Otherwise, the PSS must ensure that PSA employees not requiring access to classified information have a favorably adjudicated Tier 1 background investigation, which is the minimum background investigation for PSA employees.

**c. Temporary Duty (TDY).**

**(1)** An employee who is to be on TDY, intermittently or continuously, to a foreign location for more than 120 days in a calendar year, must have a completed Tier 3 investigation that has been favorably adjudicated, prior to beginning the travel.

**(2)** There are no special investigative requirements for all other foreign TDY assignments, 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. Additionally, there is no specific clearance requirement to visit DOT offices located in foreign countries, provided access to classified information is not required. However, 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 minimum of a Secret security clearance.

**(4)** The LOB/SO must determine whether an employee should be issued a security clearance prior to a foreign TDY. In making this decision, the LOB/SO should consider the type of work to be performed, the extent, nature, and location of contacts with FAA and other Government officials, and the length of the TDY.

**(5)** The LOB/SO can submit a request to the responsible personnel security office for a temporary clearance, if an employee scheduled for TDY needs a security clearance for a foreign TDY and does not have one. Temporary clearances will be processed as described in Chapter 7.

**(6)** The personnel security office must transmit security clearance data for employees going on TDY, as necessary, per Section 2(a)(3) of this chapter.

**d. International Conferences.**

**(1)** Head of a delegation. Any FAA employee selected to head a delegation from the U.S. to an international conference, on other than a one-time basis, is subject to a minimum of a Tier 3 investigation.

**(2)** Nominee as FAA representative at an international conference. Nomination to represent FAA at an international conference is subject to completion of a minimum of a Tier 1 investigation. This investigation has normally been conducted on Federal employees, but not necessarily on technical advisors or other representatives from industry. If an advisor or other representative from industry is selected to represent the FAA at an international conference, the FAA office arranging for the advisor's services must contact the personnel security office at least three weeks prior to the date that the delegation is scheduled to depart. The personnel security office will then determine if a Tier 1 investigation was already conducted on the technical advisor or other industry representative, which may be the case if the person holds a U.S. Government security clearance or is a military reservist. The personnel security office will initiate the appropriate eQIP investigation request for the person to complete, if a Tier 1 investigation has not been completed. The sponsoring office must then ensure that the forms are completed and submitted to the personnel security office to 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 an FAA employee to visit NATO headquarters or a similar activity must ensure in advance that they contact their personnel security office to process any special clearance(s) required. They should ask about clearance requirements when making the visit arrangements, and provide the request to their personnel security office at least three weeks in advance of the visit, to allow time for processing, per Chapter 7.

**3. Reporting Requirements for Clearance Holders Traveling Abroad.** All FAA employees who have access to classified information or hold a sensitive position are required to report foreign travel and foreign contacts to AXP, per requirements from SEAD 3, as outlined in Chapter 7.

## Chapter 11. Program Evaluation and Quality Control

**1. Introduction.** The Personnel Security Policy and Programs Division, AXP-100, is responsible for periodically evaluating the personnel security program throughout the ASH organization to ensure it is operating efficiently and effectively. Evaluations help assess whether ASH's products and services meet established standards, quality expectations, and are consistent with Agency policy and applicable law. AXP-100 is responsible for conducting evaluations that will encompass applicant, employee, contractor, and non-employee processes.

**2. Evaluation Standards.**

**a.** A team of two or more PSSs from AXP-100, one of which will be designated as the team leader, will conduct the program evaluation. The team may also include a PSS from another office, other than the office under review.

**b.** The evaluation team will conduct evaluations that cover applicant, employee, contractor, and non-employee personnel security operations to:

**(1)** Assess overall program effectiveness;

**(2)** Determine compliance with this Order and applicable SOP(s);

**(3)** Measure performance against established standards;

**(4)** Identify areas requiring guidance or policy change;

**(5)** Identify local successes and best practices; and

**(6)** Provide recommendations on corrective actions regarding program shortfalls that may be identified.

**c.** Evaluations will consist of interviews of employees associated with the personnel security operation, file reviews, and reviews of database reports.

**d.** Evaluations will cover a representative number or percentage of records and personnel, sufficient to identify problematic areas and patterns.

**e.** The evaluation team will conduct a sufficient number of interviews of employees associated with the personnel security operation to ensure a representative sample is obtained. In addition, the team will interview any PSS whose cases appear deficient during the review process.

**f.** The team leader will provide written notice to the office to be evaluated at least 30 calendar days prior to commencement of the evaluation.

**g.** The team will hold in-brief and out-brief meetings with site management to introduce team members, explain the evaluation process, and discuss findings.

**h.** The team leader will sufficiently support any findings and recommendations with relevant documentation.

**i.** The evaluation team will provide a final written report to AXP-1 and the appropriate AXP Division Manager within 60 calendar days of the evaluation. The report will include a candid evaluation of policy and program effectiveness and will identify findings, any on-the-spot corrections made, recommendations for corrective actions, best practices, and noteworthy contributions to program operations.

**j.** If necessary, the appropriate AXP Division manager must respond in writing to AXP-1 within 60 calendar days after receipt of the report, certifying corrective actions taken.

**3. Quality Control.** In addition to scheduled onsite program evaluations, AXP-100 will also periodically perform quality control activities to monitor compliance with this Order and applicable law; ensure consistency across AXP; monitor timeliness of processes; and identify areas needing attention. Quality control activities may include spot checks of ITS records, adjudication reviews, reviewing database reports, and other similar activities. AXP-100 will refer any identified deficiencies to the appropriate AXP manager for action.

**4. Report Retention.** The appropriate AXP Division Manager must retain a copy of the program review for his or her site, and can use the program review for in-house training of personnel. AXP-100 will also maintain copies of all reports, to ensure that any deficiencies found are corrected, and not repeated in future reviews. Prior to any new evaluation, AXP-100 will review the old reports to identify any repeat deficiencies noted in previous reports.

## Appendix A. Related Publications and References

Title 5, Code of Federal Regulations (CFR), Part 731, Suitability.

Title 5 CFR Part 732, National Security Positions.

Title 5 CFR Part 736, Personnel Investigations.

Title 5 CFR Part 1400, Designation of National Security Positions.

Title 32 CFR Part 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

5 U.S.C. § 552a, Privacy Act of 1974.

28 U.S.C. § 1746 Unsworn Declarations Under Penalty of Perjury.

34 U.S.C. § 20351 Child Care Worker Employee Background Checks.

49 U.S.C. § 40122 Federal Aviation Administration Personnel Management System.

Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004.

EO 10577, Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service.

EO 12829, National Industrial Security Program.

EO 12968, Access to Classified Information.

EO 13467, Reforming Process Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.

EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust.

EO 13526, Classified National Security Information.

EO 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities.

EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.

EO 13741, Amending Executive Order 13467 to Establish the Roles and Responsibilities of the National Background Investigation Bureau and Related Matters.

EO 13764, Amending the Civil Service Rules, EO 13488 and EO 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters.

Security Executive Agent Directive (SEAD 1), Security Executive Agent Authorities and Responsibilities.

Security Executive Agent Directive 3 (SEAD 3), Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.

Security Executive Agent Directive 4 (SEAD 4), National Security Adjudicative Guidelines.

Security Executive Agent Directive 5 (SEAD 5), Collection, use, and retention of publicly available social media information in personnel security background investigations and adjudications.

Security Executive Agent Directive 6 (SEAD 6), Continuous Evaluation.

Security Executive Agent Directive 7 (SEAD 7), Reciprocity of Background Investigations and National Security Adjudications.

Security Executive Agent Directive 8 (SEAD 8), Temporary Eligibility.

Joint Memorandum from the Office of the Director of National Intelligence and the Office of Personnel Management, Approval of Revised Federal Investigative Standards, December 2012.

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

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.

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

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

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

Office of Management and Budget Circular No. A-130, Managing Information as a Strategic Resource, July 28, 2016.

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

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

FAA Order 1600.76, Sensitive Compartmented Information (SCI) Program Management.

FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI).

FAA Order 1600.2, Classified National Security Information (CNSI).

FAA Order 1600.69, FAA Facility Security Management Program.

FAA Order 1600.78, Personal Identity Verification (PIV) Card and Other Identification Cards.

FAA Order 1370.121, FAA Information Security and Privacy Program & Policy.

FAA Order 1270.1, Freedom of Information Act Program.

DOT Order 1630.2, Personnel Security Management Program.

DOT Order 1642.2/MAO 280-4, North Atlantic Treaty Organization (NATO) Program.

PAC Memorandum January 22, 2015, Implementation of the Quality Assessment Standards for Background Investigations.

## Appendix B. Definitions

Classified National Security Information (CNSI): Information that has been determined under EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. (EO 13526, section 6.1(i))

Cohabitant: A person with whom the subject resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the subject resides for reasons of convenience (e.g., a roommate).

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.

Contractor Employee: A person employed as or by a contractor, subcontractor, or consultant supporting FAA through a contract, PO, lease agreement or other similar agreement.

Counterintelligence: Information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (50 U.S.C § 3003(3)); OR

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities. (EO 12333, section 3.4(a))

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.

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.

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.

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

Nexus: A direct or logical connection between a person's behavior and the position's duties and responsibilities.

Non-employee: A person who is neither an FAA employee nor a contractor employee, who by agreement with the FAA, has access to FAA facilities, systems, SUI, resources and/or classified national security information (CNSI) similar to the access that FAA employees and contractor employees have.

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 national security.

Probationary period: A one-year period intended to give an employer an opportunity to assess, on the job, the employee's overall fitness and qualifications for continued employment, and to permit the removal, without adverse action procedures, of an employee whose performance or conduct does not meet acceptable standards.

Public Trust Position: Any position so designated under Title 5 CFR Part 731. A position that 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.

Reciprocity: The practice of recognizing and accepting prior background investigations and fitness, suitability or security determinations, in lieu of initiating a new 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.

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 is granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the U.S., and any doubt will be resolved in favor of national security.

Sensitive Compartmented Information: Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is handled within formal access controls systems established by the Director of National Intelligence.

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

Special Agreement Check: An investigative product offered by DCSA that consists of a check of investigations conducted by DCSA, OPM, or other federal investigative agencies, and a fingerprint-based search of FBI criminal files.

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.

Trusted Information Provider: 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.

## Appendix C. Frequently Used Acronyms

| Acronym | Term |
|---|---|
| AAM | Office of Aerospace Medicine |
| AAQ | Acquisition & Contracting |
| AHR | Office of Human Resources Management |
| ASH | Office of Security and Hazardous Materials Safety |
| AXI | Office of Investigations |
| AXP | Office of Personnel Security |
| CSF | Contract Security File |
| CNSI | Classified National Security Information |
| CO | Contracting Officer |
| COR | Contracting Officer Representative |
| DOJ | Department of Justice |
| DOS | Department of State |
| DOT | Department of Transportation |
| DCSA | Defense Counterintelligence and Security Agency |
| EFI | Expandable Focused Investigation |
| EO | Executive Order |
| eQIP | Electronic Questionnaire for Investigations Processing |
| FAA | Federal Aviation Administration |
| FBI | Federal Bureau of Investigation |
| FIS | Federal Investigative Standards |
| FOIA | Freedom of Information Act |
| HSPD | Homeland Security Presidential Directive |
| ISP | Investigative Service Providers |
| ITS | Investigations Tracking System |
| LAA | Limited Access Authorization |
| LER | Labor and Employee Relations |
| LOI | Letter of Inquiry |
| LOB | Line of Business |
| MARAD | Maritime Administration |
| NATO | North Atlantic Treaty Organization |
| NISP | National Industrial Security Program |
| NISPOM | National Industrial Security Program Operating Manual |
| NTS | National Training Standards |
| ODNI | Office of the Director of National Intelligence |
| OF | Optional Form |
| OPM | Office of Personnel Management |
| PDT | Position Designation Automated Tool |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| PO | Purchase Order |

| Acronym | Term |
|---|---|
| PSA | Personal Service Agreement |
| PSF | Personnel Security File |
| PSMM | Personnel Security Management Manual |
| PSS | Personnel Security Specialist |
| ROI | Report of Investigation |
| SAC | Special Agreement Check |
| SAP | Special Access Program |
| SCI | Sensitive Compartmented Information |
| SEAD | Security Executive Agent Directive |
| SecEA | Security Executive Agent |
| SF | Standard Form |
| SO | Staff Office |
| SOP | Standard Operating Procedures |
| SOW | Statement of Work |
| SUI | Sensitive Unclassified Information |
| SuitEA | Suitability Executive Agent |
| VAR | Visit Access Request |

## Appendix D. Suitability Factors and Considerations

Criteria for making suitability determinations.

**1. General**. The PSS must base their suitability determination on the presence or absence of one or more of the specific factors (charges) in Section 2 of this appendix.

**2. Specific factors**. In determining whether a person is suitable for Federal employment, only the following factors will be considered a basis for finding a person unsuitable and taking a suitability action:

**a.** Misconduct or negligence in employment;

**b.** Criminal or dishonest conduct;

**c.** Material, intentional false statement, or deception or fraud in examination or appointment;

**d.** Refusal to furnish testimony as required by 5 CFR 5.4;

**e.** Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;

**f.** Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;

**g.** Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and

**h.** Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

**3. Additional considerations**. Adjudicators must consider any of the following additional considerations to the extent any of them are deemed pertinent to the individual case:

**a.** The nature of the position for which the person is applying or in which the person is employed;

**b.** The nature and seriousness of the conduct;

**c.** The circumstances surrounding the conduct;

**d.** The recency of the conduct;

**e.** The age of the person involved at the time of the conduct;

**f.** Contributing societal conditions; and

**g.** The absence or presence of rehabilitation, or efforts toward rehabilitation.