

ORDER

1600.1E

PERSONNEL SECURITY PROGRAM



07/25/05

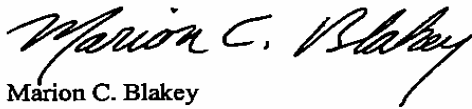
**DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION**

FOREWORD

This directive documents the Federal Aviation Administration's Personnel Security Program and establishes procedures and responsibilities in implementing the program in accordance with applicable laws and regulations.

As the FAA, our mission is to ensure safe, secure, and efficient air travel. Our ability to do this depends on the adequacy, reliability, and security of our facilities, automated systems, information, and resources. You should apply the security measures that are outlined in this order during the applicant and employee hiring process so that all employees and applicants are treated equally and fairly. When implemented, we will eliminate security weaknesses and tighten controls over the hiring process and also ensure appropriate risk assessments and security screenings are performed.

It is incumbent upon each assistant and associate administrator, director, manager, and FAA employee to ensure full understanding and compliance with this order.



Marion C. Blakey
Administrator

TABLE OF CONTENTS

	Page No.
FOREWORD	i
CHAPTER 1. INTRODUCTION	
1. Purpose.....	1-1
2. Distribution.....	1-1
3. Cancellation.....	1-1
4. Explanation of Changes.....	1-1
5. Forms.....	1-2
6. References to Days.....	1-2
7. Authority to Change this Order.....	1-2
8. Objectives.....	1-2
9. Exceptions to Requirements and Standards.....	1-2
10. Scope.....	1-3
11. Policy.....	1-3
12. Definitions.....	1-4
CHAPTER 2. GENERAL	
1. Responsibilities.....	2-1
2. Safeguarding Rights and Privacy of Applicants and Employees.....	2-4
CHAPTER 3. PERSONNEL SECURITY OPERATIONS AND RESPONSIBILITIES.	
1. General.....	3-1
2. Standards of Operation.....	3-1
3. Personnel Security Operational Responsibilities.....	3-1
CHAPTER 4. DESIGNATING POSITION SENSITIVITY AND RISK LEVELS	
1. Position Sensitivity and Risk Level Designation.....	4-1
2. Responsibility for Position Sensitivity and Risk Level Designations.....	4-1
3. Risk Levels.....	4-1
4. Sensitivity Levels.....	4-2
5. Position Sensitivity and Risk Level Designation Process.....	4-2
6. Official Record of Position Risk and Sensitivity Designation.....	4-3
7. Coding of Position Risk and Sensitivity Levels on Personnel Documents.....	4-3
Figure 1. Risk/sensitivity Level Coding.....	4-3
8. Position Risk and Sensitivity Level Designation Procedures.....	4-4
9. Minimum Levels for Certain Positions.....	4-11
Figure 2. Category of Positions.....	4-11

	Page No.
10. Regional Level Program Placements.....	4-12
11. Regional Level Positions.....	4-13
Figure 3. Designated Positions.....	4-13
CHAPTER 5. PERSONNEL SECURITY INVESTIGATION REQUIREMENTS AND PROCEDURES	
Section 1. Investigative Requirements	5-1
1. General.....	5-1
2. Types and Scope of Background Investigations.....	5-1
3. Basic Investigative Requirements.....	5-3
4. Specific Requirements: Special-Sensitive Positions.....	5-6
5. Specific Requirements: Critical-Sensitive Positions.....	5-7
6. Specific Requirements: Non-critical-Sensitive Positions.....	5-9
7. Specific Requirements: High-Risk Positions.....	5-9
8. Specific Requirements: Moderate-Risk Positions.....	5-10
9. Specific Requirements: Low-Risk Positions.....	5-11
10. Specific Requirements for Certain Positions.....	5-11
11. Exceptions to Investigative Requirements.....	5-11
Section 2. Waiver Requirements	5-12
1. Waiver of Pre-placement Investigative Requirements.....	5-12
2. Special Procedures for Accelerated Hiring.....	5-19
Section 3. Investigation Process	5-20
1. Initiating, Monitoring, and Closing Investigations.....	5-20
2. Additional SSE Investigation.....	5-23
3. Reciprocity, Standards and Procedures for Using Previous Investigations.....	5-24
4. Obtaining and Reviewing Previous Investigations.....	5-25
Section 4. Investigative Forms	5-27
1. Forms Required for Investigations.....	5-27
2. Completion of Forms.....	5-28
3. Originals and Copies.....	5-30
CHAPTER 6. PERSONNEL SECURITY RECORDS	
1. Personnel Security Files (PSF)	6-1
2. Non-selected Applicants.....	6-2
3. Transfer of PSF.....	6-2
4. Separated Employees.....	6-2
5. Protection of Personnel Security Records.....	6-3
6. Employee Review of PSFs.....	6-4
7. Privacy Act Requirements.....	6-5
8. Agreements to Release Personnel Security Records.....	6-6

CHAPTER 7. PERSONNEL SUITABILITY STANDARDS, CRITERIA AND ADJUDICATION

1. General.....	7-1
2. Suitability.....	7-1
3. Personnel Suitability Standard and Criteria.....	7-2
4. Coordinating Personnel Security Information.....	7-3
5. Suitability Adjudication.....	7-3
6. Suitability Adjudication Process.....	7-4
7. Documentation and Notification.....	7-5

CHAPTER 8. PERSONNEL SECURITY STANDARDS, CRITERIA, AND ADJUDICATION

1. Personnel Security Standard and Criteria.....	8-1
2. Security Adjudication.....	8-3
3. Responsibility for Security Adjudications.....	8-3
4. Case Adjudication Procedures.....	8-3
5. Timeliness of Adjudications.....	8-4
6. Security Adjudication Guidelines.....	8-5
7. Guideline A: Allegiance to the United States.....	8-7
8. Guideline B: Foreign Influence.....	8-8
9. Guideline C: Foreign Preference.....	8-9
10. Guideline D: Sexual Behavior.....	8-10
11. Guideline E: Personal Conduct.....	8-11
12. Guideline F: Financial Consideration.....	8-13
13. Guideline G: Alcohol Consumption.....	8-14
14. Guideline H: Drug Involvement.....	8-15
15. Guideline I: Emotional, Mental, and Personality Disorders.....	8-16
16. Guideline J: Criminal Conduct.....	8-17
17. Guideline K: Security Violations.....	8-17
18. Guideline L: Outside Activities.....	8-18
19. Guideline M: Misuse of Information Technology Systems.....	8-18
20. Records to be Maintained.....	8-19

CHAPTER 9. ACCESS AUTHORIZATIONS

1. General.....	9-1
2. Limitations and Restrictions on Access to Classified Information.....	9-2
3. Request Procedures.....	9-3
4. Interim Clearances.....	9-3
5. Temporary Clearances.....	9-5
6. Final Clearances.....	9-6
7. Clearance Granting Procedures and Documentation.....	9-6
8. Special Access Authorizations.....	9-7
9. Terminating Access Authorizations.....	9-8
10. Visit clearance Requests.....	9-9

CHAPTER 10. ADVERSE SECURITY ACTIONS	
1. General.....	10-1
2. Preliminary Actions.	10-1
3. Security Clearance Denial, Suspension, and/or Revocation.....	10-1
4. Appeal.....	10-3
5. Employment of Individuals Previously Separated for Security Reasons.....	10-4
CHAPTER 11. ACCESS TO AUTOMATED INFORMATION SYSTEMS	
1. General.....	11-1
2. Access Requirements.....	11-1
3. Procedures.....	11-2
CHAPTER 12. FOREIGN ASSIGNMENTS AND TRAVEL	
1. General.....	12-1
2. Investigative Requirements.....	12-1
CHAPTER 13. SECURITY CLEARANCES AND AUTHORIZATIONS FOR IMMIGRANT ALIENS	
1. General.....	13-1
2. Investigative Requirements for Foreign Nationals.....	13-1
3. Procedures for Limited Access Authorizations.....	13-1
4. Procedures for Immigrant Alien Security Clearances.....	13-1
5. Approval for Visits by Foreign Nationals Cleared by other Agencies.....	13-2
CHAPTER 14. NATIONAL EMERGENCY PERSONNEL SECURITY PROCEDURES	
1. Purpose.....	14-1
2. Activation of Standby Procedures.....	14-1
3. Standby Procedures: Modification of Investigative Requirements.....	14-1
4. Required Plans for Personnel Security Operations During a National Emergency.....	14-2
CHAPTER 15. PROGRAM EVALUATION	
1. Introduction.....	15-1
2. Program Mission Statement.....	15-1
3. Evaluation Standards.....	15-1
4. Evaluation Criteria.....	15-1
5. Responsibilities.....	15-2
6. Preliminary Phase.....	15-4
7. On-site Evaluation.....	15-6

	Page No.
8. Findings and Recommendations.....	15-6
9. Supporting Documentation.....	15-6
10. Report Writing and Retention.....	15-7
 APPENDICES	
APPENDIX A.	
Definitions.....	A-1
APPENDIX B.	
Sample Letter for DCII Checks.....	B-1
APPENDIX C.	
Personnel Security Forms.....	C-1
APPENDIX D.	
Statutory Debarment Issues.....	D-1
APPENDIX E.	
Investigating Child Care Services Employees.....	E-1
APPENDIX F.	
DOT F 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act.....	F-1
APPENDIX G.	
Security Briefing Guidance for Access to Classified Information.....	G-1

CHAPTER 1. INTRODUCTION

- 1. Purpose.** This order states personnel security policy under the Department of Transportation (DOT) Order DOT 1630.2, Personnel Security Management, and establishes related standards, criteria, and procedures for the Federal Aviation Administration (FAA) consistent with applicable laws, Executive Orders (E.O.), and Government-wide regulations governing the Personnel Security Program.
- 2. Distribution.** This order is distributed to the division level in headquarters, regions, and centers, with a limited distribution to all field office and facilities.
- 3. Cancellation.** Order 1600.1D, Personnel Security Program, dated February 5, 1998.
- 4. Explanation of changes.** This order:
 - a.** Updates personnel security policy and procedures to include:
 - (1) New investigative requirements, including the Access National Agency Check with Inquiries, National Agency Check with Law Enforcement Inquiries and Credit, and Child Care National Agency Check.
 - (2) New waiver procedures for moderate risk positions.
 - b.** Removes all references to the Contractor Security Program which is now found in FAA Orders 1600.72, Contractor and Industrial Security Program, and 1600.73, Contractor and Industrial Security Program Operating Procedures.
 - c.** Delegates the initial responsibility for security clearance denials and revocations to the Director of Internal Security and Investigations, AIN-1, with final authority to the Assistant Administrator for Security and Hazardous Materials, ASH-1.
 - d.** Revises office titles and routing symbols for the ASH organization.
 - e.** Combines certain appendices into chapters.
 - f.** Changes references to current DOT/FAA databases, such as, the Consolidated Personnel Management Information System, Integrated Personnel and Payroll System, etc., to the generic term of FAA-approved databases.
 - g.** Establishes the Personnel Security Program's evaluation process.
 - h.** Eliminates Appendix 6, Suitability Adjudication Procedures and places it in a Personnel Security Supplement for internal use by ASH personnel.

5. Forms. Refer to Appendix C, Personnel Security Forms, for a listing of forms used in FAA's Personnel Security Program.

6. References to Days. In this order, unless otherwise stated, all references to days refer to calendar days.

7. Authority to Change this Order. The Administrator has the authority to approve changes that establish or revise policy, delegate authority, or assign responsibility. ASH-1 can 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.

8. Objectives. The objectives of the Personnel Security Program are to ensure that employment or continued employment of persons in the FAA will promote the efficiency of the service and that the national security will be safeguarded. As the FAA, we must achieve this through consistent application of personnel security standards, criteria, and procedures referenced below.

a. E.O. 10450, Security Requirements for Government Employment, as amended, dated April 27, 1953.

b. E.O. 12958, Classified National Security Information, as amended by E.O. 13292, dated March 25, 2003.

c. E.O. 12968, Access to Classified Information, dated August 2, 1995;

d. Title 5, Code of Federal Regulations (CFR), Parts 731, Personnel Suitability; 732, National Security Positions, and 736, Personnel Investigations.

e. Investigative Standards for Background Investigations for Access to Classified Information, Security Policy Board (SPB) Issuance I-97, approved by the President, dated March 24, 1997.

f. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, SPB Issuance 2-97, approved by the President, dated March 24, 1997.

g. Investigative Standards for Temporary Eligibility for Access, SPB Issuance 3-97, approved by the President, dated March 24, 1997.

9. Exceptions to Requirements and Standards. ASH-1 has authority to approve any exceptions to the requirements and standards stated in this order including region and center supplements.

10. Scope. All employees and DOT/FAA-sponsored child care center workers (Appendix E) must apply the provisions of this order. FAA contractor employees are covered under the latest edition of FAA Orders 1600.72 and 1600.73.

11. Policy. As the FAA, we will:

a. Not employ or retain a person in employment unless a determination is made on behalf of the Administrator that the person's employment will promote the efficiency of the service.

b. Not employ or retain a person in employment by FAA unless a determination is made on behalf of the Administrator that such employment is clearly consistent with the interests of national security.

c. Grant a person eligibility for access to classified information only when facts and circumstances indicate that access to this information is clearly consistent with the national security interests of the United States. We must resolve any doubt in favor of the national security.

d. Ensure that all employees responsible for making suitability and security determinations have completed formal FAA-approved adjudicative training within 1 year from the date of this order, or within 18 months of hiring, if hired after the date of this order.

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 the classified information to perform his or her duties; and the person signed an approved classified information nondisclosure agreement. In exceptional circumstances, the servicing security element can grant access to classified information to persons on whom the 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 our employees and applicants through consistent application of personnel security standards, criteria, and procedures as specified in applicable laws, regulations, and orders. We will not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information, or use the denial of access to classified information as a substitute for appropriate adverse suitability determination or disciplinary actions.

g. Provide all applicants and employees the opportunity to explain or refute any unfavorable information before the information is used as a basis for any adverse personnel, security, or similar action against them.

h. Not employ any person whom the Secretary of Transportation has removed from employment for national security reasons without the Secretary's prior approval. This authority cannot be re-delegated.

i. Disclose investigative and personnel security records only to the extent necessary under this order; the latest editions of FAA Order 1200.23, Public Availability of Information; FAA Order 1280.1, Protecting Privacy of Information About Individuals; and any other orders or directives that implement the Privacy Act and Freedom of Information Act.

12. Definitions. Refer to Appendix A.

CHAPTER 2. GENERAL

1. Responsibilities.

a. Administrator. The Administrator is responsible for ensuring that the FAA maintains a Personnel Security Program consistent with applicable laws, regulations, and orders. This program ensures that a person's employment and continued employment with FAA promotes the efficiency of the service and is consistent with national security interests.

b. Assistant Administrator for Security and Hazardous Materials (ASH-1). ASH-1 has the primary responsibility for carrying out the FAA's Personnel Security Program, providing general direction for the program throughout FAA, and ensuring that resources needed for conducting an effective program are available and efficiently used.

c. Director, Office of Internal Security and Investigations (AIN-1). AIN-1 is responsible for the Personnel Security Program operations and direct program implementation in the regions, centers, and headquarters; and, in coordination with the Director, Office of Field Operations, AHS-1, for appraising the effectiveness and efficiency of the program. AIN-1 is also responsible for promulgating personnel security standards and guidelines that are applicable throughout FAA.

d. Director, Office of Field Operations (AHS-1). AHS-1 is responsible for Personnel Security Program operations and direct program implementation in the regions and centers.

e. Directors of Offices and Services. Directors of offices and services are responsible for ensuring that their subordinates understand and are complying with Personnel Security Program requirements.

f. Regional Administrators and Center Directors. Regional administrators and center directors are responsible for carrying out and complying with this order in their respective regions and centers.

g. Manager, Personnel Security Division (AIN-400). Under AIN-1, AIN-400, serves as the FAA's Personnel Security Manager and is responsible for:

- (1) Implementing and maintaining an effective Personnel Security Program.
- (2) Ensuring compliance with personnel security and suitability investigative requirements.
- (3) Assisting the Office of Human Resource Management and operating offices in suitability adjudication.

- (4) Providing appropriate training throughout FAA for designating position risk and sensitivity levels, and for security and suitability adjudication.
- (5) Ensuring that position risk and sensitivity levels are properly determined.
- (6) Adjudicating security issues, granting security clearances, and, as necessary recommending revocation and denial of security clearances to AIN-1.
- (7) Evaluating the effectiveness of the Personnel Security Program.
- (8) Preparing consolidated reports for and on behalf of AIN-1, AHS-1, and ASH-1.
- (9) Providing guidance and direction throughout FAA on all personnel security matters.

h. Managers of Servicing Security Elements (SSE). Under AHS-1, the managers of the Security and Hazardous Materials Divisions are responsible for:

- (1) Implementing and maintaining an effective Personnel Security Program within their area of responsibility.
- (2) Ensuring compliance with personnel security and suitability investigative requirements.
- (3) Assisting Human Resource Management Divisions and operating offices in suitability adjudication.
- (4) Providing appropriate training throughout their area of responsibility for designating position risk and sensitivity levels, and for security and suitability adjudication.
- (5) Ensuring that position risk and sensitivity levels are properly determined.
- (6) Adjudicating security issues, granting security clearances, and, as necessary, recommending revocation and denial of security clearances to AIN-400.
- (7) Providing guidance and direction throughout their areas of responsibility on all personnel security matters.

i. Managers of Human Resource Management Divisions (Personnel). Personnel managers are responsible for:

- (1) Working with operating offices in collecting and submitting paperwork for required personnel security and suitability investigations on employees and applicants.
- (2) Obtaining authorization from their SSE prior to processing personnel actions to place persons in public trust or sensitive positions.
- (3) Ensuring that manual and automated master position description records accurately reflect approved position risk and sensitivity level designations.
- (4) Adjudicating suitability issues in coordination with their SSE and the operating offices.
- (5) Advising management officials regarding adverse actions against employees.

j. All FAA Managers. With respect to personnel security, general management responsibilities include:

- (1) Ensuring that persons under their jurisdiction fully understand and are complying with personnel security standards, criteria, and procedures, thus appropriately protecting the interests of national security, the FAA and our employees, and promoting the efficiency of the service.
- (2) Obtaining authorization from their SSE prior to processing personnel actions to place persons in public trust and sensitive positions.
- (3) Identifying and reporting to their SSE any significant deviation from personnel security standards, criteria, or procedures.
- (4) Sharing responsibility with the appointing or approving official for ensuring completion of the required forms for personnel security investigations.

k. Employees. Employees are responsible for:

- (1) Familiarizing themselves with pertinent security regulations pertaining to their assigned duties, and the standards of conduct required for persons holding positions of trust. Recognizing and avoiding the kind of personal behavior that could result in rendering them ineligible for continued assignment in such a position. Maintaining continued eligibility for these positions.
- (2) Reporting to their SSE any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security, as required by E.O. 12968.

- (3) Protecting all classified information from unauthorized disclosure and reporting all contacts with persons, including foreign nationals, seeking a way to obtain unauthorized access to such information.
- (4) Reporting all violations of security regulations to their SSE.

2. Safeguarding Rights and Privacy of Applicants and Employees. If you are the SSE, you must follow and implement the procedures listed below per FAA Orders 1200.23 and 1280.1.

a. You 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.

- (1) Applicants and employees have the right to make an oral or written reply. This practice, commonly known as due process, prevents security from making errors that might otherwise result from mistakes in identity or erroneous information and provides an applicant or employee the opportunity to present mitigating information that is unknown to adjudicating officials.

- (2) Provide the applicant or employee with the appropriate Privacy Act advisements as specified in the latest edition of FAA Order 1600.20, Civil Aviation Security Investigations Handbook.

- (3) Furnish any records of the unfavorable information, including the employee's or applicant's response to the information, only to persons who have a need to know in their official capacity.

b. You must control investigative information gotten under a pledge of confidence keeping the commitment you made to the source of that information.

c. You must control medical information of a sensitive, personal nature obtained in conjunction with an investigation to ensure that it is not disclosed to persons who do not need it for official purposes. Do not use medical information to make a security or suitability determination until it has been properly interpreted by a medical official trained in analysis of the specific type of medical information concerned. If the medical official concludes that it might be harmful to an applicant or employee to see any of the medical information, you must deny access to that information to the person except through a medical official chosen by him or her.

d. You must ensure that all persons to whom information is being disclosed have a need to know it in an official capacity before releasing investigative information to anyone outside your organization. Also, the person receiving the information must ensure that the information is disclosed only to others who have a need to know it in an

official capacity. All persons reviewing the information will be required to sign FAA Form 1600-12, Investigative Record Review, however, the Subject of the information does not need to sign.

e. You must regard all Personnel Security Files, reports of personnel investigations, personal history statements, records of response to unfavorable information, computerized personnel security data, and other personnel security records and documents as Privacy Act information. Carefully protect them during handling, transmission, release, and storage following the procedures specified in the latest edition of FAA Order 1280.1.

f. If you receive a Freedom of Information Act (FOIA) request for the types of records mentioned in paragraph 2e of this chapter, apply Privacy Act considerations with all procedural requirements listed in the latest editions of FAA Orders 1200.23 and 1280.1.

CHAPTER 3. PERSONNEL SECURITY OPERATIONS AND RESPONSIBILITIES

1. General. This chapter prescribes FAA standards and responsibilities for conducting personnel security operations and for maintaining personnel security records.

2. Standards of Operation. FAA's personnel security operations must meet the following standards:

a. Operations will be conducted at organizational levels where they are closely controlled to ensure compliance with FAA and Department of Transportation (DOT) requirements, and must be managed in an efficient and effective manner.

b. Professionally qualified program managers will direct personnel security operations in servicing security elements (SSE). SSE and Human Resource Management Division (Personnel) managers can delegate responsibility for security and suitability adjudication, but must do so only to specialists who are fully trained to evaluate reports and results of personnel investigations and who have successfully completed an approved personnel security and suitability adjudication course.

c. SSEs will maintain close controls, conduct periodic evaluations as necessary, and closely monitor program operations when an operating office delegates personnel security operations to a field office.

3. Personnel Security Operational Responsibilities. SSEs have the primary responsibility for personnel security operations. However, Personnel and operating office officials will assist them by performing certain personnel security operational duties. The paragraphs below contain basic responsibilities for SSE, Personnel, and operating offices.

a. If you are the SSE, you must:

(1) Designate a program manager who will implement the FAA Personnel Security Program within your area of responsibility.

(2) Ensure that position sensitivity and risk level designations are accurate for all positions within your area of responsibility.

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

(4) Check national investigations indices for prior investigations concerning applicants and employees.

- (5) Process requests for waiver of pre-placement investigative requirements, as specified in chapter 5, section 2, paragraph 1 of this order. Conduct local agency and other checks as necessary.
- (6) Receive results of all investigations on applicants and employees from the Office of Personnel Management (OPM) or other sources. Review investigative reports to determine the adequacy of the investigation and to identify security or suitability issues.
- (7) Conduct or arrange for any additional investigation necessary to resolve security or suitability issues.
- (8) Provide due process to applicants and employees when required by chapter 2, paragraph 2 of this order.
- (9) Make security determinations on all cases involving sensitive positions and grant or deny security clearances. Advise your Personnel and operating offices of these determinations.
- (10) When requested, advise and assist your Personnel and operating offices in adjudicating suitability on applicants or employees.
- (11) Prepare and conduct, or ensure that your operating offices conduct security briefings for employees as needed.
- (12) Provide guidance to your Personnel and operating offices on personnel security policies and operating procedures.
- (13) Periodically evaluate the Personnel Security Program to ensure that it is operating effectively and efficiently.
- (14) Process visit clearance requests and certify security clearances as necessary.
- (15) Advise your Personnel and operating offices of all changes in costs of background investigations.

b. If you are the operating office, you must:

- (1) Designate a Personnel Security Coordinator to perform tasks listed in paragraph 3 of this chapter, and notify your SSE whenever a new coordinator is designated.
- (2) Recommend position sensitivity and risk level designations on positions under your jurisdiction. On all newly established or revised positions, coordinate

with your SSE prior to submitting a Standard Form 52, Request for Personnel Action, to designate the sensitivity or risk level per chapter 4, Designating Position Sensitivity and Risk Levels.

- (3) Ensure that all Optional Forms (OF) 8, Position Description, or equivalent, either electronic or hard-copy, show the approved sensitivity or risk-level designation, as well as any requirement for access to classified information. Place a remark on the OF-8 indicating the level of access required; i.e., Top Secret, Secret, Confidential, or other.
- (4) Ensure that vacancy announcements state that appointment is subject to a favorably adjudicated personnel security investigation enabling the granting of a security clearance, when appropriate
- (5) Ensure that before placing, or making any commitment to place a person in a special-sensitive, critical-sensitive, non-critical-sensitive, high-risk or moderate-risk position, your SSE and Personnel office have determined that the pre-placement investigative requirement was met or that an appropriate waiver was granted.
- (6) Ensure that you submit a request for waiver to your SSE for processing when emergency conditions exist that may hinder meeting the investigative requirement prior to placement in the position.
- (7) Budget for the costs of conducting personnel security investigations, or coordinate with your SSE to ensure budgeting for these costs.
- (8) Obtain or assist your SSE and Personnel office in collecting personnel security questionnaires, fingerprints, and other forms as required for personnel security processing and ensure that the forms are submitted in time to initiate investigations. Identity of the forms can be found in chapter 5, section 4, paragraph 1 of this order.
- (9) Conduct or arrange for security briefings for new employees and employees with newly granted security clearances. Periodically conduct or arrange for additional briefings to maintain a high level of security awareness. (Refer to Appendix G, Security Briefing Guidance for Access to Classified Information.)
- (10) Advise your SSE of any questionable conduct or activity by an employee that would raise a security or suitability issue.
- (11) Maintain records of the risk and sensitivity levels of your organization's positions.

(12) Maintain records of the security clearances held by your organization's employees. Maintain records as prescribed by the latest edition of FAA Order 1280.1.

c. If you are the Personnel office, you must:

- (1) Coordinate with your SSE on each new or revised position description as needed to ensure that the original OF-8 or equivalent shows the approved risk or sensitivity level.
- (2) Ensure that all vacancy announcements contain appropriate information about any investigative or personnel security clearance requirements that are a condition of employment in the position.
- (3) Obtain or participate with your operating offices in collecting personnel security questionnaires, fingerprints, and other forms as required for personnel security processing, and ensure that the paperwork is properly completed and submitted in time to initiate investigations. Identity of the forms can be found in chapter 5, section 4, paragraph 1 of this order.
- (4) Get available Official Personnel Folder (OPF) data about previous investigation(s) and provide this information to your SSE when an applicant is a current or former Federal employee,
- (5) Coordinate with your SSE regarding any information about an applicant that raises a security or suitability issue. This includes information disclosed on an employment application or personnel security questionnaire, or from pre-placement inquiries, including prior employers, the OPF, or any other sources.
- (6) Refer any information about an employee that would raise a security or suitability issue to your SSE.
- (7) Get approval from your SSE before placing any person in a special-sensitive, critical-sensitive, non-critical-sensitive, or high-risk position. Ensure the requirements of chapter 5 of this order are met.
- (8) Maintain accurate and current records of the sensitivity or risk-level designation for each position.
- (9) Keep personnel security documents in the OPF as specified in chapter 9, paragraph 7 of this order.
- (10) Enter the sensitivity or risk-level designation for each new position in an FAA-approved database.

(11) Adjudicate and make final suitability determinations, as required, on all cases with significant adverse information, coordinating with your SSE and appropriate operating officials.

d. If you are the Personnel Security Coordinator, you must:

- (1) Become familiar with the policies and requirements of this order.
- (2) Maintain liaison for your organization with your SSE and Personnel office.
- (3) Assist your SSE in determining the risk or sensitivity level of each position in your organization and maintain a record of these designations. Update the records when positions change or are abolished.
- (4) Arrange for the prompt submission of necessary forms to initiate personnel security investigations.
- (5) Arrange for briefings when employees from your office are granted security clearances, and debriefings when they leave or their clearance is terminated.
- (6) Maintain security clearance information for your organizations.
- (7) Promptly notify your SSE regarding visits by employees within your organization to other FAA facilities, and to other agencies, when security clearance certifications are required prior to the visits.
- (8) Advise your SSE regarding proposed details of persons to your organization whenever the details are to sensitive or public trust positions, and notify them when the detail ends.
- (9) Notify your SSE about any questionable employee conduct or activity that raises a security or suitability issue.
- (10) Promote an understanding of the Personnel Security Program's purpose and requirements within your organization.
- (11) Keep the head of your organization informed of substantive problems affecting implementation of the Personnel Security Program.
- (12) Recommend any new or modified procedures or policies believed to be in your organization's best interest to your SSE.

CHAPTER 4. DESIGNATING POSITION SENSITIVITY AND RISK LEVELS

1. Position Sensitivity and Risk Level Designation. Human Resource Management Divisions (Personnel) and operating offices must designate positions based on their level of risk in terms of suitability for employment, access to automated information systems (information resources), or level of sensitivity in terms of national security.

a. Risk Level Designation. Personnel and operating offices must designate positions that are not designated as national security positions at a risk level commensurate with the public trust responsibilities and attributes of the position as it relates to the efficiency of the service. They must rank them according to the degree of adverse impact an unsuitable employee could cause. They must designate positions where the incumbent has access to, or the responsibility for, information resources facilities, systems, or activities at a risk level commensurate with the responsibilities and other attributes of the position based on the extent to which an incumbent could cause damage to information resources or realize significant personal gain.

b. Sensitivity Designation. Personnel and operating offices must designate positions having national security duties at a national security sensitivity level necessary to ensure appropriate screening under E.O. 10450. They must assess the degree of damage that a person occupying a particular position could cause to the national security.

2. Responsibility for Position Sensitivity and Risk Level Designations. The servicing security element (SSE) is responsible for ensuring that correct risk or sensitivity-level designations are determined for every position within its jurisdiction. Personnel and operating offices must coordinate all position risk or sensitivity levels for new position descriptions with their SSE and with headquarters offices and services as necessary to ensure uniform designations for positions common in more than one region or center. Paragraphs 9 and 11 of this chapter list minimum risk levels for certain positions.

3. Risk Levels. There are three position risk levels, as follows:

a. Low Risk. Positions with the potential for impact involving duties of limited relation to the FAA mission with program responsibilities that affect the efficiency of the service. This level includes positions which have limited impact on information resources.

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. This level includes positions that have significant program responsibilities affecting large information resources.

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 broad scope of policy or program authority. This level includes positions that have major program responsibilities affecting information resources.

4. Sensitivity Levels. There are three sensitivity levels for designating positions with regard to national security:

a. Non-critical sensitive. Positions with the potential for causing serious damage to the national security.

b. Critical sensitive. Positions with the potential for causing exceptionally grave damage to the national security.

c. Special sensitive. Positions that are determined to be at a level higher than critical sensitive because of special requirements other than authority under E.O. 10450. This category includes all positions requiring access to Sensitive Compartmented Information (SCI).

5. Position Sensitivity and Risk Level Designation Process.

a. SSEs will use the risk-level designation procedures outlined in paragraph 8 of this chapter to ensure that positions are uniformly designated. These procedures include the criteria for designating risk levels based on information resources duties and responsibilities. They will use the national security criteria for approving sensitivity levels in conjunction with the risk-level designation procedures to ensure proper designation of national security positions.

b. Personnel and operating offices must designate positions requiring access to classified information at one of the three sensitivity levels in paragraph 4 of this chapter. Paragraph 8 of this chapter specifies the minimum sensitivity level for each level of access.

c. In many cases, particularly at the low-risk level, position risk is relatively clear. Personnel and operating offices may not need to apply all of the specific designating procedures in paragraph 8 of this chapter. Similarly, identical positions may require only occasional case-by-case analysis. Apply specific procedures on at least a random basis to ensure proper designations even when risk levels may appear obvious.

d. Personnel and operating offices can designate national security positions, particularly those requiring Top Secret or SCI access, at the appropriate sensitivity level without applying the more detailed procedures. However, if the duties and responsibilities of the position warrant designation as a high-risk position, designate it at least critical sensitive, even if the level of access required is no higher than Secret.

6. Official Record of Position Risk and Sensitivity Designation. Personnel and operating offices must document position risk and sensitivity level designations on FAA Form 1600-59, Position Risk/Sensitivity Level Designation Record. The Personnel office is responsible for maintaining all forms unless arrangements are made with their SSE to do so. The SSE should maintain a copy of the form when the position is designated as sensitive. FAA Forms 1600-59 can also be maintained electronically in lieu of retaining hard copies. If an FAA Form 1600-59 already exists for a position, it is not necessary to reproduce another one.

7. Coding of Position Risk and Sensitivity Levels on Personnel Documents. The following coding is required for Government-wide use on appropriate personnel documents, such as, the Standard Form (SF) -50, Notification of Personnel Action, and SF-52, Request for Personnel Action. SSEs and Personnel offices must use the coding to record a position's level in the FAA-approved database. Information resources positions, as determined according to paragraph 8 of this chapter, will be identified by the letter *C* after the numerical coding.

Figure 1. Risk/sensitivity Level Coding

RISK/SENSITIVITY LEVEL	CODING
High risk	6
Moderate risk	5
Special sensitive	4
Critical sensitive	3
Non-critical sensitive	2
Low risk	1

a. SSEs and Personnel offices must enter information concerning position sensitivity and risk-level designations, investigations initiated and completed, security clearance actions, waivers of investigative requirements, and other information as required by OST into the FAA-approved database. They must promptly enter all information. All employees with responsibility for entering information must ensure that the data maintained in the system are complete, accurate, and current.

b. SSEs and Personnel offices must ensure that the sensitivity or risk-level designation entered into the FAA-approved database for each position matches that shown on all personnel action forms. In any case where it does not, such as on an SF-52, the Personnel office should enter the designation using the coding shown above.

c. The Personnel Security Division, AIN-400, will represent the FAA in all discussions with OST concerning the data to be entered into the security subsystem; format for data entry; which data are mandatory or optional; which offices can view, enter, or change data; and data archiving and deletion.

8. Position Risk and Sensitivity-Level Designation Procedures. If you are the Personnel or operating office, you must use the process specified in this paragraph to provide a systematic way of uniformly designating position risk and sensitivity levels. Designate each agency program for its impact and scope related to the efficiency of the service (program placement) and then designate each position for its degree of risk to its program (tentative risk level). This paragraph also contains specific program placements for offices and divisions at the region level and minimum risk and sensitivity-level requirements for certain FAA positions. (Refer to paragraphs 9 through 11 of this chapter.)

a. Sensitivity-level designation.

(1) You must designate all sensitive positions having national security duties requiring access to classified information as either non-critical sensitive, critical sensitive, or special sensitive. Listed below are the minimum sensitivity levels to use for positions requiring access to specific levels of classified information. Record the level of access which makes a position sensitive as a final adjustment factor (block IV) on FAA Form 1600-59. You must designate:

(a) positions requiring access to Confidential or Secret information at least non-critical sensitive;

(b) positions requiring access to Top Secret information at least critical sensitive; and

(c) positions requiring access to SCI as special sensitive.

(2) You must designate all Executive positions as critical sensitive.

(3) SSEs only need to document the designation when it is apparent that the risk-level criteria described below would not affect a sensitivity-level determination. For example, if a position requires access to SCI, automatically designate the position as special sensitive regardless of other risk factors involved.

b. Risk-level designation. The risk-level designation process consists of designating each position for its degree of risk to its program, and making any final adjustments necessary because of unique factors specific to certain positions or to ensure organizational uniformity of operations.

(1) Program placement. Personnel and operating offices must follow the procedures below when determining program placement.

(a) Determine the program's impact on the efficiency of the service by identifying the area of primary program focus and then relating that area to one of the impact descriptions (major, substantial, moderate, or limited) listed in the left column of Chart A. The area of primary focus will be one of the following:

- 1 Accounting for, auditing, or disbursement of public funds;
- 2 Administrative, regulatory, or policy control over public and private programs or operations;
- 3 Protection of the national security;
- 4 Enforcement of Federal laws; or
- 5 Protection of life or property.

(b) If a program has more than one area of primary focus, or if questions arise as to placement of a program at one of two impact descriptions, base a decision on the best interests of the FAA's mission.

(c) Determine the program's scope of operations in terms of the efficiency of the service, choosing from one of the scopes (worldwide, Government-wide, multi-agency, or agency) listed across the top of Chart A.

(d) Use Chart A to determine program placement (major, substantial, moderate, or limited).

(2) Position risk points and tentative risk level. Consider the duties and responsibilities of the position, in the context of the program and the risk the position has for damage or abuse to the program, when determining position risk points. Determine the degree of impact on the program of each of five risk factors and the assignment of points to each risk factor. Combine the sum of the risk points and the program placement to determine the tentative risk level. Follow the specific procedures below:

(a) Determine the degrees of impact for each of the five risk factor descriptions shown across the top of Chart B. For all of the factors except supervision received, use the degree descriptions shown in the left column. For supervision received, use the degree descriptions shown in the right column.

(b) Assign a point value for each risk factor to numerically reflect the degree of impact. The greater the impact, the more points assigned. Although Chart B only shows point values of 1, 3, 5, and 7, points may be assigned at the 2, 4, and 6 values to reflect borderline determinations.

(c) Add the point values for each of the risk factors to determine the total risk points.

(d) Use Chart C to find the tentative risk level, applying the program placement determined above (left column) and the total risk points (top of the chart).

CHART A

Scope of Operations				
IMPACT	WORLDWIDE: Operational activity is carried out worldwide, with primary focus in either the public or the private sector.	GOVERNMENTWIDE Operational activity is carried out Government-wide, to all sectors, with primary focus on the public sector Government-wide.	MULTI-AGENCY: Nationally or regionally with primary focus extending to more than one agency in the public sector, or to the elements in the private sector impacted by the agencies.	AGENCY: Operations of the agency, or an agency's region or area, with primary focus extending to the elements in the private sector impacted by the agency.
MAJOR: Impacts directly on the survival, stability, and continued effectiveness of Government operations, the promotion of major Government fiscal goals, or a primary social, political, or economic interest of the Nation.	MAJOR	MAJOR	SUBSTANTIAL	MODERATE
SUBSTANTIAL: Impacts directly on the efficiency and effectiveness of a sizeable segment of the Federal work force, or the interests of large numbers of individuals in the private sector.	MAJOR	SUBSTANTIAL	SUBSTANTIAL	MODERATE
MODERATE: Impacts directly on the effectiveness of an agency's operations, the fiscal interests of an agency, or affects the social, political, or economic interests of individuals, businesses, or organizations in the private sector.	SUBSTANTIAL	MODERATE	MODERATE	LIMITED
LIMITED: Limited impact on the operational effectiveness of one or a few programs in an agency, or the interests of a limited number of individuals in the private sector.	MODERATE	MODERATE	LIMITED	LIMITED
Program Placement				

CHART B

RISK FACTOR DESCRIPTIONS					
DEGREE	DEGREE OF PUBLIC TRUST:	FIDUCIARY MONETARY RESPONSIBILITY:	IMPORTANCE TO PROGRAM:	PROGRAM AUTHORITY:	SUPERVISION RECEIVED:
	The consensus of confident expectation for honesty, integrity, reliability, responsibility, or justice placed in a position.	Authority or ability to obligate, control, or expend public money or items of monetary (bonds, etc.) value.	Impact the individual position has, due to status, in or influence on the program as a whole, either individually or collectively.	Ability to manipulate authority or control the outcome or results of all or key portions of a program or policy.	Frequency work is reviewed and nature of the review. DEGREE
MAJOR: Potential for Independently compromising the integrity and effectiveness of a major program element or component, or in conjunction with others, damaging all phases of program operations.	7	7	7	7	Limited: Occasional review only with respect to major policy issues by superior without expertise 7 in the technical aspects of program policy and operations.
SUBSTANTIAL: Potential for reducing the efficiency of overall program operations, or the overall operations of major program elements or components independently, or through collective action with others.	5	5	5	5	Periodic: Ongoing spot review of policy and major operational considerations of work by superior, with some knowledge 5 of program operations, but with minimal technical program expertise.
MODERATE: Potential for reducing the efficiency of the overall or day-to-day operations of a major program element or component, through independent action or collectively with others.	3	3	3	3	Moderate: Technical: Ongoing spot review of work in connection with important operation 3 issues by superior with technical program expertise.
LIMITED: Potential for damage not meeting above criteria.	1	1	1	1	Close Technical: 1 Continuing review of all phases of work by supervisor with technical program expertise.

POSITION RISK POINTS

CHART C

II. POSITION RISK POINTS

PROGRAM PLACEMENT	5-10	11-17	18-23	24-29	30-33	34-35
MAJOR	Low Risk (LR)	Moderate Risk (MR)	Moderate Risk (MR)	High Risk (HR)	High Risk (HR)	High Risk (HR)
SUBSTANTIAL	Low Risk (LR)	Moderate Risk (MR)	Moderate Risk (MR)	Moderate Risk (MR)	High Risk (HR)	High Risk (HR)
MODERATE	Low Risk (LR)	Low Risk (LR)	Moderate Risk (MR)	Moderate Risk (MR)	Moderate Risk (MR)	High Risk (HR)
LIMITED	Low Risk (LR)	Low Risk (LR)	Low Risk (LR)	Low Risk (LR)	Moderate Risk (MR)	High Risk (HR)

POSITION RISK LEVEL

(3) Final adjustment factors. Some positions, by the very nature of the duties and responsibilities of the program or the positions, require designation at certain levels of risk.

(a) Uniqueness. Factors that are unique, not fully accounted for in the above procedures, and can cause final adjustments include:

- 1 Special investigative or criminal justice duties.
- 2 Control of an automated monetary system (key access entry).
- 3 Few-of-a-kind positions with special duties, such as special assistant to the Administrator.
- 4 Support positions with no responsibilities for preparation or implementation of public trust program policies and plans, but involving regular contact with, and ongoing knowledge of, all or most of such material; e.g., budget analyst.
- 5 Any other factors believed relevant, provided they are documented.

(b) Uniformity. Clearly indicated needs for uniformity in position designation because of authority level or program placement level that may serve as a basis for making adjustments include:

- 1 The need for managers of major agency programs or divisions at the same level of authority to be placed at the same risk level.

2 The need for all positions within a particular program to be at a risk level paralleling the program's placement level. This would occur in those cases where the placement level is determined to be so overriding as to negate any specific risk considerations associated with individual positions within the program.

(c) Final adjustment.

1 You must make decisions on adjustment only after careful analysis of positions in terms of any uniqueness or uniformity factors that may apply. Document all adjustment factors on FAA Form 1600-59.

2 In order to ensure uniformity and consistency in risk-level designations, AIN-400 will assist regions and centers as necessary in reviewing position descriptions for positions common in more than one region or center. When doing so, they will coordinate with headquarters operating offices and services as needed, particularly for straight-lined organizations.

c. Information resources positions. Risk-level criteria for positions involving access to information resources are an integral part of risk and sensitivity-level designation. In addition to any public trust or national security criteria that may apply, Personnel and operating offices must apply the following criteria to any position with information resources duties and responsibilities:

(1) **High risk.** Positions at the highest level of risk to information resources. This includes positions in which the incumbent is responsible for the planning, direction, and implementation of information resources security program; has a major responsibility for the direction, planning and design of information resources, including the hardware and software; or can access a system during its operation or maintenance in such a way that there is relatively high risk for causing grave damage or realizing a significant personal gain. Such positions may involve:

(a) Responsibility for the development and administration of FAA information resources security programs, including direction and control of risk analyses and threat assessments.

(b) Significant involvement in life-critical or mission-critical systems.

(c) Responsibility for the preparation or approval of data for input into an information resources that does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

(d) Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from information resources of: (1) dollar amounts of \$10 million per year or greater; or, (2) lesser amounts if the activities of the person are not subject to technical review by higher authority to ensure the integrity of the system.

(e) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and management of systems hardware and software.

(f) Other positions that involve relatively high risk for effecting grave damage or realizing significant personal gain.

(2) Moderate risk. Positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of information resources, and whose work is technically reviewed by a higher authority at the high-risk level to ensure the integrity of the system. Such positions may involve:

(a) Responsibility for systems design, operation, testing, maintenance, and monitoring that is carried out under technical review of higher authority at the high-risk level to ensure the integrity of the system. This level includes, but is not limited to:

1 Access to, and processing of, proprietary data, information protected by the Privacy Act, and Government-developed privileged information involving the award of contracts. This criterion applies when the access is to a major FAA information resources and not just to information contained in a personal computer or local area network. The nature, extent, and volume of the information will be considered in applying this criterion.

2 Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.

(b) Other positions that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in high-risk positions.

(3) Low risk. Information resources positions not falling into one of the above risk levels.

d. Personnel and operating offices should use the higher of the levels determined as the final risk level when information resources duties and responsibilities also involve determinations under the procedures in paragraph 8b of this chapter, in addition to this paragraph. If the position is sensitive because of national security responsibilities, a determination of high risk under the information resources criteria will result in a

designation of at least critical sensitive. Adjustments due to information resources criteria must be recorded on FAA Form 1600-59 as final adjustment factors.

e. Personnel and operating offices must designate the following job series as information resources positions: 332, Computer Operator; 334, Computer Specialist; 335, Computer Clerk or Computer Assistant; and 1550, Computer Scientist. Other positions not necessarily in one of these series but with significant information resources responsibilities, such as, employee's responsible for information resources security, will also be designated as information resources positions. Duties involving use of a computer or access to information resources, by themselves, do not automatically make a position an information resources position.

9. Minimum Levels for Certain Positions. Because of uniqueness, special responsibilities, and the need for uniformity throughout the FAA, Personnel and operating offices must designate positions in the following categories at least at the risk levels shown, regardless of the level determined under the other criteria and procedures of this chapter.

Figure 2. Category of Positions

Category of Position	Position Risk Level Shall be at Least
a. Employee is responsible at the national headquarters level for the development and approval of national plans, policies, or programs for continuity of FAA operations during national emergencies.	High Risk
b. Manager responsible for the conduct of accident investigations and the enforcement standards through the certification/inspection process.	Moderate Risk
c. Division manager, or comparable level manager at a region or center, or an office or service director at headquarters.	High Risk
d. Manager of an office which is required to have regular public contacts with other governmental organizations or organizations in the private sector that demand the highest degree of trust.	High Risk
e. Contracting officer or specialist who has sole, final authority to approve contracts in excess of \$1,000,000 in value, or acquire or dispose of lands or facilities in excess of \$1,000,000 in value, when the approval or other action is not subject to any higher-level approval or concurrence.	High Risk

f. Contracting officer or specialist who has sole, final authority to approve contracts up to \$1,000,000 in value, or acquire or dispose of lands or facilities up to \$1,000,000 in value, when the approval or other action is not subject to any higher-level approval or concurrence.	Moderate Risk
g. Budget officers in headquarters, regions, and centers.	High Risk
h. Budget analysts in headquarters, regions, and centers.	High Risk
i. Employee is responsible at the regional, center, or headquarters level for overall management of: (1) An activity's property accountability system, to include the conduct of property inventories and the governing of survey boards; (2) acquisition and disposal of lands or FAA facilities; (3) contracting and the issuing of grants; and (4) accounting and/or disbursing of Government funds.	High Risk

10. Regional Level Program Placements. As the Personnel and operating offices, you should follow the program placement designations for offices and divisions at the regional level, as described in paragraph 8 of this chapter, unless circumstances unique to a region dictate that a program will be at a higher level. This is to ensure uniformity throughout the FAA in designating positions common in more than one region. To the extent that these programs exist at centers on a scale comparable to that of a region, you should apply the stated levels below.

a. Air Traffic	Moderate
b. Aircraft Certification	Moderate
c. Airports	Moderate
d. Airway Facilities	Moderate
e. Assistant Chief Counsel	Moderate
f. Aviation Medical	Moderate
g. Civil Rights	Limited
h. Flight Standards	Moderate
i. Human Resource Management	Limited

j. International Affairs	Major
k. Logistics and Procurement	Limited
l. Public Affairs	Moderate
m. Regional Administrator and immediate staff	Moderate
n. Regional Operations Center	Moderate
o. Resource Management	Limited
p. Security	Moderate

11. Regional Level Positions. The following are some positions common in most regions that Personnel and operating offices should designate at least at the levels shown. Other criteria and procedures in this chapter may require a higher level designation or designation as a sensitive position. Regional considerations can also dictate that a position warrants a higher designation because of other duties unique to that position in a particular region. Use this listing as guidance in designating other positions in the listed operating offices. To the extent that comparable positions exist at headquarters or at centers, positions there should be designated as shown below. The coding corresponds to that shown in paragraph 7 of this chapter.

Figure 3. Designated Positions

Position	Risk Level (Code)
a. Air Traffic:	
(1) Air Traffic Control Specialist (Center)	5
(2) Air Traffic Control Specialist (Terminal)	5
(3) Air Traffic Control Specialist (Flight Service Station)	1
(4) Air Traffic Assistant	1
b. Aircraft Certification:	
(1) Manager, Technical Support Staff	5
(2) Aerospace Engineer	5
(3) Aviation Safety Inspector	5

c. Airports:

- | | |
|--|---|
| (1) Manager, Airports District Office | 5 |
| (2) Program Officer/Executive Officer | 5 |
| (3) Airport Certification Safety Inspector | 5 |
| (4) Program Analyst | 1 |

d. Airway Facilities:

- | | |
|--|---|
| (1) Engineer | 5 |
| (2) Airway Transportation Systems Specialist | 5 |
| (3) Engineering Technician | 5 |
| (4) Electronics Technician | 5 |
| (5) Systems Management Office Manager | 5 |
| (6) Program Support Unit Manager | 5 |

e. Assistant Chief Counsel:

- | | |
|-----------------------------|---|
| (1) General Attorney | 5 |
| (2) Other support positions | 1 |

f. Aviation Medical:

- | | |
|---------------------------------------|---|
| (1) Assistant Regional Flight Surgeon | 5 |
| (2) Drug Abatement Program Manager | 5 |
| (3) Occupational Health Nurse | 1 |

g. Civil Rights: Equal Employment Opportunity Specialist 5**h. Flight Standards:**

- | | |
|-------------------------------|---|
| (1) Aviation Safety Inspector | 5 |
|-------------------------------|---|

i. Human Resource Management:

- | | |
|---|---|
| (1) Employment Branch Manager | 5 |
| (2) Personnel Staffing, Position Classification,
Employee Development, Employee Relations, and
Labor Relations Specialist | 5 |
| (3) Drug Program Coordinator | 5 |

(4) Assistants and Clerical personnel working with the employee drug program	1
(5) Employee Relations Specialist (Employee Assistance Program)	5
j. Logistics & Procurement: All positions, unless other criteria in this chapter apply	1
k. Public Affairs:	
(1) Public Affairs Specialist	5
(2) Writer/Editor	1
l. Regional Administrator & Regional Executive Manager	5
(1) Support Staff	5
m. Regional Operations Center: Regional Duty Officer	5
n. Information Resources:	
(1) Supervisory Computer Systems Administrator	6
(2) Supervisory Computer Systems Specialist	5
(3) Computer Specialist	5
(4) Computer Assistant	1
o. Security: Other criteria apply to all positions	6

CHAPTER 5. PERSONNEL SECURITY INVESTIGATION REQUIREMENTS AND PROCEDURES

Section 1. Investigative Requirements

1. General. This chapter prescribes FAA minimum investigative requirements and procedures for exceptions to those requirements. The position risk or sensitivity level, and, in some cases, the security clearance required of an employee holding the position, govern the type of investigation required. The personnel security specialist (PSS) located in a servicing security element (SSE) is responsible for initiating all investigations to the Office of Personnel Management (OPM).

2. Types and Scope of Background Investigations.

a. FAA requests the following investigations from OPM:

- (1) National Agency Check (NAC)
- (2) National Agency Check and Inquiries (NACI)
- (3) National Agency Check with Law Enforcement Inquiries and Credit (NACLC)
- (4) Child Care National Agency Check and Inquiries (CNACI)
- (5) Access National Agency Check and Inquiries (ANACI)
- (6) Minimum Background Investigation (MBI)
- (7) Limited Background Investigation (LBI)
- (8) Background Investigation (BI)
- (9) Single Scope Background Investigation (SSBI)
- (10) Reimbursable Suitability/Security Investigation (RSI)
- (11) Periodic Reinvestigation (PRI)
- (12) Periodic Reinvestigation with Residence Coverage (PRIR)
- (13) Periodic Reinvestigation for Single Scope Background Investigation (SSBI-PR)

(14) Upgrade Investigation (SGI, BGI, LGI). The SGI upgrades a BI to an SSBI; the BGI upgrades an LBI to a BI; and the LGI upgrades an MBI to an LBI.

(15) Update Investigation (SDI, BDI, LDI). The SDI updates an SSBI; the BDI updates a BI; and the LDI updates an LBI.

b. Special Agreement Checks. OPM will conduct Special Agency Checks to provide specific types of coverage tailored to an agency's needs. PSSs must obtain a release signed by the person before OPM can conduct any checks.

c. Minimum Coverage. All investigations will cover the most recent 3 years of a person's life but will not normally extend back beyond his or her 16th birthday unless necessary to obtain a minimum of 3 years of coverage or to resolve an issue.

d. Personal Interview. OPM will conduct one or more interviews of the Subject of the investigation in all SSBI, BI, MBI, LBI, SGI, BGI, SSBI-PR, LGI, and PRI cases.

e. Credit Searches. OPM will conduct credit searches as part of the NACLC, ANACI, MBI, LBI, BI, SSBI, PRI, SSBI-PR, SGI, BGI, LGI, BDI, and LDI. As the PSS, you must ensure that the Subject signs DOT F 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Report Act (Appendix F), authorizing OPM to conduct the search. Obtain the form *prior* to initiating any of the mentioned investigations, and keep it in the Subject's Personnel Security File (PSF). You do not need to send this form to OPM with the initiation of the investigation.

f. Expanded Coverage. The PSS can request that OPM expand all background investigations in scope and coverage as necessary to resolve an issue.

g. Extra Coverage.

(1) The PSS can request extra background investigation coverage of the following attributes, if it is appropriate to the position. OPM investigators may ask persons they interview additional questions about the Subject in order to cover them. These questions may include:

(a) Managerial or supervisory attributes, that includes ability to speak and write clearly and concisely; scope, quality, and extent of supervisory experience; ability to get people to work together effectively; resourcefulness; initiative; adaptability; judgment; discretion; ability to cooperate with co-workers, supervisors, and subordinates; and possible conflicts of interest.

(b) Public contact attributes, that include ability to meet and deal with all types of people, diplomacy, tact, personal appearance, and speaking ability.

(c) Law enforcement attributes, that include ability to react to emergencies and conditions of stress, maturity, stability, judgment, and discretion.

(d) Outside the United States attributes for Subject and spouse that include ability to represent the Government favorably; ability to meet and deal successfully and to adjust to a foreign environment; and whether there are any prejudices, defects in judgment, personal problems, traits, or weaknesses that might discredit the United States if the Subject is stationed in a foreign country.

(2) The SSE can negotiate with OPM for other special coverage in a background investigation if warranted by the position or by known suitability or security issues.

3. Basic Investigative Requirements. As the PSS, you must become familiar with the minimum investigative requirements for each sensitivity or risk-level designation.

a. Special-sensitive position. You must ensure that a person who is newly-hired; already working for the Federal Government and transferring to FAA from another agency; or an FAA employee who is assigned to work in a special-sensitive position has a completed SSBI. Evaluate and favorably adjudicate the SSBI for suitability and security before the person is placed in the position or the requirements of section 2, paragraph 1 of this chapter are met.

b. Critical-sensitive position. You must ensure that a person who is newly-hired; already working for the Federal Government and transferring to FAA from another agency; or an FAA employee who is assigned to work in a critical-sensitive position has a completed BI or SSBI. Evaluate and favorably adjudicate the SSBI or BI for suitability and security before the person is placed in the position or the requirements of section 2, paragraph 1 of this chapter are met.

c. Non-critical-sensitive position. You must ensure that:

(1) A newly-hired person has a completed ANACI or higher-level investigation that is evaluated and favorably adjudicated for suitability and security, or has met the requirements of section 2, paragraph 1 of this chapter.

(2) An FAA employee who is assigned to work in a non-critical-sensitive position has a completed, favorably adjudicated ANACI or higher level investigation, or has met the requirements of section 2, paragraph 1 of this chapter.

(3) A person already employed by the Federal Government who is transferring to FAA from another agency, has a completed, favorably adjudicated ANACI,

a NACLIC (as long as you can verify that another investigation containing the inquiries portion of the investigation was completed), or has met the requirements of section 2, paragraph 1 of this chapter.

d. High-risk position. You must ensure that a person who is newly-hired; already working for the Federal Government and is transferring to FAA from another agency; or an FAA employee who is assigned to work in a high-risk position has a completed BI or SSBI that is evaluated and favorably adjudicated, or has met the requirements of section 2, paragraph 1 of this chapter.

e. Moderate-risk position. You must ensure that:

(1) A person who is newly-hired; already working for the Federal Government and transferring to FAA from another agency; or an FAA employee who is assigned to work in a moderate-risk position has a completed NACI or higher-level investigation that is evaluated and favorably adjudicated, or has met the requirements of section 2, paragraph 1 of this chapter.

(2) A person who is newly-hired; already working for the Federal Government who is transferring to FAA from another agency; or an FAA employee who is assigned to work in a moderate-risk position with fiduciary responsibilities has a completed NACI and credit check, a higher-level investigation that is evaluated and favorably adjudicated, or the requirements of section 2, paragraph 1 of this chapter are met. These positions might include, but are not limited to, contracting officers, contract specialists, positions in accounting or budget, and other positions where the incumbent has a major responsibility involving authority or ability to obligate, control, or expend public money or items of monetary value.

f. Low-risk position. You must ensure that a NACI is initiated within 14 days after the person is placed in the position and evaluated and favorably adjudicated as soon as possible upon completion.

g. Periodic Reinvestigations (SSBI-PR, PRI and NACLIC). You must ensure that:

(1) An SSBI-PR is completed within 5 years from the date of the last SSBI or SSBI-PR on each incumbent of a special-sensitive position and on each incumbent of a critical-sensitive position for which the position requires a Top Secret security clearance. Review the PSF and the Official Personnel Folder (OPF), if available, as part of the SSBI-PR.

(2) A PRI is completed within 5 years from the date of the last BI, SSBI or PRI on each incumbent of a high-risk position or a critical-sensitive position for which the position requires a Secret clearance. Review the PSF and OPF, if available, as part of the PRI.

(3) A NACLCL is completed within 10 years from the date of the last investigation or reinvestigation on each incumbent of a non-critical-sensitive position if the position requires a Secret clearance. Review the PSF and OPF, if available, as part of the NACLCL.

h. Credit checks for fiduciary positions. You must conduct a credit check on all persons employed in positions with fiduciary responsibilities at least once every 5 years, regardless of other investigation requirements that may apply. Initiate a credit check unless the employee signs DOT Form 1631 or one is on file in the PSF. If a person is being placed in a position with fiduciary responsibilities and there is no pre-placement investigation required, or if such a requirement is waived, you should conduct a credit check as soon as possible, but not later than 14 days after placement. You do not need to conduct a new credit check if one was conducted within the last 5 years as part of another investigation.

i. Upgrade Investigations. You must conduct the appropriate Upgrade Investigation (SGI, BGI or LGI) when an MBI, LBI or BI was completed within the past 5 years, and the next higher level investigation is now required because an employee is being promoted or reassigned to a position with a higher risk or sensitivity level. This investigation will bring the required investigation up to standards. It must be completed, evaluated and favorably adjudicated before the person is placed in the position or has met the requirements of section 2, paragraph 1 of this chapter.

j. Update Investigations. You must conduct the appropriate Update Investigation (SDI, BDI or LDI) in lieu of the required investigation whenever an LBI, BI or SSBI was completed within the past 5 years, the same level investigation is now required, or the person had a break in Federal service of more than 2 years.

k. Investigations on former Federal employees. You must conduct the required investigation on any former Federal employee who has had a break in service in excess of 2 years. If there is no break in service in excess of 2 years, a new investigation is not required unless there is a periodic reinvestigation requirement or an upgrade investigation is necessary. You must credit any one or a combination of the following employments the same as Federal employment when determining continuity of service:

(1) Active duty in any branch of the U.S. military service.

(2) Employment for or as a U.S. Government contractor for which the person had an investigation conducted by a Government agency.

(3) Employment by the District of Columbia Government.

l. Changes in risk or sensitivity level. An employee can remain in a position when there is a change to the risk or sensitivity level, however, you must initiate a new investigation within 14 days of the change, if one is required.

m. Movement from a public trust position to a national security position. If an employee moves from a position of public trust to one of national security, he or she must complete an SF-86 for your review before placement. You do not need to conduct a reinvestigation if the employee already has the required investigation for the position unless an update is needed, or information disclosed on the newly completed SF-86 or other special circumstances warrant additional investigation.

n. Incomplete investigations. You may determine that an investigation received from OPM that is not entirely complete can be adjudicated for suitability and security if the outstanding portion is not likely to affect a final adjudication or help to resolve any issues. Consider such an investigation complete for the purpose of meeting a pre-placement investigation requirement. (This investigation is also referred to as an OPM closed pending case.)

o. Military personnel and medical records checks. You should request military and medical records for persons who are being considered for safety-related positions when there is evidence of prior military service. You can also request a military records check on any person to help resolve suitability or security issues raised during the investigative process.

4. Specific Requirements: Special-Sensitive Positions.

Case Circumstances

Investigation/Action Required

a. Candidate with no prior investigation.

SSBI completed prior to placement.

b. Candidate with prior SSBI completed within past 5 years, and no break in service of 2 years or more.

Review prior investigation, current records, and personal history statement. No SDI necessary unless needed to resolve a suitability or security issue.

c. Candidate with prior SSBI completed within past 5 years, but break in service of more than 2 years.

Review prior investigation, current records, and personal history statement, and completion of SDI before placement.

d. Candidate with prior SSBI completed more than 5 years ago (with no updating investigation), but no break in service.

SSBI. May be post-placement.

- | | |
|--|---------------------------------------|
| e. Candidate with prior SSBI completed more than 5 years ago (with no updating investigation) and any break in service. | SSBI completed prior to placement. |
| f. Candidate with BI completed within the past 5 years. | SGI completed prior to placement. |
| g. Candidate with LBI, MBI, ANACI, NACI, or NAC. | SSBI completed prior to placement. |
| h. Candidate is incumbent of another special-sensitive position whose last investigation was completed 5 or more years ago. | SSBI-PR completed prior to placement. |

5. Specific Requirements: Critical-Sensitive Positions.

Case Circumstances

Investigation/Action Required

- | | |
|---|--|
| a. Candidate with no prior investigation. | SSBI or BI completed prior to placement. |
| b. Candidate with prior SSBI completed within past 5 years and no break in service of 2 years or more. | Review prior investigation, current records, and personal history statement. No new investigation necessary unless needed to resolve suitability or security issue. |
| c. Candidate with prior BI completed within past 5 years and no break in service of 2 years or more. | Review prior investigation, current records, and personal history statement. If position requires Top Secret clearance, initiate SGI, which may be completed post-placement. Otherwise, no new investigation necessary unless needed to resolve suitability or security issue. |

- | | |
|---|---|
| d. Candidate with prior SSBI or BI completed within past 5 years, but break in service of more than 2 years. | Review prior investigation, current records, and personal history statement. If position requires a Top Secret clearance, SGI or SDI completed prior to placement. Otherwise, BDI completed prior to placement. |
| e. Candidate with prior SSBI or BI completed more than 5 years ago (with no updating investigation), but no break in service. | SSBI-PR if Top Secret clearance required; otherwise, PRI. May be post-placement. |
| f. Candidate with prior SSBI or BI completed more than 5 years ago (with no updating investigation), and any break in service. | SSBI or BI completed prior to placement. |
| g. Candidate with LBI completed within past 5 years. | SSBI completed prior to placement if Top Secret clearance required. Otherwise, BGI completed prior to placement. |
| h. Candidate with MBI, ANACI, NACI, or NAC. | SSBI or BI completed prior to placement. |
| i. Candidate is incumbent of critical-sensitive or high-risk position whose last BI or SSBI was completed 5 or more years ago. | Initiate SSBI-PR or PRI. May be completed post-placement. |

6. Specific Requirements: Non-critical-Sensitive Positions.

Case Circumstances

Investigation/Action Required

- | | |
|--|---|
| a. Candidate with no prior investigation. | ANACI and Subject interview completed prior to placement. |
| b. Candidate with prior SSBI, BI, LBI, MBI, and Subject interview completed within the past 5 years and no break in service of more than 2 years. | Review prior investigation, current records, and personal history statement. No new investigation necessary unless needed to resolve suitability or security issue. |

- | | |
|---|--|
| c. Candidate with prior SSBI, BI, LBI, MBI, NACI and Subject interview, but break in service of more than 2 years. | New NACI with credit and Subject interview completed prior to placement. |
| d. Candidate with a NACI or NAC. | NACI with credit and Subject interview completed prior to placement. |
| e. Candidate is incumbent of non critical-sensitive position whose last ANACI or NACLCLC was more than 10 years ago. | Initiate a NACI with credit or NACLCLC. May be post-placement. |

7. Specific Requirements: High-Risk Positions.

Case Circumstances

Investigation/Action Required

- | | |
|--|--|
| a. Candidate with no prior investigation. | BI completed prior to placement. |
| b. Candidate with prior SSBI or BI completed within past 5 years, and no break in service of 2 years or more. | Review prior investigation and current records. No new investigation necessary unless needed to resolve suitability issue. |
| c. Candidate with prior SSBI or BI completed within past 5 years, but break in service of more than 2 years. | Review prior investigation, current records, and personal history statement. BDI completed prior to placement. |
| d. Candidate with prior SSBI or BI completed more than 5 years ago (with no updating investigation), but no break in service. | PRI. May be post-placement. |
| e. Candidate with prior investigation of any type completed more than 5 years ago (with no updating investigation), and any break in service. | BI completed prior to placement. |
| f. Candidate with LBI completed within past 5 years. | BGI completed prior to placement. |

g. Candidate with MBI, ANACI, NACI, or NAC.

BI completed prior to placement.

h. Candidate is incumbent of critical-sensitive or high-risk position whose last BI or SSBI was completed 5 or more years ago.

Initiate PRI. May be completed post-placement.

8. Specific Requirements: Moderate-Risk Positions.

Case Circumstances

Investigation/Action Required

a. Candidate with no prior investigation.

NACI completed prior to placement. If position has fiduciary responsibilities, NACI with credit completed prior to placement.

b. Candidate with prior SSBI, BI, LBI, MBI, ANACI, or NACI completed within the past 5 years and no break in service of more than 2 years.

Review prior investigation, current records, and personal history statement. If position has fiduciary responsibilities, initiate credit check if not previously done. No additional investigation necessary unless needed to resolve a suitability issue.

c. Candidate with prior SSBI, BI, LBI, MBI, ANACI, NACI, or NACI, but break in service of more than 2 years.

New NACI completed prior to placement. If position has fiduciary responsibilities, NACI with credit completed prior to placement.

d. Candidate with NAC.

NACI initiated prior to placement. If position has fiduciary responsibilities, NACI with credit initiated prior to placement.

e. Candidate is incumbent of non-critical-sensitive or moderate-risk position whose last investigation was more than 5 years ago.

Review prior investigation, current records, and personal history statement. If position has fiduciary responsibilities, initiate credit check. No additional investigation necessary unless needed to resolve a suitability issue.

9. Specific Requirements: Low-Risk Positions.

Case Circumstances	Investigation/Action Required
a. Candidate with no prior investigation.	NACI initiated no later than 14 days after placement.
b. Candidate with prior NACI, MBI, LBI, ANACI, BI, SSBI, and no break in service of more than 2 years.	If not current FAA employee, review prior investigation. No new investigation necessary unless needed to resolve a suitability issue.
c. Candidate with prior NACI, MBI, LBI, BI, or SSBI, but break in service of more than 2 years.	NACI initiated no later than 14 days after placement.
d. Candidate with NAC.	NACI initiated no later than 14 days after placement.

10. Specific Requirements for Certain Positions.

a. Communications Security (COMSEC) positions. The latest edition of FAA Order 1600.8, Communications Security (COMSEC), contains specific investigative requirements for COMSEC manager and alternate COMSEC manager positions. These requirements are in addition to those contained in this chapter.

b. Positions in the Office of the Assistant Administrator for Security and Hazardous Materials, ASH-1. A BI is the minimum level investigation conducted on all employees in ASH and subordinate offices. All ASH personnel in positions designated special sensitive or critical sensitive will be subject to the investigation required for their level.

11. Exceptions to Investigative Requirements. As the PSS, you should become familiar with the below exceptions to investigative requirements.

a. Exempt Positions. Certain low-risk positions are exempt from the investigative requirements. These positions may include: intermittent, seasonal, per diem, or temporary, in which a person's employment does not exceed an aggregate of 180 days in either a single continuous or series of appointments; and positions located outside the United States that are occupied by persons who are not U.S. citizens. You must not grant access to classified information or to restricted areas for security reasons to these people. Although no investigation is required for these people, it is recommended that you conduct a fingerprint check.

b. Detailed Positions/Temporary Promotions. An employee must meet the normal investigative requirements if a detail or temporary promotion is into a special-sensitive, critical-sensitive, non-critical-sensitive, high-risk, or moderate-risk position, prior to any detail or temporary promotion that is in excess of 120 days. You must ensure that the employee has the required investigation for the clearance if access to classified information is required. Review the prior investigation; OPF, if available; PSF; and current investigative forms if the detail is to a special-sensitive, critical-sensitive, or high-risk position is less than 120 days. If a detail originally scheduled for 120 days or less is unexpectedly extended for another period of 120 days or less, you can let the employee continue in the position without meeting the normal investigative requirements. Do not allow the employee to continue in a series of details in excess of 240 days unless the required investigation is in progress or the requirements of section 2, paragraph 1 of this chapter are met.

c. Other Positions. You are not required to conduct an investigation for persons who are not paid by the FAA for their services, such as, volunteers, interns, experts, etc. It is, however, recommended that you conduct a fingerprint check on them.

Section 2. Waiver Requirements

1. Waiver of Pre-Placement Investigative Requirements.

a. Criteria.

(1) E.O. 10450 requires that waiver of the pre-placement investigative requirements on persons entering sensitive positions may be made only "in case of emergency" provided the department or agency concerned finds that such action is necessary in the national interest. The Office of the Secretary, Office of Security, M-40, has delegated the authority to AIN-1 to grant waivers for persons entering special-sensitive and critical-sensitive positions. FAA has adopted procedures whereby AIN-1 in conjunction with the Human Resource Management Divisions (Personnel) can approve the placement of persons entering non-critical-sensitive positions, provided the procedures in section 2, paragraph 1c(2) are met. AIN-1 has further delegated this authority to the servicing security elements (SSE).

(2) As the personnel security specialists (PSS), you will provide authorization and assurance to the Personnel or operating offices that either the pre-placement investigative requirements were met or you granted a waiver prior to appointing a person to a sensitive position. Personnel or operating offices cannot make a firm starting date commitment to a person to begin working in such a position until you have given them authorization to do so. If, through clerical or other error, a person is permanently appointed to a sensitive or public trust position without meeting the investigative requirements, the Personnel or operating office must contact you immediately to initiate the appropriate investigation.

(3) FAA has adopted procedures whereby AIN-1 in conjunction with the Personnel office may approve a person's placement in a moderate-risk or high-risk position prior to the completion of the appropriate investigation, provided that the procedures outlined in section 2, paragraph 1c(1) and (3) are followed. AIN-1 has delegated this authority to the SSE to approve all placements for persons in moderate-risk positions.

b. Request and processing procedures. If you are the operating office, you must follow the procedures below when requesting a waiver.

(1) You must submit a written request to your SSE for a waiver of a pre-placement investigative requirement. This request must include:

(a) the nature of the waiver being requested; e.g., a waiver to allow appointment (reassignment, promotion, etc., as applicable) of (name of Subject) to a (position risk or sensitivity level) position prior to completion of the required investigation;

(b) the position's title, grade, and location;

(c) a justification of the emergency situation; e.g., critical operational impact if the person cannot be placed in the position at the present time or by a particular date; and

(d) the level of security clearance required, if for a sensitive position, justification of the need for that clearance, and a statement that the person will not have access to classified information until the required investigation is completed and the SSE has granted the necessary clearance.

(2) You must submit the waiver request to your SSE, as soon as possible, allowing at least 3 weeks for processing for special-sensitive, critical-sensitive and high-risk positions.

(3) You or your Personnel office will advise the applicant of the need to obtain a waiver and the importance of promptly submitting all required forms to the SSE. Your SSE will contact the applicant for an interview for special-sensitive, critical-sensitive and high-risk positions.

(4) You must wait until your SSE approves the waiver or provides assurance that the investigation requirements have been met before you make a firm starting date commitment to any applicant.

c. SSE Processing. If you are the PSS from the SSE, you must follow the procedures below when processing a waiver request.

(1) Special-sensitive, critical-sensitive, and high-risk positions. For waiver requests for these positions, you must:

(a) Review the operating office's request for inclusion of all required information, including sufficient justification, and promptly re-contact that office if the request is incomplete.

(b) Obtain the candidate's completed investigative forms (SF-86, Questionnaire for National Security Positions or SF-85P, Questionnaire for Public Trust Positions, and SF-86A, Continuation Sheet for Questionnaires SF-86, SF-85P, and SF-85, if applicable); Optional Form (OF) 306, Declaration for Federal Employment; employment application; and DOT Form 1631.

(c) Conduct a Subject interview covering, but not limited to, past and present employment, education, and residences; arrests and convictions; use of alcohol and illegal drugs; mental health; and financial responsibility. Ask the Subject if there is anything in his or her background that could raise a question of personal character or loyalty to the United States. Use the questions on the investigative forms as a guide in conducting the interview, and ask the Subject about any information furnished on them that is not entirely favorable. Conduct the interview telephonically when the Subject is not readily available for a personal interview at your office.

(d) Check with the appropriate law enforcement agency or previous employer if information appears on the Subject's investigative forms or employment application that raises a significant security or suitability issue. Disapprove the waiver request unless you are satisfied that the issues stated below have been adequately addressed. These issues are:

1 Any arrests, charges, convictions, or incarceration within the last 5 years.

2 Any drug-related arrests, regardless of when they occurred.

3 More than one felony arrest, regardless of when they occurred.

4 Any discharge from employment or resignation after being told he or she would be fired, within the last 5 years.

5 Any discharge from employment involving drug or alcohol use, or a question of the applicant's integrity, regardless of when it occurred.

- (e) Document, date, and sign written results of the Subject interview, including specific mention of the elements covered in the interview and a summary of any information the Subject provided that was not completely favorable. Also include the Subject's explanation about any information furnished on the investigative forms or employment application that is not entirely favorable.
- (f) Conduct a credit check.
- (g) Conduct law enforcement searches, if possible.
- (h) Contact the Subject's current or most recent former employer.
- (i) Review the PSF, if available, and conduct a check of the agency's databases for records of any FAA investigation, if the candidate is a current or former FAA employee.
- (j) Contact the current or former employing agency's security office (for current and former Federal employees only), if other than FAA.
- (k) Address any other issues, such as admitted drug or alcohol use, financial problems, treatment for a mental condition, security clearance revocation, other-than-honorable military discharge, or association with a questionable organization, with regard to the nature, extent, and recency of the conduct, before granting the waiver.
- (l) Initiate the required investigation and enter the information into the FAA-approved database.
- (m) Prepare a transmittal memorandum to AIN-400 if there is no significantly unfavorable information regarding the Subject and if the operating office's request contains sufficient justification. You should include in the memorandum:
 - 1 Nature of waiver request; i.e., from (operating office identification), to place (name of applicant) into a (position sensitivity or risk level).
 - 2 Subject's current security clearance, if any, and basis; and title and grade level of Subject's present position, if FAA employed. In addition, state the results of a review of Subject's PSF.
 - 3 The type, date, and results of any previous investigation(s), if not FAA employed. If you cannot review the previous investigation within a reasonable period of time, so stipulate. Indicate results of

telephonically conducted checks with Subject's present or most recent employer.

4 Date and results of the Subject interview, including specific mention of the elements covered in the interview and a summary of any information the Subject provided that was not completely favorable. Include the Subject's explanation about any information furnished on the investigative forms or employment application that is not entirely favorable.

5 The date the investigation was sent to OPM. A copy of Subject's investigative forms and employment application should be attached.

6 The results of the credit search, any local agency and law enforcement checks.

7 Your recommendation for approval.

8 The request from the operating office.

(2) Non-critical sensitive. For placement of persons in non-critical-sensitive positions, you must:

(a) Review the operating office's request for inclusion of all required information, including sufficient justification, and re-contact that office if the request is incomplete.

(b) Obtain and review the candidate's completed investigative forms; OF-306; employment application; and DOT F 1631, if applicable, and conduct appropriate local agency checks as necessary.

(c) Review the PSF, if available, and check the appropriate FAA-approved database for records of any FAA investigation, if the candidate is an FAA employee.

(d) Check with the appropriate law enforcement agency or previous employer if information appears on the Subject's investigative forms or employment application that raises a significant security or suitability issue. Disapprove the waiver request unless you are satisfied that the issues are adequately addressed. These issues are:

1 Any arrests, charges, convictions, or incarceration within the last 5 years.

2 Any drug-related arrests, regardless of when they occurred.

3 More than one felony arrest, regardless of when they occurred.

4 Any discharge from employment or resignation after being told he or she would be fired, within the last 5 years.

5 Any discharge from employment involving drug or alcohol use, or a question of the applicant's integrity, regardless of when it occurred.

(e) Address any other issues, such as admitted drug or alcohol use, financial problems, treatment for a mental condition, security clearance revocation, other-than-honorable military discharge, or association with a questionable organization, with regard to the nature, extent, and recency of the conduct, before granting the waiver.

(f) Conduct a Subject interview only if the documents provided, or the information obtained, contain unfavorable information. Conduct the interview telephonically when the applicant or employee is not readily available for a personal interview at your office. The Subject interview must cover, but not be limited to, past and present employment, education, and residences; arrests and convictions; use of alcohol and illegal drugs; mental health; and financial responsibility. Use questions from the investigative forms as a guide in conducting the interview.

(g) Document, date, and sign written results of Subject interview, including specific mention of the elements covered in the interview and a summary of any information the Subject provided that was not completely favorable. Also include the Subject's explanation about any information furnished on the investigative forms or employment application that is not entirely favorable.

(h) Approve the request if satisfied that it is justified and that the available information raises no significant security or suitability issues, and notify your Personnel office to place the person in the position. If you disapprove the request, notify your Personnel office not to place the person in the position.

(3) Moderate risk. For placement of persons in moderate risk positions, you must:

(a) Obtain and review the candidate's completed investigative forms, OF-306; employment application; and DOT F 1631, if applicable, and conduct appropriate local agency checks as necessary. Review the PSF, if available, and check the appropriate FAA-approved database for records of any investigation if candidate is an FAA employee.

(b) Check with the appropriate law enforcement agency or previous employer if information appears on the Subject's investigative forms or employment application that raises a significant security or suitability issue.

Disapprove the waiver request unless you are satisfied that the issues are adequately addressed. These issues are:

- 1 Any arrests, charges, convictions, or incarceration within the last 5 years.
- 2 Any drug-related arrests, regardless of when they occurred.
- 3 More than one felony arrest, regardless of when they occurred.
- 4 Any discharge from employment or resignation after being told he or she would be fired, within the last 5 years.
- 5 Any discharge from employment involving drug or alcohol use, or a question of the applicant's integrity, regardless of when it occurred.

(c) Conduct a Subject interview only to resolve issues if the documents provided, or information obtained, contain unfavorable information. Conduct the interview telephonically when the applicant or employee is not readily available for a personal interview at your office. Do not conduct an interview if the documents provided are favorable.

(d) Document, date, and sign written results of Subject interview, including specific mention of the elements covered in the interview and a summary of any information the Subject provided that was not completely favorable. Also include the Subject's explanation about any information furnished on the investigative forms or employment application that is not entirely favorable.

(e) Approve the request if the available information raises no significant security or suitability issues, and notify your Personnel office to place the person in the position.

(f) Disapprove the request if the available information raises significant security or suitability issues that cannot be adequately addressed during the waiver process, and notify your Personnel office not to place the person in the position until the investigation is completed, and you have favorably adjudicated it.

(4) AIN-400 processing and notification of decision. For special-sensitive, critical-sensitive, and high-risk positions, AIN-400 will promptly review each of your waiver requests for sufficiency of justification and inclusion of all required information. They will grant the waiver and notify you in writing of the approval if there is no significantly unfavorable information. AIN-400 will disapprove any waiver request that contains significantly unfavorable or questionable information and contact you directly.

2. Special Procedures for Accelerated Hiring.

a. The Office of Internal Security and Investigations and the headquarters Office of Human Resource Management can jointly enter into an agreement with particular operating offices to establish procedures for accelerated hiring of applicants into specific safety-critical positions. Each SSE and their corresponding Personnel office can also enter into these agreements. The procedures under such an agreement permit applicant hiring following basic qualification determinations and limited initial security investigation. The Office of Aviation Medicine (Medical) is normally a party to the agreement, if the position requires applicants to meet certain medical qualifications. Each involved organization will conduct part of the process and satisfactorily complete it before Personnel or operating offices can give applicants hiring commitments. The security procedures under such an agreement will allow for accelerated hiring while still providing for some basic background checks on applicants prior to hiring. The procedures can be used for non-critical-sensitive and moderate-risk positions and are an alternative to a waiver of the pre-placement investigative requirements processed under section 2, paragraph 1 of this chapter.

b. When the SSE, Personnel, Medical, and an operating office agree to apply accelerated hiring procedures to a particular category of positions, they must also agree on the specific security checks to be conducted before the SSE gives personnel security approval to begin the process. At a minimum, the PSS must:

- (1) Review the completed employment application and investigative forms.
- (2) Conduct a fingerprint check with OPM.
- (3) Conduct checks with state or local law enforcement agencies covering areas where the applicant has worked or lived for a significant period of time during the most recent 5 years.

c. The SSE and Personnel must also agree to conduct a check of military records and record indices at the National Personnel Records Center in St. Louis, Missouri, for information pertinent to security, suitability, and medical qualifications. The PSS must conduct the checks on all applicants, whether or not they claim to have served in the military, and furnish any medical information obtained to Medical through the appropriate office.

d. The SSE can issue implementing instructions for the security processing of applicants under these procedures and do so jointly with Personnel and other concerned offices. These instructions may specify, for example, that employees from an operating office interview applicants and review the employment application and the investigative forms, and make an initial determination as to whether or not an applicant can continue to be processed for hiring prior to completion of the required investigation.

e. Personnel cannot hire an applicant under these procedures prior to completion of the required investigation if any of the issues listed below were admitted by the applicant in the employment application or investigative forms, or if the checks conducted revealed any of the issues. The PSS must make every effort to adequately address the issues below before notifying their Personnel office.

- (1) Any arrests, charges, convictions, or incarceration within the last 5 years.
- (2) Any drug-related arrests, regardless of when they occurred.
- (3) More than one felony arrest, regardless of when they occurred.
- (4) Any discharge from employment or resignation after being told he or she would be fired, within the last 5 years.
- (5) Any discharge from employment involving drug or alcohol use, or a question of the applicant's integrity, regardless of when it occurred.

f. Personnel or operating offices cannot commit to hiring an applicant being processed under these procedures without specific approval from their SSE.

g. The SSE can initiate the required investigation at any time; or, at the latest, within 14 days following the date the person enters on duty, after granting approval to hire an applicant, once they have completed the required checks.

Section 3. Investigation Process

1. Initiating, Monitoring, and Closing Investigations. As the personnel security specialist (PSS), you are responsible for ensuring that all requests for investigations are submitted to OPM as required by this chapter. Human Resource Management Divisions (Personnel) are responsible for obtaining, or working with operating offices to obtain, all completed forms from applicants and employees. Section 4, paragraph 1 of this chapter specifies the forms to be submitted for each type of investigation. You must work together with your Personnel and operating offices to ensure that the necessary investigations are requested as required.

a. Initiating investigations for new hires and reassignments.

- (1) Personnel and operating offices must ensure that employees and applicants are not entered on duty into other than low-risk positions without prior approval from you. They must ensure that applicants or employees complete all necessary investigative forms. Forms can be completed either electronically or manually and must be submitted to the SSE for processing. Currently applicants and employees are using a fill-in version of the electronic form, however, OPM is

instituting an agency-wide electronic system called the Electronic Questionnaires for Investigations Processing (e-Qip) system. The e-Qip system is a secure website that is designed to house all personnel investigative forms. Instead of distributing paper forms to prospective applicants and Subjects of investigations, agencies will authorize a user into the e-Qip system where the user completes the forms on-line and submits it to the SSE. This system is being slowly integrated into FAA, however, in the future, e-Qip will be the sole system for completing and submitting security forms.

(2) As the PSS, you must review the investigative forms for accuracy and completeness, and for any possibility of a previously conducted investigation, and return any forms that are incomplete to your Personnel or operating office, applicant, or employee. Your Personnel or your operating office must then ensure that the applicant or employee makes the appropriate correction(s) and the forms get returned to you. The operating office will assist you and the Personnel office by ensuring that an employee promptly completes, submits, and corrects, as necessary, all required investigative forms.

(3) As the PSS, you must enter the required information and the OPM-assigned Security Office Identifier (SOI) on the personnel security questionnaire, and initiate the investigation to OPM for processing. Section 4, paragraph 1 of this chapter specifies the forms needed for each type of investigation.

b. Investigations on employees due to upgraded risk or sensitivity level, need for access to classified information, or need for periodic reinvestigation. As the PSS, you must:

(1) Notify your operating office when an employee requires an investigation for one of the reasons stated above. The operating office must see that you promptly receive all necessary investigative forms from the employee. If the employee requires a new investigation because the risk or sensitivity level was upgraded, he or she must submit the investigative forms to you within 12 days from the date on which the upgrade takes effect. If a PRI or SSBI-PR is required, or the investigation is needed for you to grant access to classified information, the employee must ensure that they give you the investigative forms within 14 days from the date they are requested.

(2) Review the investigative forms for accuracy and completeness, and return incomplete forms to the employee. The employee must promptly make any correction(s) necessary and return the forms back to you. Your operating office can assist by making sure that the employee promptly corrects and resubmits, as necessary, all required forms.

(3) Enter the required information and the OPM-assigned SOI on the personnel security questionnaire and initiate the investigation to OPM for processing.

(4) Send all investigative forms for SSE managers assigned to your region to AIN-400 for review and initiation of the appropriate investigation, and adjudication of the completed investigation. Review and initiate investigative forms for PSSs and assistants assigned to your region, but use the AIN-400 SOI so that OPM will send the completed investigation directly to them for adjudication. Take all reasonable steps to ensure that reports of investigation on SSE employees are not opened by, or otherwise made accessible to, the Subject of the investigation. In no case will the Subject of an investigation be involved in his or her initiation or processing other than by furnishing the required forms and providing other requested information.

(5) Ensure that all investigative forms for FAA Executives are submitted to AIN-400 for processing.

c. Payment for investigations.

(1) If you are an operating office or division, you must:

(a) Fund personnel security investigations through operational funds to pay for investigations on your employees and on applicants applying for positions in your office.

(b) Provide the SSE with the accounting code information necessary to have the costs charged appropriately, unless there has been a specific allotment made to them to pay for all investigations for operating offices it services.

(2) If you are an SSE, your PSS must:

(a) Enter accounting code information in the Agency Use Only block on the investigative forms.

(b) Make a copy of the portion of the first page that contains the Agency Use Only block and the employee's or applicant's name, and send it to the appropriate headquarters, regional, or center accounting division.

(3) SSEs and their operating offices and divisions can use other acceptable methods for notifying their accounting division.

d. Submission to OPM. PSSs must complete the entire package as outlined in section 4, paragraph 1 of this chapter, and transmit it to OPM either electronically or by mail to OPM, FIPC, Boyers, Pennsylvania 16018.

e. Discontinuing investigations. As the PSS, you should:

(1) Discontinue an investigation whenever it becomes clear that the investigation is no longer needed, such as, when an applicant is no longer being considered for

employment or an employee leaves the FAA. Coordinate with M-40, OST, when a person transfers to another DOT administration. Your Personnel and operating offices must immediately notify you when they become aware that discontinuing an investigation is warranted.

(2) Telephonically advise OPM to discontinue an investigation. You may follow up with written notification that includes the reason for the discontinuance.

(3) Notify your servicing accounting office and advise your operating office of the expected charge for the incomplete investigation, if any. Contact OPM to resolve any subsequent question as to the charge for an incomplete investigation, if necessary.

f. Completion of investigations and documentation.

(1) The SSE will be sent all reports of investigation from OPM identified by the SOI code on the investigative forms. The PSS must review all reports and provide the employee or applicant with the opportunity to respond to unfavorable information, as required by chapter 2, paragraph 2 of this order, whenever a report raises issues that warrant taking unfavorable action against the person investigated.

(2) The SSE will receive a completed certification of investigation from OPM with each completed investigation. An SSE official must sign the certification and forward it to the Personnel office to file in the permanent side of the employee's OPF. The SSE must retain the certification with the reports of investigation, if the investigation was conducted on an applicant who is not subsequently hired.

2. Additional Security Investigation. The SSE can conduct an additional investigation on a completed report of investigation from OPM, if necessary, prior to making a suitability or security determination.

a. Criteria for opening an investigation.

(1) As the PSS, you can request that an investigation be opened whenever:

(a) the additional work required consists of interviews with additional sources or extensive records checks;

(b) there is at least one material, unresolved issue, the resolution of which is necessary to make a suitability or security determination; and

(c) the Subject of investigation is still an employee or under active consideration for employment.

- (2) As the PSS, you should not request that an investigation be opened:
- (a) solely to conduct an interview with an employee or applicant, or to conduct brief, follow-up records checks with courts or law enforcement agencies;
 - (b) to conduct checks that can be conducted electronically or by mail;
 - (c) when existing reports resolve all material issues, such as, issues whose resolution will be likely to affect a suitability or security determination;
 - (d) when admissions by the Subject provide sufficient information on which to make a suitability or security determination; and
 - (e) when issues, even if unresolved, are minor or in the distant past, and resolution would not affect a suitability or security determination.

b. Procedures. The SSE must conduct all investigations according to the procedures in the latest edition of FAA Order 1600.20, Civil Aviation Security Investigations Handbook. If an investigation is not necessary, the PSS must interview the Subject or send a letter or memorandum to him or her to fulfill the due process requirements prescribed in chapter 2, paragraph 2 of this order.

c. Documentation. If the PSS finds that there is substantial investigative work in addition to an interview with the employee or applicant, all of the investigative results, including the interview, should be reported in an FAA report of investigation. The PSS should prepare a memorandum to the PSF to document the results of an interview, any written statement from the Subject, and any additional checks they conducted. Sign and date all documentation.

3. Reciprocity, Standards and Procedures for Using Previous Investigations.

a. Some applicants for FAA employment and some newly-hired employees, especially persons transferring from other Government agencies, will have already been investigated by a Federal department or agency. As the PSS, you must use these investigations when practicable to reduce the number of investigations that FAA requests from OPM, thereby reducing investigative costs and avoiding delays in waiting for investigations to be completed.

b. As the PSS, do not duplicate any previously conducted background investigation when it meets the scope and standards for the level of a security clearance required. Your SSE is responsible for granting security clearances and determining whether a person was previously cleared or investigated by the U.S. Government. You must use any previously

granted security clearance that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance as the basis for issuance of a new clearance without further investigation or adjudication.

c. As the PSS, you should accept previously conducted investigations and access adjudications, if available, without requiring additional investigations, unless there is a break in the person's Federal employment or military service in excess of 2 years, or unless you are aware of unfavorable information about the person that might affect a security adjudication and that was unknown at the time of the previous investigation. Do not apply this requirement if a previous clearance was an interim or temporary one and was not based on a completed investigation of the type required for a final clearance at that level.

d. As the PSS, you should be alert to any information indicating that the applicant had a previous investigation. When reviewing investigative forms look for information, such as, recent Federal employment; military service, including service with the National Guard or reserves; employment with a Government contractor where the person might have had a comparable investigation; and a claim by the person that he or she had a previous investigation or a security clearance.

e. As the PSS, you should review previous investigations when readily available prior to giving your Personnel or operating office permission to employ a person in a sensitive or public trust position. If possible, obtain a copy of the investigation for the person's PSF.

f. As the PSS, you should obtain as much information as possible about a previous investigation if one is not readily available before the person is employed in a sensitive or public trust position. Contact the agency that conducted the investigation, an employing agency's security office, or an agency that granted the person a security clearance for investigation information, and request a copy of the investigation and review it as soon as possible.

g. An investigation conducted by a state or local government agency can provide useful information, particularly in determining whether or not to waive a pre-placement investigative requirement. However, the PSS cannot use this investigation regardless of how extensive it is, because it does not meet investigative requirements for Federal employment.

4. Obtaining and Reviewing Previous Investigations.

a. OPM.

(1) OPM maintains the Security/Suitability Investigations Index (SII), which is an index of investigations conducted by them and certain other Federal agencies. If you are the PSS, you must check this index whenever there is an indication that

they or another agency have conducted an investigation. Conduct the SII check telephonically; by completing Office of Federal Investigations (OFI) Form 79B, Request for Search of OPM Records, and sending it to OPM, Federal Investigations Processing Center (FIPC), Boyers, Pennsylvania, 16018; or electronically, if you can do that through a direct data link to FIPC. Provide the SOI that OPM has assigned to you when writing or telephoning request.

(2) Other investigations. When an SII check or other documentation reveals that OPM previously conducted another type of investigation, the PSS must obtain and review a copy of that investigation.

b. Department of Defense (DOD).

(1) DOD indexes its investigations in the Defense Central Investigations Index (DCII), maintained by the Defense Security Service (DSS). These include investigations on military personnel, DOD civilian employees, and DOD contractor personnel. The PSS must prepare and send a letter to DSS formatted as shown in Appendix B, when requesting a check of this index. DSS will then check the DCII and provide the PSS with the results and a copy of any report of investigation on file.

(2) The Defense Industrial Security Clearance Office (DISCO), an office of DSS, grants security clearances to DOD contractor employees. The PSS can conduct name checks with DISCO and get investigation and security clearance information by calling DISCO in Columbus, Ohio, at 888-282-7682. FAA's facility code is *FAA*. The PSS can obtain copies of investigations conducted for DISCO clearances through DCII.

c. Federal Bureau of Investigation (FBI). The PSS must prepare DOT Form 1600.14, FBI Record Check Request to request a check of the FBI's investigations index, and a copy of any report of investigation the FBI might have. Mark the block at the top of the form titled, *FBI Name Check*, and mail the completed form to: U.S. Department of Justice, Federal Bureau of Investigation, Records Branch, Washington, DC 20535.

d. Other Federal agencies. Some Federal agencies have authority, either by law or through agreement with OPM, to conduct their own investigations pursuant to E.O. 10450. These agencies include the Department of State, Central Intelligence Agency, Peace Corps, U.S. Secret Service, Internal Revenue Service, U.S. Customs Service, and U.S. Postal Service. The PSS can contact the agency security office for a check of its files and to obtain a copy of any report that the agency might have if an applicant or employee has been employed by one of these agencies, or if there is an indication that one of them conducted an investigation on the person. If the agency will not release a copy of an investigation but permits review at an office in the Washington, DC, area, AIN-400 will assist regional PSSs by reviewing the report, documenting the results, and providing the PSS with the information. The PSS can request a copy of an

OPM investigation if there is any indication that they have a copy of it. OPM will furnish a copy of another agency's investigation if it is on file and if it meets their criteria for release.

Section 4. Investigative Forms

1. Forms Required for Investigations. This paragraph specifies the forms that you, the personnel security specialists (PSS) must submit to OPM for initiation of personnel security investigations and contains additional instructions for their completion and submission.

a. Required forms. You should consider the risk or sensitivity level of the position that an employee occupies, or for which he or she is under consideration, when determining which OPM forms are required for an investigation. The specific type of investigation being requested does not affect which forms are needed. The required forms are as follows:

(1) Low risk positions:

- (a) SF-85, Questionnaire for Non-Sensitive Positions, if the person is a Federal employee or applicant.
- (b) SF-86A, Continuation Sheet for Questionnaires SF-86, SF-85P, and SF-85, if there is insufficient space on the SF-85 for all of the employments, residences, or periods of education which the person is required to list.
- (c) SF-87, Fingerprint Chart, if the person is a Federal employee or applicant.
- (d) FD-258, FBI Fingerprint Chart, if the person is a child care services provider, or under special circumstances; i.e., interns, volunteers, etc.
- (e) Employment application, if the person is a Federal employee or applicant and the investigation is in conjunction with an appointment action.
- (f) Optional Form (OF) 306, Declaration for Federal Employment.

(2) Moderate-risk and high-risk positions:

- (a) SF-85P, Questionnaire for Public Trust Positions.
- (b) SF-86A if there is insufficient space on the SF-85P for all of the employments, residences, or periods of education which the person is required to list.

- (c) SF-85P-S, Supplemental Questionnaire for Selected Positions, if OPM granted the FAA approval to use the form for the position in question.
 - (d) SF-87 if the person is a Federal employee or applicant.
 - (e) FD-258 if the person is a child care services provider, or under special circumstances; i.e., interns, volunteers, etc.
 - (f) Employment application, if the person is a Federal employee or applicant and the investigation is in conjunction with an appointment action.
 - (g) OF-306.
 - (h) DOT F 1631, if the person has fiduciary responsibilities, and for persons in high-risk positions.
- (3) Non-critical-sensitive, critical-sensitive, and special-sensitive positions:
- (a) SF-86, Questionnaire for National Security Positions.
 - (b) SF-86A if there is insufficient space on the SF-86 for all of the employments, residences, or periods of education which the person is required to list.
 - (c) SF-87 if the person is a Federal employee or applicant.
 - (d) Employment application, if the investigation is in conjunction with an appointment action.
 - (e) OF-306.
 - (f) DOT F 1631 for all sensitive position.

2. Completion of Forms. When completing security forms either electronically or manually, the employee or applicant must:

- a.** type or clearly print their responses;
- b.** follow all instructions that accompany the form. The PSS should accept only complete forms, with all required information shown. Forms are not acceptable unless signed and dated;
- c.** list employment, education, and residence history and account for all periods of time to the extent required. For example, if a form requires an employment history for

the past 7 years, then the answer to that question must account for all periods of time within the past 7 years; and

d. completely answer all questions on the form, even if the information was previously provided on a form that was used to conduct an earlier investigation, such as, employment history. Only the PSS can make exceptions to this requirement, and then only with OPM's consent.

e. If you are the PSS, you must apply the following requirements to the amendment of forms already provided to the Personnel office and your SSE:

(1) You must return all investigative forms that are not properly completed to the person being investigated, and follow this procedure whenever possible. If the person being investigated is at a different location, and circumstances do not allow sufficient time to return it to him or her, amend the form following telephonic discussion with the person to ensure that additional information placed on the form or a change to a previous answer is consistent with the person's intent and is made with his or her concurrence.

(2) You can amend certain items on investigative forms or have the person being investigated make the changes. Use OPM Form FIPC 391, Certification of Amended Investigative Form, which lists the items to which this requirement applies, for forms that are filled out manually. An amended investigative form is not acceptable unless the person being investigated has initialed and dated all changes to any specified items or unless you have certified the changes on the FIPC 391.

(3) You must initial, date, and provide the SOI or SON code on all changes that you make to items other than those specified on the FIPC 391.

(4) Under no circumstances will anyone other than the person being investigated alter or amend any information that he or she is required to furnish on an investigative form unless the change or addition is certified as stated above.

f. Manual or electronic fingerprints for the SF-87 and FD-258 will be taken only by an individual trained to do so. Both the person being printed and the individual taking the prints must sign the form. The individual taking the prints will verify the identity of the Subject and note in the appropriate block any missing fingers and any scars.

g. The PSS must not submit investigative forms to OPM unless they are signed and dated by the applicant or employee within the previous 120 days. If over 120 days, the person who completed the investigative form must re-sign, re-date, and make any other changes prior to sending it to OPM.

3. Originals and Copies. The PSS must submit to OPM an original or a copy of the security form. In addition to the security form, the employment application, the OF-306, and any additional forms must be submitted for all investigations on newly-hired Federal employees and applicants.

CHAPTER 6. PERSONNEL SECURITY RECORDS

1. Personnel Security Files (PSF).

a. As the personnel security specialist (PSS), you must establish PSFs for all employees in special-sensitive, critical-sensitive, non-critical-sensitive and high-risk positions, and when there are reports of investigation or other personnel security materials on an employee warranting retention. You should establish a PSF for applicants when investigations are initiated or reports of investigation are obtained. Do not keep a PSF on every employee. You can create alphabetical files in lieu of a separate PSF to keep documents, such as, FAA Form 1600-54, Notification of Personnel Security Action, FAA Form 1600-25; Security Termination Statement; etc., if this is the only information on the individual.

b. PSF contents. The PSS may keep the following type of information in the PSF, when available:

- (1) FAA Form 1600-54, Notification of Personnel Security Action.
- (2) SF-85, Questionnaire for Non-sensitive Positions.
- (3) SF-85P, Questionnaire for Public Trust Positions.
- (4) SF-85P-S, Supplemental Questionnaire for Selected Positions.
- (5) SF-86, Questionnaire for National Security Positions.
- (6) FAA Form 1600-25, Security Termination Statement.
- (7) DOT Form 1681, Identification Card/Credential Application.
- (8) Reports of investigation completed by the Office of Personnel Management (OPM) and other agencies. You can destroy National Agency Checks and Inquiries (NACI) reports containing minor or outdated unfavorable information that is insignificant for use in any future suitability or security adjudications, and NACI reports that contain no unfavorable information. Keep a summary of the minor unfavorable information or a note that the results contained no unfavorable information. Enter all such notations into the Investigation Tracking System. You can use these notations in future adjudications or in processing waiver requests when the NACI information is not immediately available from OPM.
- (9) Reports of investigation (ROI) completed by FAA.

- (10) A copy of OPM's INV 79A case transmittal form documenting final adjudicative action.
- (11) Copies of all pertinent correspondence, including that to or from OPM, another Government agency, the operating office, the Human Resource Management Divisions (Personnel), or the applicant or employee.
- (12) Appropriate forms or memoranda documenting temporary or interim security clearances.
- (13) A record of all disclosures or reviews of information contained in the PSF by persons outside the servicing security element (SSE).
- (14) Copies of pertinent adjudication documentation conducted by your office.
- (15) Copies of all interview records conducted by your office.

2. Non-selected Applicants. If an applicant was not selected because unfavorable information was received in the SSE, the PSS should keep the applicant's PSF for a period of 1 year from the date of non-selection. If the PSF contains an FAA ROI, the PSS should keep the PSF for 5 years. In any other situations where the information is favorable, i.e., the applicant turned down the position, the job announcement was canceled, etc., the PSF should be kept for 30 days, if one was created.

3. Transfer of PSFs. As the PSS, you must ensure that PSFs are transferred appropriately when an employee transfers from within FAA or to a DOT administration.

a. Forwarding to another SSE. You must send all PSFs for employees who are transferring within FAA from one jurisdiction to another to the gaining SSE.

b. Forwarding to another DOT administration. You must forward a PSF to the Office of Security, M-40, when an employee transfers to another DOT administration.

4. Separated Employees. When employees separate from FAA and do not transfer to another DOT administration, you must keep and destroy the employee's PSFs and other personnel security records as follows:

a. Keep significant personnel security or suitability information in accordance with the latest edition of FAA Order 1350.15, Records Organization, Transfer, and Destruction Standards.

b. Do not keep any insignificant personnel security or suitability information, or PSFs that do not contain an FAA ROI for more than 30 days following termination of an employment unless the employee:

- (1) is on military or other leave status;
- (2) is expected to be re-employed within 5 years; or
- (3) is known to be involved in administrative action or an appeal that can result in restoration to duty.

c. Keep FAA ROI's for 5 years following termination of employment and destroyed in accordance with the latest edition of FAA Order 1350.15.

d. Keep FAA Forms 1600-25 for 1 year following termination of employment regardless of when a file is destroyed,

e. Keep other personnel security correspondence and records in accordance with the latest edition of FAA Order 1350.15.

5. Protection of Personnel Security Records. Personnel security records contain sensitive, highly privileged, and, in some cases, classified information. The PSS can disseminate OPM reports of investigation to authorized agency officials on a strict need-to-know basis, decide on the extent of dissemination, or furnish summaries or extracts of investigative reports in lieu of disseminating the entire report. All FAA employees with a need to know must carefully protect these records in their handling, transmittal, storage, and release. As the PSS, you must:

a. Control investigative information gotten under a pledge of confidence with the restrictions that the investigating agency has placed on it. Such restrictions normally preclude divulging it to the Subject of the investigation.

b. Control medical reports included as part of an investigation to ensure that they are disseminated only to persons who need them for security or suitability adjudication. Release the records to operating office managers only through aviation medical officials, who will interpret the medical information to management officials who have a need to know.

c. Protect reports of investigation, files, or other records which contain classified information under the latest edition of Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.

d. Protect, transmit, store, and destroy all files, reports of investigation, personal history statements, investigative forms, and other personnel security records and documents containing information of a personal or privileged nature under the latest

editions of FAA Orders 1600.2, and 1280.1, Protecting Privacy of Information About Individuals. Employees should not have unrestricted access to records that pertain to them, but you can provide them access to their PSF under paragraph 6 of this chapter.

(1) As a minimum, these records will be considered "For Official Use Only." You do not have to mark individual documents and records "For Official Use Only" as long as you keep them in the PSF. If these records are transmitted outside the PSF, mark them individually "For Official Use Only."

(2) You must store all reports of investigation in a locked cabinet, safe, or other equally secure area. Do not place such reports in an Official Personnel Folder.

(3) AIN-400 will maintain all personnel security records on regional and center SSE managers and PSSs and assistants, and all FAA Executives. AIN-1 will maintain all personnel security records on the AIN-400 manager.

(4) SSEs must ensure need to know before releasing reports of investigation, or extracts or summaries of these reports, to anyone outside their jurisdiction. They must ensure that persons outside their office who review FAA ROIs sign FAA Form 1600-12, Investigative Record Review, acknowledging that they understand their obligation to protect the information. FAA employees do not need to sign an acknowledgement when reviewing investigative information pertaining to them.

6. Employee Review of PSFs. SSEs must provide employees or their authorized representative the opportunity to review the employee's PSF upon request. When complying with a request for a PSF review, the PSS must:

a. Examine the file before letting an employee or representative review it, or before sending it to a field facility for review.

b. Remove any reports of investigation completed by another agency, such as OPM, DSS, or the FBI. If such a report is removed, inform the employee or representative in writing that the original of the PSF contains a report completed by (name of 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. OPM has requested that employees contact them directly to ask for a copy.

c. Remove any other information, such as, identification of a confidential source or an ongoing investigation that is exempt from release under the Privacy Act.

d. Permit review only at your office if the employee works at Washington headquarters, a regional headquarters, or a center.

e. Send a certified true copy of the PSF to the employee's facility, if the employee works at any other location. They must keep the original in their office. Enclose the copy in an envelope addressed to the employee marked, "TO BE OPENED BY ADDRESSEE ONLY," and transmit the envelope according to the requirements of FAA Order 1280.1.

f. Permit the employee or representative to review the PSF or make copies of documents in it only under the direct observation of an SSE employee when the review takes place at your office. The person overseeing the review must give the employee or representative a reasonable amount of time to review the PSF and ensure that the employee or representative does not remove any documents or pages from it.

g. Evaluate any request for access under both the Freedom of Information Act (FOIA) and the Privacy Act regardless of which the requester cites, and determine which statute in specific circumstances provides greater access.

7. Privacy Act Requirements. As the PSS, you must follow all requirements of the latest edition of FAA Order 1280.1, when responding to requests under the Privacy Act for disclosure of information in PSFs and reports of investigation.

a. Do not release any report of investigation completed by another Federal agency in response to a Privacy Act request without getting consent from that agency.

b. Follow the procedures for responding to third party inquiries contained in the latest editions of FAA Orders 1200.23, Public Availability of Information and 1280.1.

- (1) Do not release any information to a third party unless the first party to whom a record pertains signs a statement granting them permission to release the specific information requested.
- (2) Log in and answer all third party requests under the provisions of the FOIA if the first party to whom a record pertains does not sign a statement releasing the records to a third party, and the requested records are specifically part of the Privacy Act system of records, identifying the person by name, Social Security number, routing symbol, or other specific identification.
- (3) Respond to requests under the provisions of the FOIA when the information for a third party request is found in general records not identified by the person's name, Social Security number, routing symbol, or other specific identification.
- (4) Respond to requests for information concerning deceased persons, under the provisions of the FOIA.

8. Agreements to Release Personnel Security Records. The SSE must comply with any collective bargaining agreement or agreement with an individual that requires the FAA to release personnel security records on employees. No employee can enter into any agreement requiring the FAA to release a report of investigation completed by another Federal agency.

CHAPTER 7. PERSONNEL SUITABILITY STANDARDS, CRITERIA AND ADJUDICATION

1. General. It is primarily the responsibility of Human Resource Management Divisions (Personnel) and/or operating offices to make final suitability determinations, however, servicing security elements (SSE) play an important role in the suitability process. SSEs are responsible for adjudicating all Office of Personnel Management (OPM) investigations, and when they discover a potential suitability issue, they provide the information to Personnel and the operating office so they can make a final suitability determination. In order to provide consistency in the suitability process, this chapter outlines procedures that are to be followed by the SSE when making preliminary suitability adjudications. It does not apply to Personnel and operating offices who use the procedures contained in the FAA Human Resource (HR) Handbook for Suitability Determinations/Adjudication.

2. Suitability.

a. Suitability means fitness or eligibility for employment. It refers to identifiable character traits and past 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 with appropriate efficiency and effectiveness. It is distinguishable from a person's ability to fulfill the qualifications requirements of a job, as measured by experience, education, knowledge, skills, and abilities. The focus of a suitability adjudication is on whether the employment or continued employment of a person can reasonably be expected to promote the efficiency of the Federal service. Potentially disqualifying suitability factors are listed in paragraph 2 of this chapter.

b. All employees from the SSE and Personnel offices who are designated as adjudicators must meet the requirements of chapter 3, paragraph 2, and be thoroughly familiar with current laws, regulations, and criteria pertaining to suitability adjudication.

c. Although the Personnel office has the responsibility for making suitability determinations, the following employees are not subject to removal based on unsuitable determinations: employees with one year of continuous FAA service in the current period of employment, and current FAA employees who have one year of continuous service with no break in service of more than one year. These employees are, however, subject to disciplinary and removal actions under the provisions of applicable agency policy when an investigation develops information warranting such an action. In consultation with the SSE and Personnel office, the operating office manager is responsible for these actions. As exceptions, the Personnel office must retain suitability adjudication authority concerning issues raised in an initial investigation for FAA employment regardless of when the investigation is completed; and in all cases involving evidence of deception or fraud in examination or appointment, including intentional false statement on any application, questionnaire, or related document.

3. Personnel Suitability Standard and Criteria.

a. Suitability Standard. A suitability adjudication is an assessment of past and present conduct which can indicate future actions with adverse impact on the efficiency of the service. If you are the personnel security specialist (PSS), you will serve as a security adjudicator in the SSE and consider whether the conduct of the person indicates a potential for behavior that would interfere with, prevent, or otherwise adversely affect: (1) the performance of the person in the position applied for or employed in; (2) the performance of the duties and responsibilities of others in the FAA; or (3) the ability of the FAA to carry out its mandated responsibilities fully and effectively. You must consider two issues when determining potential impact on the efficiency of the service. They are: whether the conduct in question indicates a potential for inadequate or reduced performance of specific duties; and whether the conduct indicates any immediate or long-term risk for abuse of the public trust in carrying out the responsibilities of the position.

b. Criteria for Determining Suitability. The PSS must consider any of the following reasons below when making a preliminary suitability adjudication. If they believe that further action is required, they should refer the investigation to their Personnel office for final action. These criteria are as follows:

- (1) Misconduct or negligence in prior employment that would have a bearing on efficient service in the position in question, or would interfere with or prevent the FAA from effectively accomplishing its duties and responsibilities.
- (2) Criminal or dishonest conduct related to the duties to be assigned to the person, to that person's service in the position, or to the service of other employees.
- (3) Intentional false statement or deception or fraud in examination or appointment.
- (4) Refusal to furnish testimony required by civil service rules.
- (5) Alcohol abuse of a nature and duration that suggests the person would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others.
- (6) Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation.
- (7) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force.
- (8) Any statutory or regulatory bar which prevents the person's lawful employment in the position in question.

c. Additional Considerations. The PSS must consider the following factors to the extent that they deem pertinent to the individual case, when making a preliminary suitability adjudication:

- (1) The kind of position for which the person is applying or in which the person is employed, including the degree of public trust or risk in the position.
- (2) The nature and seriousness of the conduct.
- (3) The circumstances surrounding the conduct.
- (4) The recency of the conduct.
- (5) The person's age at the time of the conduct.
- (6) Contributing societal conditions.
- (7) The absence or presence of rehabilitation or efforts toward rehabilitation.

4. Coordinating Personnel Security Information. Personnel managers and all FAA supervisors must furnish to their SSE any information they receive concerning employees or applicants under their jurisdiction that may affect their suitability for employment or their holding of a security clearance because of the standards and criteria stated in paragraph 3 of this chapter, the FAA Human Resources (HR) Handbook for Suitability Determinations/Adjudication, and chapter 8, paragraph 1 of this order.

5. Suitability Adjudication.

a. The Personnel office should consult with the PSS, regarding the type of investigation necessary to resolve an issue(s), if they cannot make a determination whether the person is suitable or unsuitable. The PSS, must then initiate an investigation following the procedures in chapter 5, section 3, paragraph 1 of this order, or conduct a limited inquiry, such as, obtaining court, credit or other record information, or decline to investigate pending completion of the required investigation by OPM.

b. The Personnel office may not be able to identify suitability issues that are not evident until the required background investigation is completed by OPM or obtained by FAA, either while a person is still an applicant or after being hired. The SSE will receive investigative reports pertaining to their region from OPM, and, in some cases, reports of investigation completed by other agencies, and the PSS will conduct a preliminary suitability adjudication on this information.

c. The SSE may also receive information that could warrant an unfavorable suitability determination while investigating issues involving employee conduct. In this

instance, the PSS must provide the employee an opportunity to respond to this unfavorable information as stipulated in chapter 2, paragraph 2a of this order.

d. The SSE must forward a memo with all reports and pertinent information to the Personnel office for a final suitability determination when they have information pertaining to a potential unfavorable suitability determination.

e. The SSE must also send a copy of the report and pertinent information to the operating office when the Subject of an investigation is an FAA employee.

f. The SSE must forward to the Office of Aviation Medicine (AAM) or its regional or center Aviation Medical Division any reports of investigation or other information raising a question about a person's physical or mental fitness to perform a particular job, and notify the Personnel office when sent.

g. In the case of an FAA employee, the Personnel office, in consultation with the PSS and the operating office will make all suitability determinations, and coordinate with AAM or an Aviation Medical Division in regard to any medical issues. They are encouraged to consult with the Office of the Chief Counsel (headquarters cases) or Regional Counsel (regional and center cases) prior to making an unfavorable suitability determination.

6. Suitability Adjudication Process.

a. Suitability adjudication is a three-level process consisting of basic suitability adjudication, position sensitivity adjudication, and position performance adjudication. As the PSS, you should follow the guidelines below when making a preliminary suitability adjudication before referring cases to personnel or operating offices.

(1) The first level is basic suitability adjudication. This is an assessment of conduct as it affects a person's suitability for any position at FAA. Apply the suitability standard and criteria in paragraph 3 and adjudicate issues in and of themselves, without particular reference to their impact on employment eligibility for a specific position. You must carefully evaluate the conduct of the person as it may adversely affect his or her performance, or the ability of the agency to perform its mission, using screening standards that are designed to promote uniform and equitable decisions. When applying nexus, you must reasonably expect that the person's employment would not promote the efficiency of the service.

(2) The second level is position risk adjudication which you must apply to persons rated suitable at the basic suitability adjudication level that are being considered for employment, or retention in employment, in specific positions. Assess a person's conduct as it affects his or her suitability for employment in terms of the risk or sensitivity level of a specific position. View an issue more seriously when the

position is at a higher risk or sensitivity level in order to reflect the greater potential for adverse impact of the person's employment on the efficiency of the service.

(3) The third level is position performance adjudication that you must apply to persons who have been rated suitable at the first two levels. Assess conduct in terms of its nexus impact, or indicated potential impact, on the person's performance in a specific position, including any indicated risk for abuse of the public trust in carrying out specific duties.

b. The PSS may use the procedures contained in the PSS Supplement and this chapter as a guide when adjudicating suitability at each of the above levels, but they do not have to follow them precisely.

7. Documentation and Notification.

a. As the PSS, you must clearly document all suitability adjudications, particularly where there are serious issues. Include in the documentation a clearly written rationale with your recommendation that the person's employment or continued employment at FAA, in a position at a particular risk or sensitivity level, or in a specific position would or would not promote the efficiency of the service. You must provide all documentation to your Personnel and operating office for their use in making the final suitability determination. Maintain this record for at least 2 years from the date of the adjudication.

b. FAA must report to OPM any final adjudicative action based on an OPM report of investigation or a file OPM furnishes in response to a check of its Security Investigations Index (SII).

(1) When instructed to do so, the PSS must complete and return to OPM all OPM Forms INV 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations, which accompanies completed OPM reports of investigation.

(2) OPM uses Form OFI 79B, Request for Search of OPM Records, as well as certain other forms, some of which are printed electronically, to provide the results of an SII search and to request a report of final action taken. The PSS must complete and return the appropriate form to OPM whenever instructed to do so.

(3) If the SSE makes an adverse *security determination* that precludes any personnel suitability adjudication, the PSS must complete the OPM Form INV 79A and return it to OPM.

(4) In cases where the Personnel office renders an unfavorable suitability adjudication or the SSE renders an unfavorable security adjudication which may warrant OPM action to debar the person from Federal employment, the PSS must complete OPM Form INV 79A and include a Request for an Advisory Opinion. The PSS must coordinate this with AIN-400 prior to submitting to OPM.

CHAPTER 8. PERSONNEL SECURITY STANDARDS, CRITERIA, AND ADJUDICATION

1. Personnel Security Standard and Criteria.

a. Security Standard. The servicing security element (SSE) is responsible for granting persons access to classified national security information. They must ensure that the granting of such access to any person is clearly consistent with the national security interests of the United States. They must resolve any doubt in favor of the national security, assess past and present conduct and consider whether or not the granting of such access conforms to this standard, and deny access to classified information if the conduct listed below indicates that the person would pose a risk for damage to the national security. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel, generally the personnel security specialist (PSS).

b. Criteria. Executive Order (E.O.) 12968 states that eligibility for access to classified information will be granted only to persons whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment; freedom from conflicting allegiances and potential for coercion; and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. E.O. 10450 enumerates the following criteria that as the PSS, you must consider in making security determinations:

- (1) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.
- (2) Any deliberate misrepresentation, falsification, or omission of material facts.
- (3) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.
- (4) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.
- (5) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause the person to act contrary to the best interests of the national security.

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

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

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

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

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

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

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

c. Restrictions. E.O. 12968 specifies the following restrictions when the PSS is applying the security standard and criteria. As the FAA,

(1) we must not discriminate against any person on the basis of race, color, religion, sex, national origin, disability, or sexual orientation, when we grant access to classified information;

(2) we can investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security, when determining eligibility for access. However, we cannot make a judgment using the security standard and criteria based solely on the basis of a person's sexual orientation; and

(3) we must not make a judgment using the security standard and criteria based solely on the basis of a person's mental health counseling. We should consider some counseling as a positive factor in making eligibility determinations. We must, however, consider mental health when it directly relates to the security standard and criteria and when relevant to the adjudication of access to classified information. In this instance, we can justify further inquiry to determine whether the standard and criteria are satisfied.

2. Security Adjudication. The PSS is responsible for adjudicating all pertinent information and making determinations on access to classified national security information. If you are the PSS, refer to chapter 9, Access Authorizations, which contains more specific criteria and procedures for granting access to classified information. You should follow the guidelines contained in paragraphs 6 through 19 of this chapter when determining eligibility for access to classified information.

3. Responsibility for Security Adjudications.

a. The SSE is responsible for security adjudication of all employees and applicants for positions under their jurisdiction, except for the positions of their regional administrator, center director and deputy director. The Personnel Security Division, AIN-400, will make the security adjudication for persons in these positions. They will also adjudicate cases on SSE personnel who are directly responsible for administering the Personnel Security Program, such as, the appropriate division and branch managers, personnel security managers, and PSSs and assistants.

b. The PSS must forward all cases to AIN-400 when they conclude that a person has been coerced, influenced, or pressured to act contrary to the interests of the national security, or significant questions are raised regarding a person's loyalty to the United States. AIN-400 will forward the case to the Office of the Secretary, Office of Security, M-40, who will refer it to the FBI. The PSS must forward any cases that require an advisory opinion to AIN-400.

4. Case Adjudication Procedures.

a. During initial review of any report of investigation or any information received that raises an issue, you, as the PSS must:

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

(2) Determine if there are any significant discrepancies between activities claimed on an investigative form, OF-306, or employment application, and those shown in the report or other information received.

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

(4) Determine if any information requires referral to AIN-400.

b. The PSS can obtain additional information as needed to adjudicate a case either by requesting that OPM conduct an additional investigation if an OPM report appears to be inconclusive or incomplete, or conduct a Reimbursable Suitability Investigation to resolve an issue raised in a National Agency Checks with Inquiries, National Agency Checks with Inquiries and Credit, or Minimum Background Investigation. They can also initiate an FAA investigation to resolve issues when warranted as stated in chapter 5, section 3, paragraph 2, of this order, or question an applicant or employee about discrepancies relating to applications or investigative forms either by personal interview or interrogatory. They should not allow the person to amend such forms to eliminate the discrepancies.

c. As the PSS, you must assess all issues in question (except loyalty cases) in terms of the sensitivity of the duties and responsibilities of the position and whether any conduct in question indicates that employment of the person in a sensitive position and granting of access to classified information would pose a risk in terms of protecting the national security. Any conduct indicating that the person, through individual or collective action or inaction, can impair the security interests of the United States demonstrates a national security risk. During this assessment, use the standards and criteria stated in paragraph 1 of this chapter, and use the guidance in paragraph 6 of this chapter when making all determinations of eligibility for access to classified information.

d. As the PSS, you must give particular attention to any indication of unreliability, untrustworthiness, lack of dependability, potential for subornation or blackmail, dishonesty, or disregard for the law or established authority. Deny the applicant or employee a security clearance, or take action to revoke an existing clearance if you believe that the granting of a security clearance is not clearly consistent with the interests of the national security. You should suspend the person's access to classified information pending completion of the revocation process. (Refer to chapters 9 and 10 of this order.)

5. Timeliness of Adjudications. As the PSS, you must adjudicate cases promptly in the interests of national security, the FAA, and the person involved. Return OPM Form INV 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations, which accompanies the completed OPM reports, within 90 days from the date of receipt of the material or upon final adjudicative action, when instructed to do so. OPM requires use of this form to report the action taken.

6. Security Adjudication Guidelines.

a. General. The following adjudication guidelines, that are in effect throughout DOT, were developed by the Security Policy Board as required by E.O. 12968. The PSS must use them when determining whether the granting or continuation of eligibility for access to classified information is consistent with the interests of national security.

b. The adjudicative process. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is not a security risk.

(1) As the PSS, you must base the eligibility for access to classified information upon the person meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. You must consider available, reliable information about the person, past and present, favorable and unfavorable, in reaching a determination. Also, consider the following factor in evaluating the relevance of a person's conduct:

- (a) the nature, extent, and seriousness of the conduct;
- (b) the circumstances surrounding the conduct, to include knowledgeable participation;
- (c) the frequency and recency of the conduct;
- (d) the individual's age and maturity at the time of the conduct;
- (e) the voluntariness of participation;
- (f) the presence or absence of rehabilitation and other pertinent behavioral changes;
- (g) the motivation for the conduct;
- (h) the potential for pressure, coercion, exploitation, or duress; and
- (i) the likelihood of continuation or recurrence.

(2) As the PSS, you must judge each case on its own merits. Resolve any doubt in favor of the national security for employees being considered for access to classified information, and consider this resolution final.

(3) As the PSS, you must use common sense when determining whether the granting or continuation of eligibility for a security clearance is clearly consistent with the interests of national security, and base your determination upon careful consideration of the following, each of which is to be evaluated in the context of the whole person.

- (a) GUIDELINE A: Allegiance to the United States
- (b) GUIDELINE B: Foreign influence
- (c) GUIDELINE C: Foreign preference
- (d) GUIDELINE D: Sexual behavior
- (e) GUIDELINE E: Personal conduct
- (f) GUIDELINE F: Financial considerations
- (g) GUIDELINE G: Alcohol consumption
- (h) GUIDELINE H: Drug involvement
- (i) GUIDELINE I: Emotional, mental, and personality disorders
- (j) GUIDELINE J: Criminal conduct
- (k) GUIDELINE K: Security violations
- (l) GUIDELINE L: Outside activities
- (m) GUIDELINE M: Misuse of Information Technology Systems

(4) As the PSS, you can disqualify a person if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior even though adverse information concerning a single criterion may not be sufficient for an unfavorable determination. Notwithstanding the whole person concept, you can terminate the pursuit of further investigation in the face of reliable, significant, and disqualifying adverse information.

(5) When the PSS discovers information of a security concern about a person who is currently eligible for access to classified information, they must consider whether the person:

- (a) voluntarily reported the information;

- (b) was truthful and complete in responding to questions;
- (c) sought assistance and followed professional guidance, where appropriate;
- (d) resolved or appears likely to resolve the security concern favorably;
- (e) has demonstrated positive changes in behavior and employment;
- (f) should have his or her access temporarily suspended pending final adjudication of the information.

(6) As the PSS, you can recommend approval with a warning that future incidents of a similar nature can result in revocation of access if after evaluating information of a security concern you decide that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance.

7. Guideline A: Allegiance to the United States.

a. The concern. A person must be of unquestioned allegiance to the United States. The PSS must question a person's allegiance to the United States, if the willingness to safeguard classified information is in doubt.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act the aim of which is to overthrow the Government of the United States or alter the form of government by unconstitutional means;
- (2) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
- (3) association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means; and
- (4) involvement in activities that unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

c. Possible mitigating conditions: Conditions that can mitigate security concerns include:

- (1) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
- (2) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;
- (3) the individual's involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest; and
- (4) the person has had no recent involvement or association with such activities.

8. Guideline B: Foreign Influence.

a. The concern. A security risk can exist when a person's immediate family, including cohabitants and other persons to whom he or she is bound by affection, influence, or obligation are not citizens of the United States or can be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) an immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;
- (2) sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;
- (3) relatives, cohabitants, or associates who are connected with any foreign government;
- (4) failing to report, when required, associations with foreign nationals;
- (5) unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;
- (6) conduct that can make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;
- (7) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion, or pressure; and

(8) a substantial financial interest in a country, or in any foreign-owned or operated business that could make the individual vulnerable to foreign influence.

c. Possible mitigating conditions: Conditions that can mitigate security concerns include:

- (1) a determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;
- (2) contacts with foreign citizens are the result of official United States Government business;
- (3) contact and correspondence with foreign citizens are casual and infrequent;
- (4) the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country; and
- (5) foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

9. Guideline C: Foreign Preference.

a. The concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

b. Possible disqualifying conditions: Conditions that raise a security concern and can be disqualifying include:

- (1) the exercise of dual citizenship;
- (2) possession and/or use of a foreign passport;
- (3) military service or a willingness to bear arms for a foreign country;
- (4) accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
- (5) residence in a foreign country to meet citizenship requirements;

- (6) using foreign citizenship to protect financial or business interests in another country;
- (7) seeking or holding political office in the foreign country;
- (8) voting in foreign elections; and
- (9) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

c. Possible mitigating conditions: Conditions that can mitigate security concerns include:

- (1) dual citizenship is based solely on parents' citizenship or birth in a foreign country;
- (2) indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
- (3) activity is sanctioned by the United States; and
- (4) the individual has expressed a willingness to renounce dual citizenship.

10. Guideline D: Sexual Behavior.

a. The concern. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, can subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion.¹ Sexual orientation or preference cannot be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
- (2) compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

¹ The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

(3) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

(4) sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

(1) the behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

(2) the behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

(3) there is no other evidence of questionable judgment, irresponsibility, or emotional instability; and

(4) the behavior no longer serves as a basis for coercion, exploitation, or duress.

11. Guideline E: Personal Conduct.

a. The concern. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person cannot properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

(2) refusal to complete required security forms or releases, or provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying also include:

(1) reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

(2) the deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment

qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(3) deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

(4) personal conduct or concealment of information that can increase an individual's vulnerability to coercion, exploitation, or duress, such as, engaging in activities which, if known, can affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

(5) a pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency; and

(6) association with persons involved in criminal activity.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

(1) the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

(2) the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

(3) the individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

(4) omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

(5) the individual has taken positive steps to reduce significantly or eliminate vulnerability to coercion, exploitation, or duress;

(6) a refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements, and, upon being made aware of the requirement, fully and truthfully provided the requested information; and

(7) association with persons involved in criminal activities has ceased.

12. Guideline F: Financial Considerations.

a. The concern. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) a history of not meeting financial obligations;
- (2) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;
- (3) inability or unwillingness to satisfy debts;
- (4) unexplained affluence; and
- (5) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

- (1) the behavior was not recent;
- (2) it was an isolated incident;
- (3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce, or separation);
- (4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
- (5) the affluence resulted from a legal source; and
- (6) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

13. Guideline G: Alcohol Consumption.

a. The concern. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, and failure to control impulses; and increases the risk of unauthorized disclosure of classified information due to carelessness.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;
- (2) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;
- (3) diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;
- (4) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;
- (5) habitual or binge consumption of alcohol to the point of impaired judgment; and
- (6) consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

- (1) the alcohol-related incidents do not indicate a pattern;
- (2) the problem occurred a number of years ago and there is no indication of a recent problem;
- (3) positive changes in behavior supportive of sobriety; and
- (4) following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at

least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

14. Guideline H: Drug Involvement.

a. The concern.

(1) Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence can impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

(2) Drugs are defined as mood and behavior altering substances, and include:

(a) drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(b) inhalants and other similar substances.

(3) Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

(1) any drug abuse (see above definition);

(2) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

(3) diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(4) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program; and

(5) failure to complete successfully a drug treatment program prescribed by a credentialed medical professional. Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

- (1) the drug involvement was not recent;
- (2) the drug involvement was an isolated or infrequent event;
- (3) a demonstrated intent not to abuse any drugs in the future; and
- (4) satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.

15. Guideline I: Emotional, Mental, and Personality Disorders.

a. The concern. Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social, and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. When appropriate, a credentialed mental health professional (e.g., clinical psychologist or psychiatrist), acceptable to or approved by the Government, should be consulted so that potentially disqualifying and mitigating information can be fully and properly evaluated.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) an opinion by a credentialed mental health professional that the individual has a condition or treatment that can indicate a defect in judgment, reliability, or stability;
- (2) information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;
- (3) a pattern of high-risk, irresponsible, aggressive, anti-social, or emotionally unstable behavior; and
- (4) information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

- (1) there is no indication of a current problem;
- (2) recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation;

(3) the past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

16. Guideline J: Criminal Conduct.

a. The concern. A history or pattern of criminal activity creates doubt about a person's judgment, reliability, and trustworthiness.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

(1) any criminal conduct, regardless of whether the person was formally charged; and

(2) a single serious crime or multiple lesser offenses.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

(1) the criminal behavior was not recent;

(2) the crime was an isolated incident;

(3) the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

(4) the person did not voluntarily commit the act or the factors leading to the violation are not likely to recur; and

(5) there is clear evidence of successful rehabilitation.

17. Guideline K: Security Violations.

a. The concern. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

(1) unauthorized disclosure of classified information; and

(2) violations that are deliberate or multiple or due to negligence.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include actions that:

- (1) were inadvertent;
- (2) were isolated or infrequent;
- (3) were due to improper or inadequate training; and/or
- (4) demonstrate a positive attitude toward the discharge of security responsibilities.

18. Guideline L: Outside Activities.

a. The concern. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

b. Possible disqualifying conditions. Conditions that can raise a security concern and can be disqualifying include any service, whether compensated, volunteer, or employment with:

- (1) a foreign country;
- (2) any foreign national;
- (3) a representative of any foreign interest; and/or
- (4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

- (1) evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities; and
- (2) the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

19. Guideline M: Misuse of Information Technology Systems.

a. The concern. Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems can raise security concerns about an

individual's trustworthiness, willingness, and ability to protect properly classified systems, networks, and information. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

b. Possible disqualifying conditions. Conditions that raise a security concern and can be disqualifying include:

- (1) illegal or unauthorized entry into any information technology system;
- (2) illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;
- (3) removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations; and
- (4) introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.

c. Possible mitigating conditions. Conditions that can mitigate security concerns include:

- (1) the misuse was not recent or significant;
- (2) the conduct was unintentional or inadvertent;
- (3) the introduction or removal of media was authorized;
- (4) the misuse was an isolated event; and
- (5) the misuse was followed by a prompt, good faith effort to correct the situation.

20. Records to be Maintained.

a. PSSs must maintain a record of all security adjudications, to include the following:

- (1) A copy of the case transmittal form and OPM Form INV 79A (for each OPM investigation).
- (2) A copy of OFI Form 79B, Request for Search of OPM Records (for a file obtained from OPM through a check of the SII).

b. When a PSS proposes an adverse security action, they must maintain, at a minimum, an administrative due process file consisting of the documents mentioned in paragraph 20a of this chapter, and the following:

- (1) Copies of all communications sent to the person.
- (2) Copies of all written challenges, replies, or documentation supplied by the person, to include a written summary of any oral response.
- (3) A copy of any report of investigation from OPM, another agency, or the FAA.
- (4) Copies of any other documents related to the case.

c. For information on keeping records on non-selected applicants, refer to chapter 6, paragraph 2 of this order.

CHAPTER 9. ACCESS AUTHORIZATIONS

1. General. Access authorizations are certifications by the servicing security element (SSE) that persons are found to be sufficiently trustworthy to be allowed access to classified national security information at specified levels on a need-to-know basis, in accordance with the provisions of Executive Orders (E.O.) 12958 and 12968. These authorizations are generally called security clearances and can be granted to an employee at the Confidential, Secret, and Top Secret levels.

a. Except as provided by paragraph 2 of this chapter, access can be granted to a person who is a United States citizen, has had the appropriate investigation, and whose personal and professional history affirmatively indicate loyalty to the United States; strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment; and freedom from conflicting allegiances and potential for coercion. The person must also possess the willingness and ability to abide by regulations governing the use, handling, and protection of classified information. The personnel security specialist (PSS) is responsible for adjudicating a person's eligibility for access to classified information and recommending to their SSE manager that a clearance be granted. The PSS must apply the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, approved by the President in March 1997, for use throughout the Executive Branch (chapter 8, paragraph 6 of this order), when granting access to classified information.

b. As the PSS, you must determine that the person is eligible for access to classified information, based upon a favorably adjudicated investigation and a demonstrated need to know. Ensure that the person signs an approved nondisclosure agreement and has a briefing on the requirements for handling, protecting, and disclosing classified information. On behalf of the SSE, you can grant an interim or temporary clearance in very exceptional circumstances when official functions must be performed prior to completion of the investigative and adjudicative processes. You can request that a person undergo a reinvestigation at any time during the period the person is required to have access to classified information to ascertain whether they continue to meet the requirements for access to classified information.

c. The PSS must terminate access authorizations when no longer required.

d. As the PSS, you must ensure that especially tight controls are imposed in processing Top Secret access authorizations and requests for access to Sensitive Compartmented Information (SCI). The Department of Transportation does not have authority to grant access to SCI, but the Director of Central Intelligence can grant such access to a person when necessary for the performance of his or her duties.

2. Limitations and Restrictions on Access to Classified Information.

a. As the PSS, you must base the level of access approved for a person directly to the level of classified information that he or she needs to access. The person is, however, eligible for access to classified information at a lower level if already approved for access at a higher level. In other words, if a person has access to Top Secret information, he or she can also access information at the Confidential and Secret levels.

b. No person is eligible for access to classified information merely because of Federal service, contracting, license, certificate holder, or grantee status, as a matter of right or privilege, or as a result of their title, rank, position, or affiliation. The PSS must ensure that the request for access is justified by the operating office.

c. The FAA should keep the number of persons cleared for access to classified information to a minimum, consistent with the requirements of operations per E.O. 12968. The PSS should not grant a security clearance to a person solely to permit entry to, or ease of movement within, controlled areas when he or she has no need for access to classified information and such access can reasonably be prevented. They should not issue security clearances to:

- (1) persons in public trust positions;
- (2) persons whose regular duties do not require frequent access to classified information;
- (3) persons within a restricted, controlled, or industrial area, who do not require access to classified information;
- (4) persons who may only have inadvertent access to sensitive information or areas, such as, emergency service personnel, firemen, doctors, nurses, police, mailroom employees, or similar personnel;
- (5) persons who can be prevented from accessing classified information by being escorted by cleared personnel;
- (6) maintenance or cleaning personnel, including persons who perform maintenance on office equipment, such as, computers and photocopiers, who only have inadvertent access unless such access cannot be reasonably prevented;
or
- (7) SSE personnel who have no access to classified information.

3. Request Procedures.

a. Supervisors and managers must request security clearances for employees only when there is a demonstrated, foreseeable need for access. These requests must be in writing to their SSE. The SSE will ensure that the PSS evaluates all clearance requests to determine need in accordance with policies stated in the latest edition of FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information. The Director, Office of Internal Security and Investigations, AIN-1, will make the final determination when there is any dispute regarding the need for a clearance that cannot be resolved between the SSE and operating offices.

b. A supervisor or manager can request a temporary clearance for a specified amount of time if an employee does not need access to classified information for a period of time exceeding 6 months. The request must be in writing and sent to their SSE.

c. A supervisor or manager can request an interim clearance prior to the completion of the required investigation. They must specify the reason that the clearance should be granted before the expected completion date of the required investigation and the consequences of not waiting for the investigation to be completed. The request must be in writing and sent to their SSE.

d. A supervisor or manager can submit a request for clearances covering an entire group of employees, such as, all employees working in his or her organization who occupy a particular position or positions, or all employees working at a particular facility or in a specified office. This can be done in lieu of submitting a separate request for each employee needing a clearance. The request must be in writing and sent to their SSE. After review, the SSE can grant clearances to all employees in the specified group(s), if applicable. The PSS must review sensitivity designations as clearances are requested in order to ensure that positions have the appropriate sensitivity levels required and that these levels are adjusted as necessary.

4. Interim Clearances.

a. Confidential and Secret.

(1) As the PSS, you can grant temporary eligibility for access under exceptional circumstances such as, when an employee must perform official functions requiring access to Confidential or Secret classified information prior to completion of the required investigation. This type of access is called an interim clearance and can be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of this access. You must not use this process in lieu of a waiver or as a means to place a person in a sensitive position without the required background investigation.

(2) As the PSS, you can also grant interim clearances for access to Confidential and Secret information to employees, upon determining that they are needed and justified. Use any one of the following as the basis for granting an interim Confidential or Secret clearance prior to the completion of the required investigation:

(a) Receipt of the advance report of a favorable National Agency Check (NAC) in a current investigation or confirmation of a favorable NAC completed within the preceding 1 year.

(b) Confirmation of a completed Department of Defense (DOD) NAC on a former member of the armed forces provided that:

1 The person has not had more than a 2-year break in service between the date he or she was released from the military and the beginning date of the person's FAA employment;

2 The DOD NAC has been completed during the person's most recent enlistment and within the past 6 years; and,

3 You must review the person's DD Form 214, Armed Forces Report of Transfer or Discharge, to determine the condition under which the person was discharged from the military service.

(3) As the PSS, you must not grant an interim clearance until you have reviewed the SF-86 used to initiate the required investigation and conducted a Subject interview.

(4) As the PSS, you can grant an interim clearance for a period of not more than 6 months. If the required investigation has not yet been completed at the end of that time, you can extend the period of time that the clearance remains in effect, after checking on the status of the investigation and the information developed to date. A final clearance supersedes an interim clearance.

(5) As the PSS, you must ensure that the employee completes and signs an SF-312, Classified Information Nondisclosure Agreement, and receives the appropriate briefing, after they are granted the interim clearance. Notify the employee in writing, as E.O. 12968 requires, that further access is expressly conditioned on the favorable completion of the investigation and adjudication of its results. Immediately terminate an interim clearance if the investigative results do not warrant the granting of a final clearance.

b. Top Secret.

(a) Only the Office of Security, M-40, OST, can grant interim Top Secret clearances when there is no prior investigation. As a matter of practice, M-40 rarely grants interim Top Secret clearances and does so only in exceptional cases. As the PSS, you must forward all request for interim Top Secret clearances to the Personnel Security Division, AIN-400, when you determine that it is justified. You should include in the request copies of the SF-86 used to initiate the investigation, all available investigative information, and any other pertinent information. AIN-400 will forward the request to M-40. When approved or disapproved, AIN-400 will send you the response.

(b) The PSS must not send requests for interim Top Secret clearances unless the current Single Scope Background Investigation has been closed as pending and been favorably adjudicated.

5. Temporary Clearances.

a. The PSS can grant temporary eligibility for access, referred to as a temporary clearance, when there is a need for an employee to have this access for a limited period of time, such as, for one-time participation in a classified project, and the employee does not have the appropriate investigation that meets the requirements for a clearance.

b. The PSS can grant temporary clearances for access to Confidential and Secret information, upon determining that they are needed and justified. Only M-40 can grant a temporary Top Secret clearance.

c. Before the PSS grants a temporary clearance for access to Confidential and Secret information, they must review a current, signed SF-86 from the employee and conduct a credit check. The employee must sign DOT Form 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (Appendix F) before a credit check can be conducted.

d. The PSS can grant a temporary clearance for access to Confidential and Secret clearances for a period of time not to exceed 60 days; but, if circumstances warrant, can extend it for an additional period of time not to exceed a total of 6 months. They should establish a fixed date or event for expiration of the clearance, and limit the access granted to information related to a particular project or assignment.

e. The PSS must ensure that when an employee is being granted a temporary clearance at any level for access to another agency's classified information, that agency concurs before access is granted. They should take appropriate steps to ensure that the other agency concurs with the release of its classified information to an employee with a temporary clearance.

f. The PSS must ensure that the employee completes and signs the SF-312 and receives the appropriate briefing after you grant a temporary clearance.

6. Final Clearances. The PSS can grant a final clearance when the required investigation has been completed and they have favorably adjudicated it and reviewed and evaluated all other pertinent official records. If OPM sends the SSE a substantially complete investigation but a minor portion is still pending, the PSS can grant a clearance if they feel that the completed portion clearly supports a favorable adjudication and the pending information is unlikely to raise a material issue or help to resolve one.

7. Clearance Granting Procedures and Documentation.

a. Basic procedures.

(1) As the PSS, you must record all determinations made regarding the granting of security clearances on FAA Form 1600-54, Notification of Personnel Security Action. Use this form to document clearances granted. The forms can be produced electronically by an FAA-approved database, or manually.

(2) The PSS must ensure that Form 1600-54 accurately shows the following information:

(a) Level and date of clearance.

(b) Investigative basis and date of investigation or update investigation.

(c) Position sensitivity.

(3) The personnel security manager/supervisor or designated representative will sign and date Form 1600-54.

(4) The PSS will then send the original and operating office copy (Copy 2) of Form 1600-54, along with an SF-312 to the employee's operating office. The operating office should retain Copy 3 of Form 1600-54.

(5) The employee's supervisor must give or arrange for the required security briefing and have the employee sign Form 1600-54 and the SF-312. The supervisor or person providing the briefing must sign as a witness to the employee's signature on Form 1600-54 and the SF-312. A representative from the SSE can sign as the acceptor of the SF-312. The employee must sign Form 1600-54, acknowledging that he or she has been granted a security clearance at a specified level. Form 1600-54 needs to be signed only once unless there is a change in the clearance level of a position, or the employee receives a refresher briefing. The employee only needs to sign the SF-312 once regardless of how

many times he or she is granted a clearance. If the person being granted a clearance has previously signed an SF-312, the PSS should inform the operating office.

(6) The operating office must return the completed original Form 1600-54 and the original SF-312, if applicable, to the PSS.

(7) The PSS must keep Form 1600-54 with original signatures in the Personnel Security File, and send the Human Resource Management Division Copy 3 of the form and the SF-312 for placement in the employee's Official Personnel Folder.

b. Security briefings.

(1) Security briefings are given to all employees authorized access to classified information to ensure that they fully understand the requirements and procedures for protecting it, the specific hazards that can be expected, what to do if a compromise occurs, and their continued obligations after their clearances are terminated. Either the SSE or the employee's supervisor or manager can give the security briefing to the employee. (Refer to Appendix G, Security Briefing Guidance for Access to Classified Information.)

(2) The PSS must ensure that an employee receives a security briefing each time he or she is granted a security clearance, unless a briefing was given within the past year. They should stress the importance of attending periodic refresher briefings to their operating offices.

8. Special Access Authorizations. Access to special categories of classified information or special access programs requires additional security adjudication and briefings.

a. Requirements for access to SCI are contained in Director of Central Intelligence Directive 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to SCI.

b. The Department of Energy (DOE) issues clearances for access to DOE Restricted Data under the provisions of the Atomic Energy Act of 1954, as amended. DOE Restricted Data relate to the design, manufacture, and use of atomic weapons, the production of special nuclear material, and energy production. Restricted Data is assigned classification levels of Confidential, Secret and Top Secret similar to the levels of other national security information classified under the provisions of E.O. 12958, Classified National Security Information. Order DOT 1630.2, DOT Personnel Security Program, chapter 9, contains specific instructions regarding DOE Restricted Data clearances.

c. AIN-400 will process all requests for special access authorizations.

9. Terminating Access Authorizations.

a. Administrative termination. The PSS must administratively terminate an employee's security clearance whenever his or her FAA employment is terminated for any reason or when duty changes occur that eliminate the need for the clearance. When the latter situation exists, the employee's supervisor must send the SSE a request to terminate or reduce the level of clearance. The PSS must reassess the sensitivity level of the employee's position or re-designate the position to public trust.

b. Clearance suspension.

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

(2) The PSS must consider clearance suspension as a temporary action that will be in effect only while the question of security fitness is being investigated, while other pertinent information is being obtained and evaluated, or while legal, administrative, or other action is pending that is expected to have a bearing on whether or not the employee can continue to hold a clearance. It may remain in effect while an employee is participating in a rehabilitation program following determination of substance abuse; or in a rehabilitation program, counseling, or therapy resulting from legal action occurring outside the FAA. The SSE can reinstate the clearance whenever they believe that this action is consistent with the interests of national security, even though the employee is still participating in a rehabilitation or similar program. They must make every effort to complete all investigations expeditiously and obtain all information necessary to make a final determination regarding an employee's clearance; and, when appropriate, reinstate a suspended clearance as soon as possible. When the PSS recommends to the SSE that a clearance should be revoked, they should promptly begin the procedures to do so.

(3) The SSE must ensure adherence to the clearance suspension procedures contained in chapter 10, Adverse Security Actions, of this order, when suspending clearances.

(4) The SSE must coordinate a clearance suspension with the employee's supervisor, and send written notification of the suspension to AIN-400 for inclusion in OPM's Clearance Verification System. It is not necessary for the SSE to inform the operating office in detail of the reason for a suspension, but they must notify the office in writing that the clearance has been suspended and ensure that the employee is notified. As stated in chapter 10, paragraph 3a, of this order, a clearance suspension exceeding 10 days requires written notice to the employee.

c. Security debriefings. PSSs must ensure that all employees who vacate a sensitive position sign FAA Form 1600-25, Security Termination Statement, which constitutes a security debriefing. The official conducting the debriefing must sign the form as a witness. The PSS must keep the completed form for at least 1 year after they receive it. An employee does not need to sign this form when transferring to another sensitive position within the FAA or when a clearance is suspended, and should do so only when employment with FAA ends, a temporary clearance expires, or the person permanently transfers to public trust duties.

10. Visit Clearance Requests.

a. The PSS must process all requests for visit clearances received from other agencies or private companies and provide the appropriate operating office with necessary information regarding visitors' security clearances.

b. The PSS must process visit clearance requests to other agencies and private companies, certifying clearances on DOT Form 1630.5, Department of Transportation Visit Clearance. Operating offices must complete items 1 through 15 on this form before forwarding it to the PSS, and should do so as far in advance of the proposed visit as possible to allow for the sufficient time to process it. The PSS should certify clearances only for the specific dates necessary and in no case for a period longer than 1 year. No FAA employee or office other than the SSE can certify a security clearance to another agency or to a company.

c. The PSS must maintain a copy of all incoming visit clearance requests, and requests processed for FAA operating offices. They should not file them in an individual's personnel security file. All visit request should be destroyed 30 days after completion of the visit.

CHAPTER 10. ADVERSE SECURITY ACTIONS

1. General. This chapter prescribes procedures that the agency must follow after receiving information about an employee or applicant that results in an adverse security action. Such actions include denial, suspension, or revocation of a security clearance for access to classified information.

2. Preliminary Actions.

a. The servicing security element (SSE) must immediately assess the security factors involved when information is received that raises questions concerning the personnel security fitness of a person, and take suitable action to ensure that national security interests are protected. Also, they must consider the conclusiveness and seriousness of the information developed, the employee's access to classified information, and the opportunity the position affords the employee to commit acts contrary to national security interests.

b. The SSE manager can suspend a security clearance, but only the Assistant Administrator for Security and Hazardous Materials, ASH-1, has the authority to revoke or deny a security clearance. The SSE must ensure that strict measures are in place so that a person whose security clearance is being denied or revoked is provided the rights and opportunities stated in E.O. 12968, section 5.2. These opportunities allow the employee the option of appearing personally and presenting relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity.

3. Security Clearance Denial, Suspension, and Revocation.

a. Suspension. The SSE can decide to temporarily suspend a security clearance pending the outcome of an investigation in order to determine if revocation of the clearance is warranted. If the suspension exceeds 10 days, they must notify the employee in writing that the clearance is suspended and why, to the extent consistent with the interests of national security, and also notify the employee's supervisor and the Personnel Security Division, AIN-400.

b. Post Suspension. After the security clearance is suspended, but prior to a determination on whether to reinstate or revoke it, the operating office can, in its sole discretion: restrict the employee to the public trust duties of the position; temporarily reassign the employee to a public trust position with the same grade and pay; or place the employee on administrative leave with pay. They should consider administrative leave only if the other options are not viable.

c. Pre-Denial or Revocation. When the SSE has determined that information received on an employee warrants the denial or revocation of a security clearance, they must forward a written recommendation along with all pertinent supporting information,

including the personnel security file (PSF), to AIN-400 who will review the information and make a determination as to the validity of the proposed denial or revocation.

d. Denial or Revocation.

(1) ASH-1 must notify an employee in writing, to the extent consistent with the interests of national security, that a security clearance is being denied or revoked after a recommendation from the Director, Office of Internal Security and Investigations, AIN-1. The letter must explain why the security clearance is being denied or revoked. The explanation must be as comprehensive and detailed as the national security interests of the United States and applicable laws permit, and must advise the employee that:

(a) he or she has 30 days from the date of the notification to submit a written response to ASH-1 with any supporting documentation, and in that response, the employee can request the opportunity to appear personally before an adjudicative authority;

(b) he or she may request an extension of the response time, but must do so in writing to ASH-1, who will grant or disapprove the extension;

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

(d) he or she has the right to request from the investigating agency the entire investigative file for any investigation on which the decision is based; and

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

(2) ASH-1 must consider all timely responses and any supporting documentation submitted by the employee before making a final decision. ASH-1 must provide an opportunity for the employee to appear in person to respond to the denial or revocation decision, and present any documentary or physical evidence as part of the response. The employee's personal appearance will be at the expense of the Government, but as stated above, any expense for a personal representative will be incurred by the employee. ASH-1 will consider all such evidence before making a final decision, maintain a written summary or recording of any personal appearance, and ensure that all information is placed in the person's PSF. ASH-1 must notify the employee in writing of the final decision, and, if the decision was denial or revocation, explain to the employee that:

(a) he or she may appeal the decision to the Personnel Security Review Board chaired by the Office of Security, M-40, Office of the Secretary; and

(b) the review request must be in writing and submitted to M-40 within 30 days from the date of the final decision. ASH-1's decision will become the final decision on the employee's security clearance if he or she does not appeal to M-40 within 30 days.

e. Post Denial or Revocation.

(1) AIN-400, in coordination with the SSE will provide the Human Resource Management Division (Personnel) and the operating office all information necessary to take appropriate action under the FAA's Personnel Management System, after the procedures outlined in paragraph 3c of this chapter, are completed and a security clearance is revoked. Such action can include removing the employee or permanently reassigning him or her to a public trust position. When an employee is removed, the Personnel office must inform AIN-400 through the SSE of the action.

(2) After the procedures outlined in paragraph 3c of this chapter have been completed and a security clearance has been denied, the SSE and Personnel office must ensure that:

(a) the person will not be appointed to a position for which a clearance is required if the person denied a clearance is an applicant; or

(b) appointment or reassignment to the sensitive position will not be made if the person denied a clearance is an employee occupying a public trust position that was selected for a position requiring a clearance.

4. Appeal. E.O. 12968, section 5.2(a)(6) provides each employee or applicant whose security clearance has been denied or revoked an opportunity to appeal in writing to a high-level panel appointed by the agency. The Secretary of Transportation has chartered the Personnel Security Review Board (the Board) to fulfill this requirement. The Board adjudicates final appeals originating in any DOT administration.

a. The Board is comprised of at least three members, two of whom are selected from outside the security field.

b. The Board acts on behalf of the Secretary, except in any case in which the Secretary personally elects to make the final decision on an appeal, and makes the administratively final decision on appeals by DOT personnel of security clearance denial or revocation actions originating in any DOT organization. It has the authority to direct the granting of a clearance that a DOT administration or organization has denied, and to direct the reinstatement of a revoked clearance as if it had never been revoked. Board decisions are in writing.

c. The Board is chaired by a member from DOT's Office of Security, M-40, as appointed by the Assistant Secretary for Administration, M-1, and, may, with the approval of M-1, establish its own operating procedures.

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

5. Employment of Individuals Previously Separated for Security Reasons. The FAA cannot employ any person who has been separated from employment with any department or agency of the U.S. Government under any Federal security program (such as 5 U.S.C. Sections 7531-33, E.O. 9835, or E.O. 10450) without prior approval of the Secretary and determination by the Personnel office that the factors leading to the separation are not currently disqualifying for FAA employment. When employment of such a person is proposed, AIN-400, through the SSE, must obtain complete information regarding the basis for the separation, ensure appropriate investigation of the person's subsequent activities, ascertain whether the Personnel office has determined that the person is eligible for FAA employment, and obtain any other information the Secretary of Transportation needs to decide whether or not the person's employment is clearly consistent with the interests of national security. They must then forward this information to M-40 for forwarding to the Secretary. This approval authority will not be redelegated.

CHAPTER 11. ACCESS TO INFORMATION RESOURCES

1. General.

a. Under Office of Management and Budget Circular Number A-130, Management of Federal Information Resources, dated November 30, 2000, we, the FAA, must establish and manage personnel security policies and procedures to ensure an adequate level of security for Federal information resources. The Office of Personnel Management prescribes guidance for agency policies and procedures for information resources security which applies to all Federal employees. The FAA is required to screen all persons participating in the design, development, operation, or maintenance of sensitive applications, as well as, persons having access to sensitive information.

b. The Federal Information Security Management Act of 2002 requires Federal agencies to identify each computer system that contains sensitive information and prepare a plan for the security and privacy of each such system. P.L. 100-235 defines sensitive information as any information that if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Proprietary data is included as sensitive data.

c. FAA Order 1370.82, Information Systems Security (ISS) Program, establishes FAA's information resources security program and provides detailed guidance to ensure that we implement an appropriate level of information resources security throughout our data processing activities.

d. Personnel security is an integral part of ISS. It ensures sufficient protection for information resources and their data. Chapter 4 of this order contains procedures for designating position risk levels commensurate with duties and responsibilities involving information resources. This chapter contains personnel security requirements and procedures for information resources access. Because of the nature of information resources and the ease with which large amounts of data can be retrieved, manipulated and deleted, we are more stringent with access requirements than for the same level of data contained in records systems outside information resources.

2. Access Requirements.

a. Access defined. A person has information resources access when he or she can exercise privileges to read or write information or data electronically stored or processed in a digital format.

b. Level I data is authorization to read or write classified information or data electronically stored in a digital format. Any employee granted access to information systems Level I data must first have the appropriate level security clearance.

c. Level II data is authorization to read or write sensitive but unclassified or Privacy Act information or data that is electronically stored in a digital format. Any employee granted access to a portion of an information system containing Level II data must first have at least a completed National Agency Check with Inquires (NACI), or has met the investigative requirements in chapter 5, section 2, paragraphs 1 and 2 of this order.

d. Level III data is authorization to read or write unclassified and non-sensitive information or data electronically stored in a digital format. For an employee in a position requiring information resources access only to Level III data, the minimum investigative requirement will be a fingerprint check, unless the position is located in a critical-area, in which case the investigation requirement will be a NACI.

3. Procedures.

a. The servicing security element (SSE) must notify the operating office as to whether or not an employee meets the investigative requirements for access to the applicable level(s) of data in information systems, when a person is appointed to a position identified as an information resources position for which Level I or II access is required. On behalf of the SSE, the personnel security specialist (PSS) can grant an employee at least an interim clearance that would allow access to the level of classified information the information system contains, if Level I access is required and the employee does not have the required security clearance (refer to chapter 9 of this order). The PSS can expedite completion of the National Agency Check (NAC) portion of the NACI, and notify the operating office when the requirement is met if Level II access is required and the employee does not have a completed and favorably adjudicated NACI. Advance reports of NACs should be requested when possible.

b. The PSS must use the suitability criteria found in chapter 7 of this order and the PSS Supplement for adjudicating results of a NACI for access to Level II data. They must coordinate with the operating office regarding the delay in granting access when unfavorable information is developed which precludes granting information systems access pending completion of the investigation.

c. The PSS must not deny an employee access to any level of data in information systems based on information developed during an investigation without providing him or her due process as specified in chapter 2 of this order.

d. When the required investigation is completed, the results of the suitability adjudication process will determine whether or not the employee receives access to information resources data.

CHAPTER 12. FOREIGN ASSIGNMENTS AND TRAVEL

1. General. As the FAA, we are required to take special safeguards to protect the national interest and national security information when our employees and representatives are given foreign assignments or perform official foreign travel. For this purpose, a "foreign" location means outside the 50 states, the District of Columbia, Puerto Rico, or any of the United States possessions, territories, or trust territories. The investigative requirements and security precautions specified in this chapter apply to employees and representatives on foreign assignments or travel. Our employees assigned 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 United States 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 Department of State (DOS) regulations, all employees assigned to work in or have unescorted access to the controlled access area of an embassy or embassy annex must hold at least a Top Secret clearance. Other employees are not required to hold security clearances unless their duties require them to have access to classified information.

(2) The personnel security specialist (PSS) must ensure that all foreign positions are designated as high risk, critical sensitive or special sensitive, and employees who are selected for these positions have at least a completed and favorably adjudicated Background Investigation (BI) prior to transfer to the foreign location.

(3) The PSS must 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, Department of State, Washington, DC, 20520, for transmission to the post.

b. Personal service agreement (PSA) personnel. These are U.S. citizens who are family members of U.S. personnel stationed in foreign countries, and who are technically PSA employees under arrangements made through DOS.

(1) The PSS must ensure that all PSA employee positions are designated as high risk or critical sensitive and that they have a completed and favorably adjudicated BI or SSBI prior to being assigned to the position.

(2) The PSS will issue security clearances to PSAs only if they are required to have access to classified information or to sensitive areas at locations that receive, process, or store classified or other foreign policy or operationally sensitive information or material.

c. Temporary duty (TDY).

(1) The PSS must ensure that an employee who is to be on TDY intermittently or continuously for more than 120 days in 1 year has a completed BI prior to beginning the travel.

(2) The PSS does not need to apply any 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) Under DOS regulations, an FAA employee will not have unescorted access to U.S. Government facilities while on TDY unless he or she holds at least a Secret clearance. An employee can be escorted, however, while at an embassy or embassy annex if he or she does not have a clearance.

(4) The operating office must determine whether or not an employee should be issued a security clearance while on TDY. The decision must be based on the nature of the work to be performed; the extent, nature, and location of contacts with FAA and other Government officials; the length of the TDY; and whether or not he or she will be inconvenienced by having to be escorted. In many cases, not being allowed unescorted access for one visit to an office or embassy in a foreign location will not be an inconvenience to an employee.

(5) The operating office must contact the servicing security element (SSE) as far in advance of the trip as possible, when they determine that clearance information needs to be provided to DOS for an employee scheduled for TDY. DOS requires that the level of clearance be stated in the travel message and on the travel authorization. However, no such information should appear on any message or travel authorization without coordination with the SSE.

(6) The operating office must send a written request to the SSE for a temporary clearance if an employee scheduled for TDY needs a security clearance and does not have one. They must state in the request, the period of time for which the clearance is needed, the location(s) to be visited, and, specifically, why the clearance is necessary.

(7) The PSS must transmit clearance data for employees going on TDY, as necessary, per paragraph 2a(3) above.

d. International conferences.

(1) Head of a delegation. PSSs must ensure that any FAA employee selected to head a delegation from the United States to an international conference on other than a one-time basis is subject to a BI.

(2) Nominee as FAA representative at an international conference. Nomination to represent FAA at an international conference is subject to completion of a National Agency Check (NAC) or higher-level investigation. This investigation has normally been conducted on Federal employees, but not necessarily on technical advisors or other representatives from industry. If an advisor from industry is selected to represent us at an international conference, the FAA office arranging for the advisor's services must contact the SSE least 3 weeks prior to the date that the delegation is scheduled to depart. The PSS will then determine if a NAC was already conducted on the industry representative, for example, if the person holds a Government security clearance or is a military reservist. They will furnish the responsible office with forms for the person to complete, if a NAC has not been completed. The office must then ensure that the forms are completed and returned to the PSS to process the NAC. A NAC 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 the North Atlantic Treaty Organization (NATO) headquarters in Brussels, Belgium, NATO requires a person to have a NATO clearance. An operating office arranging for an FAA employee to visit NATO headquarters or a similar activity must ensure in advance that they contact their SSE to process any special clearance(s) required. They should ask about clearance requirements when making the visit arrangements and provide the request to security at least 3 weeks in advance of the visit to allow time for processing.

CHAPTER 13. SECURITY CLEARANCES AND AUTHORIZATIONS FOR IMMIGRANT ALIENS

1. General. Aliens are identified as either foreign nationals or immigrant aliens (refer to Appendix A). Foreign nationals are not eligible for FAA security clearances but can be granted Limited Access Authorizations. When special compelling circumstances warrant a broader "need to know," they can be processed for DOT security clearances. The Director, Office of Security, M-40, Office of the Secretary, is authorized to grant Limited Access Authorizations and security clearances to non-citizens. This authority is not further delegated. Allowing foreign nationals to repair or modify National Airspace Systems equipment or to have access to its technical data may be considered a "deemed export" and be prohibited under the Department of Commerce, Export Administration Regulations, 15 C.F.R. 730 et seq. Consult with FAA's Office of the Assistant Chief Counsel, Procurement Law Division, AGC-500, for possible restrictions.

2. Investigative Requirements for Foreign Nationals. A Background Investigation (BI) that includes overseas coverage to the fullest practicable extent is the minimum basis for granting a Limited Access Authorization or a security clearance to an alien.

3. Procedures for Limited Access Authorizations.

a. In consultation with the Office of Internal Security and Investigations, AIN-1, the servicing security element (SSE) must make a determination that specific classified information is releasable to the alien concerned. The office proposing use of the alien's services must submit a request for a Limited Access Authorization for him or her to their SSE identifying the information involved and the level of its 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.

b. The SSE must send the request with the investigative forms to the Personnel Security Division, AIN-400, who will send the package to M-40, for initiation of the required investigation. M-40 will adjudicate the investigation when it is completed and notify the SSE through AIN-400 of the results.

c. The SSE must ensure that persons to whom Limited Access Authorizations are granted are subject to the same security briefing and debriefing requirements as for a security clearance.

4. Procedures for Immigrant Alien Security Clearances.

a. The office proposing use of an immigrant alien in a sensitive position must submit a request to the SSE for the processing of a security clearance, when use of a Limited

Access Authorization is impracticable. The request must explain why the clearance is needed and state the specific tasks or projects on which the person will be working.

b. The requesting office must determine that the immigrant alien has no military obligations or other commitments to the country of which he or she is a citizen that would require him or her to serve the interests of that country's government in preference to U.S. interests.

c. The requesting office must ensure that the person has valid immigrant alien status.

d. The SSE must send the request with the investigative forms to AIN-400 who will send the package to M-40 for initiation of the required investigation. M-40 will adjudicate the investigation when it is completed and notify the SSE through AIN-400 with the results.

e. M-40 can issue an interim Secret or Confidential clearance to an immigrant alien based on the completion of a favorable National Agency Check pending completion of the BI. When the investigation is completed, M-40 will issue the final clearance or a Limited Access Authorization in lieu of a clearance. The usual security briefing requirements apply.

f. If the immigrant alien is not naturalized within 1 year following the date on which the residence requirements are met, the SSE must revoke the clearance and consider that the person reverted to foreign national status. M-40 can authorize extensions of the time limit if the SSE concludes that the delay is due to reasons beyond the person's control.

5. Approval for Visits by Foreign Nationals Cleared by Other Agencies. No FAA office will accept security clearances for foreign nationals granted by other U.S. Government agencies for visits, conferences, or other purposes without approval from M-40. The office involved must present justification to, and request approval from, M-40 through AIN-400 to the SSE.

CHAPTER 14. NATIONAL EMERGENCY PERSONNEL SECURITY PROCEDURES

1. Purpose. This chapter provides authority and procedures for planning and conducting personnel security operations in FAA under national emergency conditions, a major attack upon the United States, and lesser national emergency conditions that make it impossible or impracticable to follow normal personnel security procedures.

2. Activation of Standby Procedures.

a. The servicing security element (SSE) will activate the following standby procedures FAA-wide without further justification if a major attack upon the United States occurs which causes serious disruption of all types of communication.

b. The SSE will activate these procedures upon receipt of notice from the Secretary of Transportation that the Office of Personnel Management is temporarily deferring or discontinuing conducting investigations required by E.O. 10450.

c. The Assistant Secretary for Administration, DOT, will activate these procedures within prescribed FAA organizations or in specific geographical areas that so specifies. This decision will be based on a whether the major disaster conditions, other than an attack on the United States, make it impracticable to meet standards for investigations in subsection 3 of E.O. 10450.

3. Standby Procedures: Modification of Investigative Requirements. The Secretary of Transportation delegates special authority needed to continue personnel security operations under national emergencies. The SSE can deviate from normal personnel security requirements if they are notified that these standby procedures have been activated:

a. Authority to fill sensitive positions. The SSE can authorize filling of special-sensitive, critical-sensitive, and non-critical-sensitive positions for a limited period without the required pre-placement investigation, provided the personnel security specialist (PSS):

(1) obtains existing investigations and conduct investigations as practicable under the circumstances to afford the maximum feasible protection of national security interests;

(2) to the extent practicable under the circumstances, completes as many of the requirements for waiver of pre-placement investigations as possible that are specified in chapter 5, section 2, paragraph 1, of this order; and

(3) initiates the required investigations as soon as conditions permit.

b. Authority to fill moderate and high-risk positions. The SSE can authorize filling of moderate and high-risk positions for a limited period without the required pre-placement investigation, provided that the PSS:

- (1) obtains existing investigations and conduct investigations as practicable under the circumstances;
- (2) to the extent practicable, completes as many of the requirements for waiver of pre-placement investigations as possible that are specified in chapter 5, section 2, paragraph 1, of this order; and
- (3) initiates the required investigations as soon as conditions permit.

c. Authority to defer investigation for non-sensitive positions. The SSE can authorize that the National Agency Check and Inquiries investigation for non-sensitive positions be deferred and require only an investigation that they determine is feasible under the circumstances.

d. Authority to grant clearances on modified investigative requirements. The PSS will evaluate information developed in interim investigations using the personnel security standards and criteria contained in this order and record their determinations. On the basis of the interim investigations, they can grant interim clearances for required access to specific levels and types of classified information pursuant to E.O. 12958 and in the interests of the defense of the United States. The PSS must discontinue these clearances when the required investigations are completed and adjudicated.

4. Required Plans for Personnel Security Operations During a National Emergency.

The SSE must provide for the following plans for personnel security operations under national emergency conditions:

a. Designation and training of primary and alternate resources to conduct personnel security operations at relocation sites or under other emergency conditions.

b. Development of specific procedures to be followed in activating emergency personnel security operations.

c. Design of effective methods of pre-positioning and updating personnel security data at relocation sites.

d. Arrangement for appropriate materials and equipment available for emergency operations.

e. Assignment of sufficient investigative resources to ensure all feasible protection of national security interests under the reduced emergency investigative standards.

CHAPTER 15. PROGRAM EVALUATION

1. Introduction. The Personnel Security Program evaluation within the FAA was established to ensure that products and services provided by the Office of the Assistant Administrator for Security and Hazardous Materials, ASH, appropriately satisfy our mission, meet established standards, and are consistent with agency policy. The Office of Internal Security and Investigations, Personnel Security Division, AIN-400, is responsible for conducting these evaluations at FAA headquarters, and at the regional or center servicing security element (SSE). The program evaluation includes a review of both employees and contractors and is conducted in the SSE.

2. Program Mission Statement. Program evaluation applies to the FAA's Personnel Security Program, and includes employees, applicants and contractors. They are conducted to ensure:

a. Consistent, efficient, and appropriate implementation of the laws, orders, and procedures that govern personnel security by all responsible entities.

b. Employment of persons by the FAA promotes the efficiency of the agency and is in the best interest of the national security.

3. Evaluation Standards.

a. AIN-400 will select a team of two or more persons to conduct the evaluation. The team will consist of a team leader, generally filled by one member of the Program Evaluations and Policy Staff from AIN-400, one or two team members who are generally headquarters personnel security specialists (PSS), and, when practicable, a regional or center PSS or assistant.

b. The team's primary focus of the evaluation is to:

(1) Assess program effectiveness.

(2) Determine compliance with applicable laws, orders, and procedures.

(3) Measure performance against established standards.

(4) Provide a means to share local successes and solutions applicable FAA-wide.

c. The team leader must ensure the region or center office to be evaluated is notified at least 30 days prior to commencement of the evaluation.

4. Evaluation Criteria. The criteria below must be followed as the foundation to the conduct an evaluation.

- a. The risk or sensitivity level of a position identified in the Consolidated Personnel Management Information System or the Investigations Tracking System is appropriately designated.
- b. The personnel security investigation is appropriate for the position risk/sensitivity level.
- c. Personnel security investigations are conducted and properly adjudicated.
- d. Procedures are established for the review of personnel security investigative forms and are effective in ensuring completeness.
- e. Proper waiver procedures and interim suitability determinations are in effect.
- f. Procedures are established to ensure sufficient investigations are conducted, and if deficient, ensure appropriate measures are taken to correct the deficiency.
- g. Follow-up information is collected expeditiously to advance the adjudication process.
- h. Reinvestigations are conducted on employees in high-risk, special-sensitive, and critical-sensitive positions every 5 years.
- i. Reinvestigations are conducted on employees in non-critical-sensitive positions who hold Secret clearances every 10 years.
- j. Procedures are in place for withdrawal or downgrade of security clearances, as appropriate, to ensure persons who have been deemed untrustworthy or without the required *need to know* can no longer access classified information.
- k. Procedures are in place for ensuring due process is provided to all FAA employees and applicants.
- l. A sufficient security clearance process is in place.
- m. Procedures are in place for the protection of Privacy Act Information.
- n. Personnel Security Files contain the accurate and appropriate documentation.

5. Responsibilities.

- a. The team will follow the guidelines outlined in this order and the latest edition of FAA Orders 1600.72, Contractor and Industrial Security Program, and 1600.73, Contractor and Industrial Security Program Operating Procedures. Through careful planning, preparation, coordination, organization, and implementation, they can achieve a

successful program evaluation. The following information should serve as the team's handbook and be strictly followed in order to provide criteria and steps for the best manner in which to assess the chosen areas. Alternative or additional steps can be conducted only after consultation with the team leader. Each team member is expected to understand the requirements set forth in the referenced orders and become familiar with the steps to be performed to facilitate an efficient and effective program evaluation.

b. Preliminary phase. The team leader must:

- (1) Notify the office to be evaluated, in writing, at least 30 days prior to commencement of the on-site evaluation.
- (2) Review any requested materials in conjunction with the evaluation.
- (3) Arrange an in-brief and out-brief with site management.
- (4) Arrange interviews with regional PSSs and assistants, and managers who have oversight of the Personnel Security Program.

c. On-site evaluation. Team members are responsible for:

- (1) Conducting or attending the in-brief with site management. This briefing is an opportunity for the team leader to introduce team members, explain the evaluation process, and give details on the steps to be taken to achieve the team's goals. It also allows the team to obtain an overview of the office, its personnel, and its priorities, and offers management an opportunity to inform the team of their expectations of the evaluation.
- (2) Documenting all evaluation activities conducted and ensuring that the documentation is accurate, complete, concise, and sufficient. This should be done on a daily basis.
- (3) Conducting daily briefings with site management to discuss progress and preliminary findings, as appropriate.
- (4) Collecting all necessary supporting documentation.
- (5) Attending an out-brief with site management to discuss findings and advise them that a report will be completed and forwarded to the office within 60 days.

d. Reports.

(1) The team leader is responsible for ensuring that the report is written based on daily documentation of the findings, recommendations, and observations. It is the primary official written record of a program evaluation and is intended to provide senior management with concise, candid evaluations of policy and program effectiveness, and to inform them of conditions or situations that require attention or intervention. The team must stress major issues and shortcomings, as well as, noteworthy contributions to program operations and the FAA in the report.

(2) The team leader must determine which findings to include in the report, to whom each recommendation should be addressed (by responsible office, not by individual name), and into which category findings and recommendations fall. They must describe the report in the context of established policy and sound management practices.

(3) The team leader will complete the final report within 60 days of the conclusion of the evaluation and submit it to senior management.

6. Preliminary Phase Process.

a. Prior to conducting the program evaluation, the team must obtain from the site:

(1) Copies of previous evaluations conducted at the site, if applicable.

(2) Lists of randomly-selected headquarters or regional/center FAA employees by lines of business identified by the team leader. This list must contain, at a minimum, the following information for each employee:

(a) Full name (last, first, middle)

(b) Social security number (SSN)

(c) Position title

(d) Position risk/sensitivity level

(e) Type of investigation conducted and date of completion

(3) List of all headquarters or regional/center FAA employees who hold security clearances. This list must contain, at a minimum, the following information for each employee:

(a) Full name (last, first, middle)

- (b) Social security number (SSN)
- (c) Position title
- (d) Position sensitivity level
- (e) Type of investigation and date of completion
- (f) Type of clearance
- (g) Date security clearance was granted, downgraded, cancelled, if applicable

(4) List of all FAA employees who are in moderate and high-risk positions. This list must contain, at a minimum, the following information for each employee:

- (a) Full name (last, first, middle)
- (b) Social security number (SSN)
- (c) Position title
- (d) Position risk level
- (e) Level/type of investigation conducted and date of completion.

(5) List of all FAA contractors chosen from randomly-selected contracts. This list must contain, at a minimum, the following information for each employee:

- (a) Full name (last, first, middle)
- (b) Position title, if applicable
- (c) Position risk level
- (d) Level/type of investigation conducted and status
- (e) Date investigation was closed
- (f) Date of adjudication and whether it was favorable

b. The team will randomly select a representative sample of names from each list to review and document.

7. On-site Evaluation Process. The team will have an interview process in place that includes managers, regional team leaders with personnel security oversight, and PSSs and assistants from the SSE when conducting the program evaluation. These interviews can provide valuable information on the Personnel Security Program at the review site, as well as, ideas and suggestions for program and process enhancement. The team must:

a. Interview all PSSs and assistants to determine compliance with this order and FAA Orders 1600.72 and 1600.73.

b. Interview PSSs to ensure that procedures are established for the following: completeness of investigative forms; resolution of issues prior to granting a waiver or approving interim suitability determinations; conducting required investigations; adjudications; and granting security clearances. Also, offer the specialists the opportunity to provide any suggestions for improving these processes.

c. Review all pertinent Personnel Security Files and contract files in conjunction with this review.

d. Review the electronic data of lists of employees/contractors that were requested during the preliminary phase, and randomly select names to verify that the investigation level matches the risk/sensitivity level of the position.

e. Review Personnel Security Files for every employee who is assigned to the respective Security and Hazardous Materials Division.

8. Findings and Recommendations. Findings and recommendations are the teams contributions to improving program performance and helping the SSE handle problems more effectively. The team must ensure that recommendations are specific and clearly stated in simple language; practical and direct based on the current situation; and directed to the office, not the individual, responsible for the problem.

9. Supporting Documentation. The team must obtain sufficient and relevant documentation during an on-site review in order to support findings and recommendations. Each review step defines the required supporting documentation.

a. Representative numbers. Some of the steps require review of a representative number or percentage of documents, or interview of a representative number or percentage of persons. While not statistically valid samples, the number is sufficient to identify problematic areas and patterns.

(1) For reviews of employees and contractors, the number will not be less than 20%; unless the total number available is less than 25, in which case, the percentage to review will be 100%.

(2) For reviews of employees assigned to the Security and Hazardous Materials Divisions, the percentage will be 100%.

b. Supporting documentation. The team will use a form of review worksheet for original notes taken during interviews and document reviews. Information documented on these worksheets form the basis for the findings and recommendations. Some of the steps require the team to collect documents. They do not have to copy every document reviewed but should make copies of documents that indicate noncompliance and inefficiencies or innovative and highly successful practices.

10. Report Writing and Retention.

a. The team must include findings, corrections made (if corrections were made at the time of the on-site review), recommendations, and identification of best practices, if applicable in the report.

b. The team will prepare a written report for each program evaluation conducted and provide the final report to ASH-1, and the Office of Field Operations, AHS-1, within 60 days of the conclusion of the on-site review.

c. A copy of the report will be forwarded to the responsible SSE manager with a memo describing all findings. The SSE manager must respond in writing to AIN-400 through AHS-1 within 60 days after receipt of the report certifying all corrective action(s) that was taken.

d. The SSE must retain a copy of the program evaluation report for his or her site.

e. AIN-400 will retain a copy of the reports and all documentation for all program evaluations they conduct.

APPENDIX A. DEFINITIONS

- 1. Access.** In general, the ability to enter or pass through an area or a facility, or the ability or authority to obtain information or monetary or material resources. In relation to classified information, the ability, authority, and opportunity to obtain knowledge of such information.
- 2. Access Authorization.** Certification that a person is currently authorized to have access to classified information at specific levels.
- 3. Access National Agency Check and Inquiries (ANACI).** An investigation consisting of a National Agency Check, written inquiries, record searches, and a credit check covering specific areas of a person's background during the most recent 5 years.
- 4. Appointing/Approving Official.** The individual delegated the authority to effect appointments, reassignments, promotions, separations, or similar personnel actions regarding FAA employees or applicants.
- 5. Background Check.** Any personnel investigation conducted to meet requirements.
- 6. Background Investigation (BI).** An investigation consisting of a National Agency Check, credit search, personal interviews of Subject and sources, written inquiries, and record searches covering specific areas of a person's background during the most recent 5 years, and additional record searches during the most recent 7 years.
- 7. Child Care National Agency Check and Inquiries (CNACI).** An investigation consisting of a National Agency Check, written inquiries, state criminal history repositories checks, and record searches covering specific areas of a person's background during the most recent 5 years.
- 8. Classified Information.** Official information or material that requires protection in the interest of national security and is classified for such purpose by appropriate classification authority in accordance with the provisions of Executive Order 12958, Classified National Security Information.
- 9. Cohabitant.** An individual with whom the Subject lives, other than a spouse, child, or other relative (mother, father, brother, sister, in-laws, etc.), with whom a bond of affection, influence, obligation, or a spouse-like relationship exists.
- 10. Defense Clearance and Investigations Index (DCII).** An automated index of all investigations conducted by the Department of Defense (DOD) on military personnel, DOD civilian employees, and applicants.

- 11. Due Process.** A process that is established to protect individual rights and liberties which provides the Subject an opportunity to deny, explain or refute any allegations or adverse information used in an investigation.
- 12. FAA Employee.** Any person employed directly by the FAA. (Does not include contractors.)
- 13. Felony.** A conviction of a crime that is punishable by a possible imprisonment of more than one year.
- 14. Foreign National.** An individual who is not a citizen of the United States.
- 15. Immigrant Alien.** An individual who is lawfully admitted to the United States under an immigration visa for permanent residence.
- 16. Information Systems.** A discrete set of information resources, either in stand-alone or networked configurations, which are organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.
- 17. Interim Access Authorization.** An authorization for access to classified information granted pending completion of the required investigation.
- 18. Limited Background Investigation (LBI).** An investigation consisting of an National Agency Check, credit search, personal interviews of Subject and sources, written inquiries of selected sources covering specific areas of a person's background during the most recent 3 years, and record searches for a total of 5 years' coverage.
- 19. Limited Access Authorization.** A certification that a person is authorized to have access only to certain specified classified information which has been carefully screened by security officials for its release to that person.
- 20. Local Agency Check (LAC).** A check of records at a state or local law enforcement agency.
- 21. Minimum Background Investigation (MBI).** An investigation consisting of a National Agency Check with Inquiries, Subject interview, a credit search and telephone inquiries to follow up on written inquiries not returned.
- 22. National Agency Check (NAC).** An investigation consisting of searches of the following files: Security/Suitability Investigations Index (SII), DCII, the Federal Bureau of Investigation's (FBI) Identification Division, and the FBI's Records Management Division.

- 23. National Agency Check with Inquiries (NACI).** An investigation consisting of a National Agency Check, written inquiries, and record searches covering specific areas of a person's background during the most recent 5 years.
- 24. National Agency Check with Law Enforcement Inquiries and Credit (NACLIC).** An investigation consisting of a National Agency Check, written inquiries from law enforcement agencies, record searches, and a credit check covering specific areas of a person's background during the most recent 5 years.
- 25. National Security.** The protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs, from overt and covert attack, against or from espionage, sabotage, and subversion, and any and all illegal acts designed to weaken or destroy the United States.
- 26. National Security Position.** A position involving Government activities concerned with the protection of the national security.
- 27. Need to Know.** A determination made by an authorized holder of classified information that a prospective recipient requires access to, knowledge of, or possession of specific classified information to perform or assist in a lawful and authorized U.S. Government function or program.
- 28. Operating Office.** A line of business, an office or service in headquarters, or a division level organization in a region or center.
- 29. Periodic Reinvestigation (PRI).** An investigation updating a previous investigation and consisting of a National Agency Check, credit search, personal interview of the Subject, and selected record searches.
- 30. Periodic Reinvestigation for Single Scope Background Investigation (SSBI-PR).** An investigation updating an SSBI consisting of personal interviews of the Subject and sources, a National Agency Check, credit search, and written inquiries and record searches covering specific areas of a person's background during the most recent 5 years.
- 31. Personal History Statement.** Any data that contains personal information about an individual, such as, investigative forms, resume, SF-171, etc.
- 32. Personnel Investigation.** An investigation conducted to aid in determining an applicant's or employee's suitability for employment, qualifications for a position, or loyalty to the United States.
- 33. Personnel Security.** The standards and procedures utilized to determine and document that the employment or retention in employment of an individual will promote

the efficiency of the service and is clearly consistent with the interests of the national security.

34. Personnel Security Adjudicator. An individual in the servicing security element who conducts security adjudication.

35. Personnel Security Coordinator (PSC). An employee of an operating office assigned to coordinate personnel security functions among his or her organization, the servicing security element, and the Human Resource Management Division.

36. Personnel Security Manager. A specifically appointed individual within an agency who is primarily responsible for management and operation of the .

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

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

39. Proprietary Information. Confidential commercial or financial information.

40. Public Trust Position. A position which has the potential for action or inaction by an incumbent to affect the integrity, efficiency, or effectiveness of assigned Government activities.

41. Reimbursable Suitability Investigation (RSI). An investigation conducted by the Office of Personnel Management to resolve a suitability issue raised in a previous investigation.

42. Resources. Material and monetary items of value, such as, facilities, equipment (including, but not limited to, computers, facsimile machines, photocopiers, printers, and furniture), information databases (both hardware and software), and records in whatever form they exist.

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

44. 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. (Often referred to as a security determination.)

45. Security Clearance. Access to classified national security information at a specific level.

- 46. Security/Suitability Investigations Index (SII).** The Office of Personnel Management's (OPM) index of investigations conducted by OPM and by other agencies as reported to OPM.
- 47. Sensitive Security Information (SSI).** Information that is sensitive but unclassified that has restrictions placed on its release and disclosure.
- 48. Servicing Security Element (SSE).** The headquarters, region, or center organizational element that is responsible for providing security services to a particular activity.
- 49. Single Scope Background Investigation (SSBI).** An investigation consisting of a National Agency Check, birth records search, credit search, personal interviews of Subject and sources, written inquiries, and record searches covering specific areas of a person's background during the most recent 10 years.
- 50. Special Agreement Check (SAC).** A limited investigation (or a series of checks) conducted on a Subject, done only through special agreement between the Office of Personnel Management and an agency.
- 51. Suitability.** Fitness or eligibility for employment referring to identifiable character traits and past conduct that 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.
- 52. Suitability Adjudication.** The process of determining a person's suitability for Federal employment in a particular position.
- 53. Temporary Clearance.** An authorization for access to classified information granted for a limited period of time.
- 54. Unauthorized Disclosure.** A communication or physical transfer of classified information to a recipient unauthorized to receive it in the given circumstances.
- 55. Upgrade Investigation (UGI).** An investigation consisting of a National Agency Check, credit search, personal interviews of the Subject and selected sources, and record searches covering specific areas of a person's background since the last investigation. This investigation is for movement upward in sensitivity/risk level from between 13 to 60 months of the previous investigation's closing date. (Refer to chapter 5, section 1, paragraph 2.)
- 56. Update Investigation (UDI).** An investigation consisting of the same type of coverage as a previous investigation, conducted from between 13 and 60 months of that investigation. (Refer to chapter 5, section 1, paragraph 2.)

APPENDIX B. SAMPLE LETTER FOR DCII CHECKS

Defense Investigative Service
Investigative Files Section
Box 1211
Baltimore, Maryland 20203

Attn: DO960

Dear Sir or Madam:

Please conduct the appropriate DCII checks on the individual(s) listed below:

<u>Name</u>	<u>DPOB</u>	<u>SSN</u>
-------------	-------------	------------

Mail results to:

Attn: (Name - Personnel Security Officer)
Federal Aviation Administration
Investigations Division, AIN-400
800 Independence Avenue, SW.
Washington, DC 20591

1. Purpose Code: 06
2. Accreditation: XE023

Thank you for your cooperation in this matter.

Sincerely,

cc: AIN-400

APPENDIX C. PERSONNEL SECURITY FORMS

<u>Form Number</u>	<u>Form Name, National Stock Number, Unit of Issue, Supply Source</u>
SF-85	Questionnaire for Non-sensitive Positions, 7540-00-634-4035, 100, GSA
SF-85P	Questionnaire for Public Trust Positions, 7540-01-317-7372, 100, GSA
SF-85P-S	Supplemental Questionnaire for Selected Positions, 7540-01-368-7778, 100, GSA
SF-86	Questionnaire for National Security Positions, 7540-00-634-4036, 100, GSA
SF-86A	Continuation Sheet for Questionnaires SF-86, SF-85P, and SF-85, 7540-01-268-4828, 100, GSA
SF-87	Fingerprint Chart (Government employee), 7540-00-634-4037, 100, GSA
SF-312	Classified Information Nondisclosure Agreement, 7540-01-280-5499, GSA
OF-306	Declaration for Federal Employment, 7540-01-368-7775, 100, GSA
FD-258	FBI Fingerprint Chart (for contractor employee).*
DOT Form 1600.14	FBI Record Check Request.**
DOT Form 1630-5	Department of Transportation Visit Clearance.**
FAA Form 1600-12	Investigative Record Review, 0052-00-621-6003, sheet, FAA Depot
FAA Form 1600-25	Security Termination Statement, 0052-00-408-6001, sheet, FAA Depot
FAA Form 1600-54	Notification of Personnel Security Action, 0052-00-869-400, set, FAA Depot
FAA Form 1600-59	Position Risk/Sensitivity Level Designation Record, 0052-00-900-1000, set FAA Depot
DOT Form 1631	Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
OFI 79B	Notice of Personnel Investigation or SII Search Request***
OPM FIPC Form 391	Certification of Amended Investigative Form***

* No stock number or set unit of issue. Available from Federal Bureau of Investigation, Identification Division, Washington, DC 20537.

** No stock number or set unit of issue. Available from the Office of Security (M-70), Office of the Secretary.

*** No stock number or set unit of issue. Available from Supply Clerk, Operations Support Branch, OPM-FIPC, Boyers, PA 16018.

APPENDIX D. STATUTORY DEBARMENT ISSUES

The following issues require automatic debarment from Federal employment for the period specified below. The legal authority for debarment should be consulted prior to taking debarment action.

Issue	Debarment Period	Legal Authority
Illegally receiving, seeking, promising or offering compensation for services in matters affecting the Government	Permanent*	18 U.S.C.203
Current, habitual use of intoxicating beverages to excess	NTE 3 years	5 U.S. C. 7352
Membership in the Communist Party	Permanent	50 U.S. C. 784, et. seq.
Evidence of disloyalty; participation in a strike against the Government or knowing membership in an organization that asserts the rights to strike against the Government	Permanent	5 U.S.C. 7311; 18 U.S.C. 1918
Willful and unlawful concealment, removal, mutilation, or destruction (or attempts at the above) of public records and materials	Permanent	18 U.S.C. 2071(b)
Inciting, organizing, promoting, encouraging, engaging, or aiding others to engage in riots or civil disorder	5 years from the date the conviction becomes final	5 U.S.C. 593
Interference by an officer or member of the armed forces with elections	Permanent*	18 U.S.C. 593
Unlawful trading in public property by a collecting or disbursing officer	Permanent*	18 U.S.C. 1901
Unauthorized disclosure of information by a farm credit examiner	Permanent*(from employment examiner only)	18 U.S.C. 1907
Unauthorized disclosure of information by a National Agriculture Credit Corporation (NACC) examiner	Permanent*	18 U.S.C. 1908
Committing treason against the United States	Permanent*	18 U.S.C. 2381
Inciting, assisting, or participating in any rebellion or insurrection against the United States	Permanent*	18 U.S.C. 2383

Knowingly and willfully advocating, abetting, advising, or teaching the overthrow of the United States Government or any political subdivision of the United States	5 years from the date of the conviction	18 U.S.C. 2385
Activities intended to impair the loyalty, morale, or discipline of the United States Armed Forces	5 years from the date of conviction	18 U.S.C. 2387
Conviction for any felony; dishonorable discharge from the Armed Forces; judged or adjudicated mentally incompetent as a result of a court hearing; renounced citizenship; illegally in United States.	Permanent* (only from any position involving a requirement to carry a firearm)	Title 7 of the Omnibus Crime Control and Safe Street Act of 1968 as amended by Title 3 of the 1968 Gun Control Act.

NOTE: Also includes unlawful user of marijuana, drugs (as defined in section 4731A of the Internal Revenue Code) or stimulants (as defined in the Food, Drug and Cosmetic Act), if the person on the job would be required to carry a firearm that was transported in interstate commerce.

Knowing and willful failure to register under section 3 of the Military Selective Service Act (50 U.S.C. App. 453)	Permanent: (only from positions in executive agencies)	5 U.S.C. 3328
--	--	---------------

NOTE: Applies to individuals born after December 31, 1959, who are or were required to register and who are not registered, or did not register before the requirement terminated or became inapplicable to the individual.

***Permanent debarment is subject to review 10 years after the effective date of the debarment action when such review is requested by the person debarred. In some cases a Presidential directive may end the debarment period.**

APPENDIX E. INVESTIGATING CHILD CARE SERVICES WORKERS

1. General. This appendix states policy and procedures for the Personnel Security Program as it relates to suitability checks on child care services workers. It applies to persons working in DOT/FAA-sponsored child care centers as either employees or volunteers. Any person working in a DOT/FAA-sponsored child care services center or who provides child care services to persons under the age of 18 as part of any DOT/FAA-sponsored activity is subject to the requirements of this appendix.

2. Background.

a. 42 U.S.C. 13041 (originally Subtitle E of the Crime Control Act of 1990, Public Law 101-647), requires criminal history background checks on child care services workers either hired by or under contract to the Federal Government. In accordance with General Services Administration (GSA) guidelines, the DOT Child Care Handbook states that suitability checks will be conducted on all child care center workers and must include criminal records and background checks.

b. 42 U.S.C. 13041 defines “child care services” as including, but not limited to, child (day) care, recreational programs, health and mental health care, social services, education, foster care, residential care, treatment services, and child protective services. The provisions of this law apply to services that an agency provides to children under the age of 18.

3. Policy and Procedures. The following policy and procedures implement DOT policy within the FAA:

a. Any applicant for work in a DOT/FAA-sponsored child care center is subject to a Child Care National Agency Check and Inquiries (CNACI) investigation.

b. Human Resource Management Divisions (Personnel) and servicing security elements (SSE) must coordinate with each other to ensure that before allowing an applicant to work in a DOT/FAA child care center, either as an employee or as a volunteer, he or she completes an SF-85P, and Form FD-258, Fingerprint Card, or SF-87, if applicable. SSEs should make arrangements for applicants to get fingerprinted at an FAA facility whenever possible. If not available through FAA, an applicant may be fingerprinted by a law enforcement officer.

c. Upon receipt of the SF-85P, a personnel security specialist (PSS) who is trained to conduct personnel security interviews will review the forms and interview the applicant. They must ask the applicant if he or she has ever been arrested for, or charged with a sex crime; an offense involving a child victim; or a drug felony. Under 42 U.S.C. 13041(c), an applicant or employee will be denied employment or dismissed from a child care services position if he or she was convicted for any of these offenses.

d. The PSS must attempt to obtain the results of any prior personnel security investigation that was completed within the past 5 years, and apply the requirements of chapter 5, section 3, paragraph 3 of this order.

e. The PSS must inform the regional, center, or headquarters child care coordinator, who is normally located in the Personnel office, whenever the interview or review of the SF-85P reveals unfavorable information. The coordinator must inform the applicable board of directors and the director of the applicable child care center, that the applicant cannot begin working in the facility until the CNACI has been completed and favorably adjudicated. Unfavorable information in this instance means an arrest for one of the offenses specified above or other information that raises a significant issue that can eventually result in the FAA directing that the applicant not work in the child care center.

f. The PSS must notify the regional, center, or headquarters child care coordinator when the interview and review of the SF-85P reveals no derogatory information. The coordinator will notify the board of directors and the child care center director, that the applicant can begin working in the facility, under continuous supervision, pending completion of the CNACI. The director of the child care center must ensure that until the CNACI has been completed and favorably adjudicated, the child care worker is not left alone with children at the center.

g. The PSS must initiate the CNACI through the Office of Personnel Management (OPM). The Personnel Security Division, AIN-400, will budget for the cost of these investigations and provide each SSE with the appropriate accounting code.

h. OPM will provide all investigation results to the SSE for adjudication. As stated in chapter 7 and the PSS Supplement, when the PSS adjudicates investigations for child care workers, they must apply the same standard and criteria that they apply when adjudicating investigations on FAA applicants and employees,.

i. The PSS must assess all information of record, both favorable and unfavorable, for its relevance, recentness, and seriousness and provide fair, impartial, and equitable treatment for all child care service workers.

(1) Of particular concern in adjudications is any conduct or pattern of behavior indicating that a person's employment or volunteer work providing child care services might place children in jeopardy.

(2) Examples of specific conduct, actions, or convictions that will be considered as a basis for an unfavorable suitability determination include, but are not limited to, convincing evidence, with or without a conviction, of the crime of child molestation or abuse or neglect of a child or other dependent person entrusted to the person's care; negligence that has resulted in death or serious injury to a child or other dependent person; and a pattern of arrests or evidence of a single serious crime which raises questions about a person's suitability for the position.

(3) Of concern also is any action or pattern of behavior that might lessen the confidence of FAA personnel that an activity providing child care services is a safe, secure place for the care of their children.

j. Before making any unfavorable suitability determination, the PSS must provide the applicant or employee due process, which is an opportunity to respond to the information being considered as the basis for prohibiting the person from working at the child care center. They must interview the person, clearly explain the unfavorable information, and provide the individual the opportunity to respond. They must document the interview, including the information provided to the individual and the individual's response. The PSS must then consider any information the applicant or employee has provided before making a final suitability determination.

k. The PSS must notify the regional, center, or headquarters child care coordinator, who will notify the board of directors and the child care center director of the results of the suitability determination. In the event of an unfavorable suitability determination, the PSS must inform the coordinator in writing that the applicant or employee may not work at any DOT/FAA-sponsored child care center. The coordinator must then inform the board of directors and the child care center director in writing of the determination. The PSS must also notify the applicant or employee in writing when the suitability determination is unfavorable. Under no circumstances is the PSS to disclose to a private contractor or to an official of a private entity the specific reason(s) for any suitability determination.

l. FAA personnel responsible for arrangements for, oversight of, and liaison with DOT/FAA-sponsored child care centers must make sure that all agreements with private entities, such as agreements with boards of directors for use of FAA space for the centers, include adequate provisions and language to ensure compliance with the policies and procedures stated in this appendix.

m. All FAA employees are responsible for referring to their SSE any information about a person providing child care services as part of an DOT/FAA-sponsored activity that would raise a question about that person's suitability to continue to work with persons under the age of 18.

**APPENDIX F. DOT FORM 1631 – DISCLOSURE
AND AUTHORIZATION PERTAINING TO CONSUMER REPORTS
PURSUANT TO THE FAIR CREDIT REPORTING ACT**

UNITED STATES DEPARTMENT OF TRANSPORTATION
Disclosure and Authorization Pertaining to Consumer Reports
Pursuant to the Fair Credit Reporting Act

This is a release for the U.S. Department of Transportation to obtain one or more consumer/credit reports about you in connection with your application for employment or in the course of your employment with **the Federal Aviation Administration**.

One or more reports may be obtained for employment purposes, and used for evaluating your fitness for employment, promotion, reassignment, retention, or access to classified information.

I, _____, hereby authorize the U.S. Department of Transportation to obtain such report(s) from any consumer/credit reporting agency for employment purposes.

Signature

Date

Social Security Number

Current Organization Assigned

PRIVACY ACT STATEMENT

PURPOSE: The U.S. Government conducts background investigation and reinvestigations to establish that applicants or incumbents employed by the Government or working for Government under contract, are suitable for The Job. Information from this form is used primarily as the basis for this investigation. Complete this form only after a condition of employment has been made.

AUTHORITY: Depending upon the purpose of your investigation, the U.S. Government is authorized to ask for this information under Executive Order 10450, 10865, 1233, 12968: Sections 3301 and 9101 of Title 5, U.S. Code of Federal Regulations; sections 2165 and 2201 of Title 42, U.S. Code of Federal Regulations; sections 781 to 887 of Title 50, U.S. Code of Federal Regulations and part 5.732 and 736 of Title 5, Code of Federal Regulations. Your Social Security Number is needed to keep records accurate because other people may have the same name and birth date. Executive Order 9397 also asks Federal Agencies to use this number to help identify individuals in agency records.

VOLUNTARY NATURE OF DISCLOSURE: Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or security clearance prospects.

DISCLOSURE OF INFORMATION: The information you give us for the purpose of investigating you for employment or a security clearance, we will protect it from unauthorized disclosure. The collection, maintenance, and disclosure of background investigation information is governed by the Privacy Act. The U.S. Department of Transportation has published notices in the Federal Register describing the systems of records in which your records will be maintained. You may obtain copies of the relevant notices from the person who gave you this form. The information on this form and information we collect during an investigation may be disclosed without your consent by the Privacy Act (5 USC 552a(b)) and as follows:

1. To the Department of Justice when: a) the Agency or any component thereof; or b) any employee of the Agency in his or her official capacity, or c) any employee of the Agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or d) the U.S. Government, is a party to litigation or has interest in such litigation, and by careful review, the Agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records.
2. To a court or adjudicative body in a proceeding when: a) the Agency or any component thereof; or b) any employee of the Agency in his or her official capacity; or c) any employee of the Agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or d) the U.S. Government, is a party to litigation or has interest in such litigation, and by careful review, the Agency determines that the records are both relevant and necessary to the litigation and the use of such records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records.
3. When a record on its face, or in conjunction with other records, indicates a violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general stance, particular program stance, regulation, rule, or issued pursuant thereto, the relevant records may be disclosed to the appropriate Federal, foreign, State, local, tribal, or other public authority responsible for enforcement, investigating or prosecuting such violation or charged with enforcing or implementing the stance, rule, regulation, or order.
4. To any source or potential source from which information is requested in the course of an investigation concerning the hiring or retention of an employee or other personnel action, or the issuing or retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.
5. To a Federal, foreign, state, local, tribal, or other public authority the fact that this system of records contains information relevant to the retention of an employee, or the retention of a security clearance, contract, grant, license, or other benefits. The other Agency or licensing organization may then make a request supported by written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the Agency or to another Federal Agency for criminal, civil, administrative, personnel, or regulatory action.
6. To contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to this record for which they have been engaged. Such recipients shall be required to comply with the Privacy Act of 1974, as amended.
7. To the new media or general public, factual information the disclosures of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy.
8. To Federal, State or local Agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign Governments, in order to enable an intelligence Agency to carry out its responsibilities under the Nation Security Act of 1947, as amended, the CIA Act of 1949, as amended. Executive Order 12333 or any successor order, applicable to National Security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.
9. To a Member of Congress or a Congressional staff member in response to an inquiry of a Congressional office made at the written request of the constituent about whom the record is maintained.
10. To the National Archives and Records Administration for records management inspections conducted under 44 USC 2904 and 2906.
11. To the office of Management and Budget when necessary to the review of private relief legislation.

APPENDIX G. SECURITY BRIEFING GUIDANCE FOR ACCESS TO CLASSIFIED INFORMATION

Section 1. General

1. Briefing Responsibilities. Operating offices and servicing security elements (SSE) are responsible for ensuring that employees under their jurisdiction receive briefings and instructions with respect to their security responsibilities. Such briefings include those required prior to a person being granted access to classified national security information. section 2, paragraph 2 of this appendix, was prepared to aid offices in conducting these briefings. It is not to be taken as a substitute for review of the latest edition of FAA Order 1600.2, Classified National Security Information, and other FAA and DOT orders pertaining to the handling of classified information. It also includes items mentioned in the SF-312, Classified Information Nondisclosure Agreement. An employee can receive a security briefing either in written form, by video, verbally, etc.

2. Sample Briefing. Section 2 provides a sample briefing that contains important information that the SSE or operating office should provide to an employee when he or she is granted access to classified information. Anyone with questions concerning the use of this guidance should consult his or her SSE.

Section 2. Guidance for Protecting Classified Information

1. Responsibilities. Security is an individual responsibility. As the recipient of a security clearance, you are personally responsible for the classified information entrusted to your care. Your SSE can assist you in carrying out this responsibility, and you should feel free to ask them any questions you have about protecting classified information.

2. Classified Information: Definition and Types.

a. Classified information is national security information, defined as any information that has been determined by Executive Order or predecessor order to require protection against unauthorized disclosure in the interest of national security, and is so designated. All other information is considered unclassified.

b. There are three categories of classified information, briefly described as follows:

(1) **TOP SECRET:** Classified information that requires the highest degree of protection and the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security.

(2) **SECRET:** Classified information that requires a substantial degree of protection and the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security.

(3) **CONFIDENTIAL:** Classified information that requires protection and the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security.

c. Except as provided by statute, no other term can be used to identify classified information.

d. Only *information* can be classified. Classified information requires protection regardless of the medium by which it is presented; i.e., orally, in writing, in photographic form, or embodied in equipment or magnetic storage media.

e. Within the FAA, information can be originally classified only to the SECRET level, and then only by the Administrator, the Assistant Administrator for Security and Hazardous Materials, and, under emergency conditions, by regional administrators, and center directors.

f. TOP SECRET, NATO, Communications Security (COMSEC), Restricted Data, Sensitive Compartmented Information (SCI), and other special categories of information are subject to specialized controls with respect to access, distribution, and storage. Only specifically designated FAA offices and services have access to these types of information. If you receive or possess such information and you are not sure that your organization is specifically designated as authorized to have it, you must report the situation immediately to your SSE.

3. Assurances Needed Before Granting Access to Classified Information. Before you give anyone access to any classified information, you must:

a. Identify the person who desires access to the information and establish that he or she is cleared to the proper level. Personal recognition, by itself, isn't satisfactory because the person may not be in the position that once justified access to classified information and may no longer have a security clearance. The person's identification (ID) card only identifies the individual as a Government employee or contractor employee; it doesn't establish his or her security clearance status or *need to know*. You must have either your Personnel Security Coordinator or SSE confirm the person's security clearance status for you.

b. Establish the person's *need to know*. If you possess or control the classified information, you are responsible for establishing the *need to know* of someone to whom you disclose it. The person must justify his or her access based on official duty requirements or contractual obligations.

4. General Rules for Storing and Maintaining Classified Information. This paragraph deals with the storage and maintenance of classified information in written hard-copy form. FAA rarely generates classified information electronically. If a

situation arises where you must process, store, or maintain electronically-generated classified information, contact your respective SSE.

a. Store classified information only in GSA-approved containers (safes) with built-in, three-way combination locks. You aren't authorized to store it in other locked containers, including file cabinets that were modified with lock bars and combination padlocks.

b. Keep a safe locked when its custodian or other person authorized access to it isn't watching it continuously.

c. Use the OPEN/CLOSED sign and safe check record (SF-702, Security Container Check Sheet) each time the safe is opened or closed. If possible, someone who isn't involved in the locking of the safe should double-check it at the close of business each day to make sure it is locked, and fill in the "checked by" column of the SF-702. Otherwise, the person who locked it can also double-check it. To reduce the possibility of the safe being left unlocked, it must be double-checked each day, whether or not anyone opens it.

d. Change the safe combination at least once each year or when: (1) a person who knows the combination transfers or leaves employment; (2) there is reason to believe that an unauthorized person may have learned the combination; or (3) the safe is to be used to store material of a higher classification than the clearance level of a person who knows the current combination.

e. *Memorize the combination.* The combination has the same classification as the contents of the safe. If you write out the combination and hide it somewhere, you are violating security directives by storing classified information improperly.

f. Make sure that all classified material is returned to the safe each day.

g. Ensure that all classified information that is electronically processed or viewed is done so on information technology equipment that is explicitly approved for handling classified information.

h. Ensure that all classified information at the SECRET level and above is controlled through your facility control point. All classified messages and documents, including file and grid copies, must be accounted for when they are received or created, and returned to the Security Control Point for destruction when there is no longer a need to keep them.

i. A document control station with a custodian and alternate must be established, if your facility has a large volume of classified information. Only these persons are authorized to receive classified material from the Security Control Point. The custodian must maintain control records that show the document's control number, date,

identification, and location or disposition. Therefore, make sure that the custodian is aware of all classified document transactions.

j. Obtain a receipt for all documents classified at the SECRET level and above. When you are issued such a document, sign the original DOT F-1600.4, Classified Material Record, which the Security Control Point keeps. You will receive a copy of the form that you must file with the document in your office. Whenever you return the document to the Security Control Point for transfer or destruction, bring that copy with you.

k. Whenever you return a document to the Security Control Point, make sure that you obtain the original receipt. Doing so clears you of any further responsibility for the document.

l. Whenever you transfer a document classified SECRET or above to another office within your facility, route it through the Security Control Point for accountability.

m. Whenever you want to transmit any classified document to a location outside your facility, regardless of the document's classification level, route it through your Security Control Point. If you are going to carry the document yourself, you must possess a courier letter approved by either your regional or center SSE, or the Internal Security Division, AIN-100. The Security Control Point will make sure that it is properly wrapped and advise you of all necessary procedures.

n. You don't need a receipt for CONFIDENTIAL material. However, you must take CONFIDENTIAL documents to the Security Control Point for destruction or for transfer outside your facility.

o. Apply classification markings at the highest level to file folders, binders, envelopes, etc., containing classified documents. Apply the marking to the top and bottom of each side and to the labeled portion of file folders. Change the markings as necessary to show the current classification of the contents.

p. Whenever a classified document is out of the safe, place the appropriate cover sheet (CONFIDENTIAL, SECRET, or TOP SECRET) on it. Doing so will remind you that the document is classified and help prevent unauthorized persons from reading it.

q. Don't copy classified information unless the Security Control Point specifically authorizes you to do so. Normally, the Security Control Point will copy it for you, using equipment that is approved for the reproduction of classified information.

r. Don't destroy any classified information. Take it to the Security Control Point for destruction, along with classified waste such as typewriter or printer ribbons, notes, and mistyped pages. These items must be sealed in red striped bags and marked with your office routing symbol and date. While in your office, they must be kept in the safe to protect them in the same manner as any classified document.

5. Miscellaneous.

a. Don't discuss classified information on an unsecured telephone or where unauthorized persons might overhear it.

b. Before visiting a location where you will require access to classified information, make sure that your office processes DOT Form 1630.5, Department of Transportation Visit Clearance, through your SSE (see chapter 9, paragraph 10 of this order). This form will transmit your security clearance information to the agency or company you are going to visit.

c. Report losses, unauthorized disclosures, and possible compromises of classified information to your SSE.

d. If a visitor expresses an unusual interest in information he or she is not authorized to receive, report the situation to your SSE.