ORDER

1600.1D

AJA TAC
DOCUMENT MANAGEMENT
CENTER

PERSONNEL SECURITY PROGRAM

February 5, 1998

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

Initiated By: ACP-300

Distribution: A-WXYZE-2; A-FOF-0 (Ltd)

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.

Jane F. Garvey
Administrator

TABLE OF CONTENTS

Page No.

CHAPTER 1. INTRODUCTION 1

1. PURPOSE 1
2. DISTRIBUTION 1
3. CANCELLATION 1
4. EXPLANATIONS OF CHANGES 2
5. FORMS 3
6. REFERENCES TO DAYS 3
7. AUTHORITY TO CHANGE THIS ORDER 3
8. OBJECTIVES 3
9. EXCEPTIONS TO REQUIREMENTS AND STANDARDS 3
10. SCOPE 3
11.-199. RESERVED

CHAPTER 2. GENERAL 11

200. RESPONSIBILITIES 11
201. PERSONNEL SECURITY POLICIES 14
202. SAFEGUARDING RIGHTS AND PRIVACY OF APPLICANTS AND EMPLOYEES 15
203. DEFINITIONS 16
204.-299. RESERVED 16

CHAPTER 3. PERSONNEL SECURITY OPERATIONS, RESPONSIBILITIES, AND RECORDS 21

300. GENERAL 21
301. STANDARDS OF OPERATION 21
302. PERSONNEL SECURITY OPERATIONAL RESPONSIBILITIES 21
303. INITIATING, MONITORING, AND CLOSING INVESTIGATIONS 26
304. ADDITIONAL SSE INVESTIGATION 30
305. PERSONNEL SECURITY RECORDS 31
306. VISIT CLEARANCE REQUESTS 38
307.-399. RESERVED 39

CHAPTER 4. PERSONNEL SUITABILITY/SECURITY STANDARDS AND CRITERIA 41

400. RELATIONSHIP BETWEEN SUITABILITY AND SECURITY 41
401. PERSONNEL SUITABILITY STANDARD AND CRITERIA 42
402. PERSONNEL SECURITY STANDARD AND CRITERIA 44
403. COORDINATING PERSONNEL SECURITY INFORMATION 47
404.-499. RESERVED 47

CHAPTER 5. POSITION SENSITIVITY AND RISK LEVEL DESIGNATION AND CONTROL 51

500. POSITION SENSITIVITY AND RISK LEVEL DESIGNATION 51
501. RESPONSIBILITY FOR POSITION SENSITIVITY AND RISK LEVEL DESIGNATIONS 51

502. RISK LEVELS 52
503. SENSITIVITY LEVELS 52
504. POSITION SENSITIVITY AND RISK LEVEL DESIGNATION PROCESS 53
505. OFFICIAL RECORD OF POSITION RISK AND SENSITIVITY DESIGNATION 53
506. CODING OF POSITION RISK AND SENSITIVITY LEVELS ON PERSONNEL DOCUMENTS 54
507.-599. RESERVED 54

CHAPTER 6. PERSONNEL INVESTIGATION REQUIREMENTS 61

600. GENERAL 61
601. TYPES AND SCOPE OF BACKGROUND INVESTIGATIONS 61
602. BASIC INVESTIGATIVE REQUIREMENTS 63
603. SPECIFIC REQUIREMENTS: SPECIAL-SENSITIVE POSITIONS 68
604. SPECIFIC REQUIREMENTS: CRITICAL-SENSITIVE POSITIONS 69
605. SPECIFIC REQUIREMENTS: NONCRITICAL-SENSITIVE POSITIONS 71
606. SPECIFIC REQUIREMENTS: HIGH-RISK POSITIONS 72
607. SPECIFIC REQUIREMENTS: MODERATE-RISK POSITIONS 73
608. SPECIFIC REQUIREMENTS: LOW-RISK POSITIONS 74
609. SPECIFIC REQUIREMENTS FOR CERTAIN POSITIONS 75
610. EXCEPTIONS TO INVESTIGATIVE REQUIREMENTS 75
611. WAIVER OF PREPLACEMENT INVESTIGATIVE REQUIREMENTS 77
612. SPECIAL PROCEDURES FOR ACCELERATED HIRING 83
613.-699. RESERVED 85

CHAPTER 7. STANDARDS AND PROCEDURES FOR USING PREVIOUS INVESTIGATIONS 91

700. GENERAL 91
701. OBTAINING AND REVIEWING PREVIOUS INVESTIGATIONS 92
702. SAMPLE LETTER FOR DCII CHECKS 95
703.-799. RESERVED 95

CHAPTER 8. SUITABILITY ADJUDICATION 101

800. GENERAL 101
801. ADJUDICATION RESPONSIBILITIES 101
802. ADJUDICATION REFERRAL 101
803. INVESTIGATIONS, PROCESSING, AND SUITABILITY/SECURITY ADJUDICATION 103
804. SUITABILITY ADJUDICATION PROCESS 105
805. DOCUMENTATION AND NOTIFICATION 106
806.-899. RESERVED 108

CHAPTER 9. SECURITY ADJUDICATION 121

900. GENERAL 121
901. RESPONSIBILITY FOR SECURITY ADJUDICATIONS 121
902. CASE ADJUDICATION PROCEDURES 122

903. TIIMELINESS OF ADJUDICATIONS 123
904. RECORDS TO BE MAINTAINED 123
905.-999. RESERVED 124

CHAPTER 10. ACCESS AUTHORIZATIONS 131

1000. GENERAL 131
1001. REQUEST PROCEDURES 131
1002. INTERIM CLEARANCES 132
1003. FINAL CLEARANCES 135
1004. TEMPORARY CLEARANCES 135
1005. CLEARANCE GRANTING PROCEDURES AND DOCUMENTATION 136
1006. TERMINATING ACCESS AUTHORIZATIONS 138
1007. SPECIAL ACCESS AUTHORIZATIONS 140
1008.-1099. RESERVED 140

CHAPTER 11. ADVERSE SECURITY ACTIONS 147

1100. GENERAL 147
1101. PRELIMINARY ACTIONS 147
1102. SECURITY CLEARANCE DENIAL, SUSPENSION, AND/OR REVOCATION 147
1103. EMPLOYMENT OF INDIVIDUALS PREVIOUSLY SEPARATED FOR SECURITY REASONS 150
1104.-1199. RESERVED 150

CHAPTER 12. ACCESS TO AUTOMATED INFORMATION SYSTEMS 161

1200. GENERAL 161
1201. ACCESS REQUIREMENTS 162
1202. PROCEDURES 163
1203.-1299. RESERVED 164

CHAPTER 13. FOREIGN ASSIGNMENTS AND TRAVEL 171

1300. GENERAL 171
1301. INVESTIGATIVE REQUIREMENTS 171
1302.-1399. RESERVED 174

CHAPTER 14. SECURITY CLEARANCES AND AUTHORIZATIONS FOR ALIENS 181

1400. GENERAL 181
1401. INVESTIGATIVE REQUIREMENTS FOR ALIENS 181
1402. PROCEDURES FOR LIMITED ACCESS AUTHORIZATIONS 181
1403. PROCEDURES FOR IMMIGRANT ALIEN SECURITY CLEARANCES 182
1404. APPROVAL FOR VISITS BY FOREIGN NATIONALS CLEARED BY OTHER AGENCIES 183
1405.-1499. RESERVED 183

CHAPTER 15. NATIONAL EMERGENCY PERSONNEL SECURITY PROCEDURES 191

1500. PURPOSE 191
1501. ACTIVATION OF STANDBY PROCEDURES 191
1502. STANDBY PROCEDURES: MODIFICATION OF INVESTIGATIVE REQUIREMENTS 191
1503. REQUIRED PLANS FOR PERSONNEL SECURITY OPERATIONS DURING A NATIONAL EMERGENCY 193
1504.-1599. RESERVED 193

APPENDIX 1. GLOSSARY (6 PAGES) 1

APPENDIX 2. PERSONNEL SECURITY COORDINATOR RESPONSIBILITIES (2 PAGES) 1

APPENDIX 3. POSITION RISK AND SENSITIVITY LEVEL DESIGNATION PROCESS (18 PAGES) 1

APPENDIX 4. PERSONNEL SECURITY FORMS (2 PAGES) 1

APPENDIX 5. FORMS REQUIRED FOR INVESTIGATIONS (5 PAGES) 1

APPENDIX 6. SUITABILITY ADJUDICATION PROCEDURES (14 PAGES) 1

APPENDIX 7. STATUTORY DEBARMENT ISSUES (3 PAGES) 1

APPENDIX 8. SECURITY BRIEFING GUIDANCE FOR ACCESS TO CLASSIFIED INFORMATION (6 PAGES) 1

APPENDIX 9. INVESTIGATING CONTRACTOR EMPLOYEES (14 PAGES) 1

APPENDIX 10. NATIONAL INDUSTRIAL SECURITY PROGRAM (3 PAGES) 1

APPENDIX 11. INVESTIGATING CHILD CARE CENTER WORKERS (3 PAGES) 1

APPENDIX 12. SECURITY ADJUDICATION GUIDELINES (17 PAGES) 1

CHAPTER 1. INTRODUCTION

1. PURPOSE. This order states personnel security policy in accordance with Order DOT 1630.2, Personnel Security Handbook, and establishes for the Federal Aviation Administration (FAA) related standards, criteria, and procedures which are consistent with applicable laws, Executive Orders (E.O.), and Governmentwide regulations governing the personnel security program.

2. DISTRIBUTION. This order is distributed to the branch level in headquarters, regions, and centers, with a limited distribution to all field offices and facilities.

3. CANCELLATION. Orders 1600.1C, Personnel Security Program, dated September 19, 1989; 1600.56, Guidelines for FAA Participation in the Department of Defense (DOD) Industrial Security Program (ISP), dated August 15, 1977; and 1600.43, Federal Bureau of Investigation Information, dated July 19, 1973, are canceled.

4. EXPLANATION OF CHANGES. This order:

a. Updates personnel security policy and procedures to conform to the FAA's Personnel Management System established April 1, 1996, and to changes in Office of Personnel Management (OPM) and DOT policy and procedures. These changes include:

(1) A new definition of suitability (chapter 4).

(2) A requirement to designate as public trust positions those positions that were previously sensitive but which have no national security responsibilities (chapter 5).

(3) New investigative requirements, including the Single Scope Background Investigation, for persons needing Top Secret clearances or access to Sensitive Compartmented Information (chapter 6).

(4) Delegation to servicing security elements the authority to grant waivers of preplacement investigative requirements for noncritical-sensitive and moderate-risk positions (paragraph 611).

(5) A requirement to place the Standard Form 312, Classified Information Nondisclosure Agreement, in an employee's official personnel folder (paragraph 1005).

b. Provides more specific guidance for designating position risk levels, especially for positions common in more than one region; and for risk level designation of automated information security (AIS) positions (appendix 3).

c. Clarifies suitability adjudication procedures and more clearly specifies security and human resource management responsibilities (chapter 8).

d. Incorporates policy and procedures for implementing the National Industrial Security Program previously contained in Order 1600.56 (appendix 10).

e. Adds policy and procedures for conducting suitability checks on persons working in FAA-sponsored child care centers (appendix 11).

f. Implements provisions of E.O. 12968, Access to Classified Information, which establishes a uniform Federal personnel security program for persons considered for initial or continued access to classified information (chapters 4 and 11).

g. Elevates initial responsibility for security clearance denials and revocations to the Director of Civil Aviation Security Operations and specifies procedures for appealing these actions to a Department of Transportation (DOT) panel (chapter 11).

h. Adds more specific procedures for authorizing access to AIS positions (chapter 12).

i. Adds more specific adjudicative guidelines for determining eligibility for access to classified information (appendix 12).

5. FORMS. Refer to Appendix 4, Personnel Security Forms, for a listing of those 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 reserves the authority to approve changes which establish or revise policy, delegate authority, or assign responsibility. The Associate Administrator for Civil Aviation Security may issue changes to this order as necessary to implement and manage the personnel security program. Changes shall be coordinated with the Office of Security and Administrative Management (M-70), Office of the Secretary of Transportation (OST).

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 to safeguard the national security. These objectives shall be achieved through the consistent application of personnel security standards, criteria, and procedures prescribed in E.O. 10450, Security Requirements for Government Employment; E.O. 12968; and, as applicable, Title 5, Code of Federal Regulations (CFR), Parts 732, National Security Positions, and 736, Personnel Investigations. The objectives shall also be achieved by affording fair, impartial, and equitable treatment to all individuals seeking employment with or who are employed by the FAA.

9. EXCEPTIONS TO REQUIREMENTS AND STANDARDS. Exceptions to the requirements and standards stated in this order, to include region and center supplements to it, shall have the specific prior approval of the Associate Administrator for Civil Aviation Security.

10. SCOPE. The provisions of this order apply to all employees of the FAA; to those individuals associated with FAA directly or through classified and unclassified contracts as described in Appendix 9, Investigating Contractor Employees, and Appendix 10, National Industrial Security Program; and to persons working in FAA-sponsored child care centers as described in Appendix 11, Investigating Child Care Center Workers.

11.-199. RESERVED.

CHAPTER 2. GENERAL

200. 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 individuals' employment and continued employment within the FAA will promote the efficiency of the service and will be consistent with national security interests.

b. Associate Administrator for Civil Aviation Security (ACS-1). ACS-1 has the primary responsibility for implementing the FAA's personnel security program and shall provide general direction for the program throughout the FAA and ensure that resources needed for conducting an effective program are available and are efficiently used.

c. Director of Civil Aviation Security Policy and Planning (ACP-1). ACP-1 is responsible for promulgating personnel security standards and guidelines which shall be applicable throughout the FAA.

d. Director of Civil Aviation Security Operations (ACO-1). ACO-1 is responsible for personnel security program operations and direct program implementation in the regions, centers, and headquarters; and, in coordination with ACP-1, for appraising the effectiveness and efficiency of the program at the headquarters and field levels.

e. Directors of Offices and Services. Directors of offices and services are responsible for ensuring that their subordinates understand and comply with personnel security program requirements.

f. Regional Administrators and Center Directors. Administrators/directors are responsible for ensuring implementation of and compliance with this directive in their respective regions and centers.

g. Managers of Servicing Security Elements (SSE). Under the direction of ACO-1, the managers of the Investigations Division (ACO-300), the regional and

Aeronautical Center's Civil Aviation Security Divisions, and the Technical Center's Civil Aviation Security Staff are responsible for:

(1) Implementing and maintaining an effective personnel security program within their areas of responsibility.

(2) Designating a personnel security officer.

(3) Ensuring compliance with personnel security/suitability investigative requirements.

(4) Assisting Human Resource Management Divisions (HRMD) in suitability adjudication.

(5) Ensuring that appropriate training is provided for designating position risk and sensitivity levels, and for security and suitability adjudication.

(6) Ensuring that position risk and sensitivity levels are properly determined.

(7) Adjudicating security issues, granting security clearances, and, as necessary, recommending revocation and denial of security clearances to ACO-1.

(8) Evaluating the effectiveness of the personnel security program.

h. Managers of Human Resource Management Divisions. HRMD managers are responsible for:

(1) Working with operating offices to obtain and submit paperwork for required personnel security/suitability investigations.

(2) Obtaining authorization from SSE's prior to processing personnel actions which will place persons in public trust and sensitive positions.

(3) Ensuring that manual and automated master position description records accurately reflect approved position risk and sensitivity designations.

(4) In coordination with SSE's, adjudicating suitability issues.

(5) Advising management officials regarding adverse actions contemplated against employees.

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

(1) Ensuring full understanding of and compliance with personnel security standards, criteria, and procedures by individuals under their jurisdiction, thus appropriately protecting the interests of national security, the FAA, and the individual, and promoting the efficiency of the service.

(2) Obtaining authorization from SSE's prior to processing personnel actions which will place persons in public trust and sensitive positions.

(3) Identifying and reporting to the SSE any significant deviation from personnel security standards, criteria, or procedures.

(4) Sharing responsibility with the appointing and/or approving official for ensuring completion of the required forms for personnel security investigations.

j. Employees.

(1) Employees are responsible for familiarizing themselves with pertinent security regulations which pertain to their assigned duties. Employees must also be aware of the standards of conduct required for persons holding positions of trust. Individuals must therefore recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. Employees are ultimately responsible for maintaining continued eligibility for such positions.

(2) As required by E.O. 12968, all employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security. Employees should report such information to their SSE.

k. Contracting Offices. Contracting offices are responsible for ensuring that contractors and contractor employees who have comparable exposure to FAA's facilities, sensitive information, and/or resources or who require access to classified information are subject to the investigative requirements prescribed by this order.

201. PERSONNEL SECURITY POLICIES. Personnel security policies applicable throughout the FAA are as follows:

a. No person shall be employed or retained in employment unless a determination has been made on behalf of the Administrator that the person's employment will promote the efficiency of the service.

b. No person shall be employed or retained in employment unless a determination has been made on behalf of the Secretary of Transportation that such employment is clearly consistent with the interests of national security.

c. Appropriate background investigations shall be conducted on all persons employed by FAA. These investigations shall serve as the basis for a suitability adjudication and a security determination.

d. The FAA shall afford fair, impartial, and equitable treatment to all FAA employees and applicants through the consistent application of personnel security standards, criteria, and procedures as specified in applicable laws, regulations, and orders.

e. Applicants, employees, and contractor personnel shall be accorded all applicable legal rights to explain or refute derogatory information that is the basis for any adverse personnel or similar action taken against them.

f. No person whom the Secretary of Transportation has removed from employment for security reasons shall be employed by the FAA without the Secretary's prior approval.

g. Investigative records and personnel security files may be disclosed only to the extent necessary under the requirements of the latest editions of Order 1200.23, Public

Availability of Information; and Order 1280.1, Protecting Privacy of Information About Individuals.

202. SAFEGUARDING RIGHTS AND PRIVACY OF APPLICANTS AND EMPLOYEES. The procedures listed below shall be followed and implemented in accordance with Orders 1200.23 and 1280.1:

a. Applicants and employees shall be afforded an opportunity to explain, refute, or deny any derogatory information obtained as the result of an investigation before the FAA may take any unfavorable action based on that information, including denial of a benefit to which an individual would otherwise be entitled. The individual has the right to make an oral or written reply. This practice, commonly known as due process, prevents errors which might otherwise result from mistakes in identity or erroneous information and provides the applicant or employee the opportunity to present mitigating information which may be unknown to the adjudicating officials. The applicant or employee must be provided the appropriate Privacy Act advisements as specified in the latest edition of Order 1600.20, Civil Aviation Security Investigations Handbook. Any record of the derogatory information, to include the applicant's or employee's response to it, may be furnished only to those individuals who, in their official capacity, have a need to know such information.

b. Investigative information obtained under a pledge of confidence shall be controlled in accordance with the commitment the investigating agency made to the source of that information.

c. Medical information of a sensitive, personal nature that is obtained in conjunction with an investigation shall be carefully controlled to ensure that it is not disclosed to individuals who do not need it for official purposes. It also shall not be used 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.

d. The SSE shall ensure that before releasing investigative information to anyone outside the security element, the persons to whom the information is being

disclosed have a need to know it in an official capacity and in order to carry out a responsibility prescribed by this order. All persons receiving investigative information shall similarly ensure that it is disclosed only to persons who have a need to know it in an official capacity. All individuals reviewing the investigative information shall be required to sign FAA Form 1600-12, Investigative Record Review.

e. All personnel security files, reports of personnel investigations, personal history statements, records of response to derogatory information, computerized personnel security data, and other personnel security records and documents shall be regarded as Privacy Act information. During handling, transmission, release, and storage, they shall be carefully protected in accordance with the procedures specified in Order 1280.1.

f. Offices receiving Freedom of Information Act requests for the types of records mentioned in paragraph e shall apply Privacy Act considerations in accordance with all procedural requirements listed in the latest editions of Orders 1200.23 and 1280.1.

203. DEFINITIONS. With respect to the FAA's personnel security program, the definitions in Appendix 1, Glossary, shall apply.

204.-299. RESERVED.

CHAPTER 3. PERSONNEL SECURITY OPERATIONS, RESPONSIBILITIES, AND RECORDS

300. GENERAL. This chapter prescribes FAA standards and responsibilities for conducting personnel security operations and for maintaining personnel security records.

301. STANDARDS OF OPERATION. FAA personnel security operations shall meet the following standards:

a. The operations shall be conducted at organizational levels where they are closely controlled to ensure that they comply with FAA requirements, are managed in an efficient and effective manner, and furnish all program information which the Office of the Secretary (OST), DOT, requires.

b. In servicing security elements (SSE), only professionally qualified personnel security officers shall direct personnel security operations. SSE managers and Human Resource Management Division (HRMD) managers may delegate responsibility for security and suitability adjudication, but may do so only to specialists who are fully trained to evaluate reports and results of personnel investigations and who have successfully completed the Office of Personnel Management's (OPM) security and suitability adjudication course, or an equivalent course, prior to being authorized to adjudicate cases.

c. When an operating office delegates program authority to field offices, the SSE shall maintain close controls, conduct periodic evaluations as necessary, and closely monitor the program operations.

302. PERSONNEL SECURITY OPERATIONAL RESPONSIBILITIES. Personnel security officers have primary responsibility for personnel security operations. However, HRMD and operating office officials shall assist them by performing certain personnel security operational duties. Paragraph 200 contains basic responsibilities for SSE's, HRMD's, and operating offices. The following paragraphs state more specific responsibilities for these organizations.

a. Servicing Security Element (SSE). The SSE shall:

(1) Designate in writing a personnel security officer. The personnel security officer shall implement the FAA personnel security program within his or her area of responsibility.

(2) Ensure that position sensitivity and risk level designations are accurate for all positions within its 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 preplacement investigative requirements as specified in paragraph 611. Conduct local agency and other checks as necessary.

(6) Receive from OPM or other sources results of all investigations on applicants and employees. 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 paragraph 202a.

(9) Make security determinations on all sensitive cases and grant or deny access to classified information; i.e., security clearances. Advise HRMD's of these determinations.

(10) Participate with the HRMD and/or operating offices in adjudicating suitability on applicants or employees.

(11) Prepare and conduct, or ensure that operating offices conduct, security briefings for employees as needed.

(12) Provide guidance to the HRMD and operating offices on personnel security policies and operating procedures.

(13) Periodically evaluate the personnel security program in its area of responsibility to ensure that it is operating effectively and efficiently.

(14) Process visit clearance requests and certify security clearances as necessary.

(15) Advise operating offices and HRMD's of all changes in costs of background investigations.

b. Operating office. The operating office shall:

(1) Designate a personnel security coordinator to perform tasks listed in Appendix 2, Guidelines for Personnel Security Coordinators, and notify the SSE whenever a new coordinator is designated.

(2) Recommend position sensitivity and risk level designations on positions under its jurisdiction. On all newly established or revised positions, coordinate with the SSE prior to submitting a Standard Form (SF) 52, Request for Personnel Action, to designate the sensitivity or risk level in accordance with Chapter 5, Position Sensitivity and Risk Level Designation and Controls, and Appendix 3, Position Risk and Sensitivity Level Designation Process.

(3) Ensure that all Optional Form 8's (OF-8), Position Description, or electronic equivalent, 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) When appropriate, ensure that vacancy announcements state that appointment is subject to a favorably adjudicated personnel security investigation enabling the granting of a security clearance.

(5) Obtain approval from the SSE before placing, or making any commitment to place, a person in a special-sensitive, critical-sensitive, noncritical-sensitive, or high-risk or moderate-risk position.

(6) Request waivers of preplacement investigative requirements when emergency conditions exist which preclude the ability to meet these requirements.

(7) Budget for the costs of conducting personnel investigations, or coordinate with the SSE to ensure budgeting for these costs.

(8) Obtain or assist HRMD's in obtaining personnel security questionnaires, fingerprints, and other forms as required for personnel security processing. Appendix 5, Forms Required for Investigations, identifies the forms required to initiate specific investigations. Ensure that paperwork is properly completed and submitted in time to initiate investigations as required by Chapter 6, Personnel Investigation Requirements, and paragraph 303.

(9) Conduct or arrange for security briefings for new employees and employees with newly granted security clearances. Periodically conduct additional briefings to maintain a high level of security awareness.

(10) Advise the SSE of any questionable conduct or activity by an employee which would raise a security or suitability issue.

(11) Maintain records of the risk and sensitivity levels of its organization's positions.

(12) Maintain records of the security clearances held by its organization's employees. Maintain records as prescribed by the latest edition of Order 1280.1, Protecting Privacy of Information About Individuals.

c. Human Resource Management Division (HRMD). The HRMD shall:

(1) Coordinate with the SSE on each new or revised position description to ensure that the original

OF-8 or electronic 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 which are a condition of employment in the position.

(3) Obtain or participate with operating offices in obtaining personnel security questionnaires, fingerprints, and other forms as required for personnel security processing. Appendix 5, Forms Required for Investigations, identifies the forms required to initiate specific investigations. Ensure that paperwork is properly completed and submitted in time to initiate investigations as required by Chapter 6, Personnel Investigation Requirements, and paragraph 303.

(4) When an applicant is a current or former Federal employee, obtain available Official Personnel Folder (OPF) data about previous investigation(s). Provide this information to the SSE when the person is applying for other than a low-risk position, and advise the SSE whenever the OPF contains no conclusive proof of a prior investigation.

(5) Coordinate with the SSE any information about an applicant which would raise a security or suitability issue. This includes information disclosed on an employment application or personnel security questionnaire, or from preplacement inquiries, prior employers, the OPF, or any other sources.

(6) Refer to the SSE any information about an employee which would raise a security or suitability issue.

(7) Obtain approval from the SSE before placing any person in a special-sensitive, critical-sensitive, noncritical-sensitive, or high-risk or moderate-risk position.

(8) Retain personnel security documents in the OPF as specified in paragraph 1005a.

(9) Enter into the Integrated Personnel and Payroll System (IPPS) the sensitivity or risk-level designation for each new position.

(10) Adjudicate suitability, as required, on all cases with significant adverse information, coordinating with the SSE and appropriate operating officials.

303. INITIATING, MONITORING, AND CLOSING INVESTIGATIONS. SSE's are responsible for ensuring that all requests for investigations are submitted to OPM as required by Chapter 6, Personnel Investigation Requirements, and this paragraph. HRMD's are responsible for obtaining, or working with operating offices to obtain, all completed forms from applicants and appointees that the FAA must submit to request OPM to conduct the investigations. Appendix 5, Forms Required for Investigations, specifies the forms to be submitted for each type of investigation. SSE's will normally submit requests for investigation to OPM, but HRMD's or operating offices may submit them for persons in low-risk positions if headquarters, regional, or center procedures specify that they will do so. SSE's, HRMD's, and operating offices shall work together to ensure that the necessary investigations are requested as required.

a. New hires and reassignments.

(1) The HRMD and the operating office shall ensure that the applicant or employee properly completes all necessary personnel security forms, and shall submit them to the SSE in time to allow for processing to OPM as required by chapter 6. Both the HRMD and operating offices shall ensure that employees and applicants are not entered on duty into other than low-risk positions without SSE approval.

(2) The SSE shall review the personnel security forms for accuracy and completeness and for any possibility of a previously conducted investigation. It may return to the HRMD or operating office for correction any form which is incomplete. The HRMD or operating office shall then ensure that the applicant or employee makes the appropriate correction(s) and shall return the form to the SSE. When the person is an FAA employee, the operating office shall assist the HRMD and the SSE by ensuring that the employee

promptly completes, submits, and corrects, as necessary, all required personnel security forms.

(3) The SSE shall enter the required information on those portions of a personnel security questionnaire which an agency must complete and shall submit to OPM the forms necessary to initiate the investigation. Appendix 5 specifies the forms needed for each type of investigation. The SSE shall enter its OPM-assigned Security Office Identifier (SOI) on all personnel security questionnaires.

b. Investigations on employees due to upgraded risk or sensitivity level, need for access to classified information, or need for periodic reinvestigation.

(1) When the SSE notifies an operating office that an employee requires an investigation for one of these reasons, the operating office shall ensure that the employee completes all necessary personnel security forms and promptly submits them to the SSE. When a new investigation is required because the risk or sensitivity level has been upgraded, the employee shall submit the forms to the SSE within 12 days of the date on which the upgrade takes effect. When a Periodic Reinvestigation (PRI) or Periodic Reinvestigation for Single Scope Background Investigation (PRIS) is required, or the investigation is required before the SSE can grant access to a particular level of classified information, the employee shall submit the forms to the SSE within 14 days of the date on which the SSE requests them.

(2) The SSE shall review the personnel security forms for accuracy and completeness, and shall return to the employee any form which is incomplete. The employee shall promptly make any correction(s) necessary and return the form to the SSE. The operating office shall assist the SSE by ensuring that the employee promptly corrects and re-submits, as necessary, all required personnel security forms.

(3) The SSE shall enter the required information on those portions of a personnel security questionnaire which an agency must complete and shall submit to OPM the forms necessary to initiate the investigation. Appendix 5 specifies the forms needed for each type of investigation.

The SSE shall enter its SOI on all personnel security questionnaires except as provided by paragraph b(4) below.

(4) When it is necessary to initiate an investigation on an SSE manager, personnel security officer, or personnel security specialist, personnel other than the subject of the investigation shall process the necessary forms. The Investigations Division (ACO-300) shall assist regional and center SSE's upon request and shall initiate all investigations on SSE managers, using the ACO-300 SOI. SSE's shall take all reasonable steps to ensure that when reports of investigation on SSE personnel are received from OPM, they are not opened by or otherwise made accessible to the subjects of the investigations. SSE's may enter the ACO-300 SOI on questionnaires for personnel security officers and specialists to ensure proper control over completed reports. In no case shall the subject of an investigation be involved in its initiation or processing other than by furnishing the required forms and providing other requested information.

c. Distribution of SF-85, Questionnaire for Nonsensitive Positions; SF-85P, Questionnaire for Public Trust Positions; SF-85P-S, Supplemental Questionnaire for Selected Positions; and SF-86, Questionnaire for National Security Positions. The SSE shall send the original of the appropriate questionnaire to OPM and shall retain a copy in the personnel security file. It shall also make a copy of that portion of the first page which 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. Furnishing the accounting division only the Agency Use block and the employee's or applicant's name protects information on the rest of the form from disclosure to persons who have no need to know its contents.

d. Payment for investigations. Personnel security investigations, including fingerprint checks on contractor employees, are funded by each office or division through operational funds. Unless there has been a specific allotment to the SSE to pay for all investigations for operating offices it services, each operating office shall pay the costs for investigations on its employees and on applicants for its positions. The operating office responsible for payment shall provide the SSE with the

accounting code information necessary to have the cost charged appropriately. The SSE shall enter that information in the Agency Use Only block on the SF-85, SF-85P, or SF-86.

e. Submission to OPM. The SSE shall complete the entire package as outlined in appendix 5 and transmit it to OPM, FIPC, Boyers, Pennsylvania 16018. Any information that the FAA has developed from preliminary investigation or record searches concerning the person to be investigated must be forwarded to OPM with the request for investigation.

f. Discontinuing investigations.

(1) The SSE shall discontinue an investigation whenever it becomes clear that the investigation is no longer needed, as when an applicant is no longer being considered for employment or an employee leaves the FAA. If the person transfers to another DOT administration, the SSE shall coordinate with the Office of Security (M-70), OST, before doing so. The HRMD and operating offices shall immediately notify the SSE when they become aware that discontinuing an investigation is warranted.

(2) In discontinuing an investigation, the SSE shall telephonically advise OPM to do so and shall follow up with a written notification which shall include the reason for the discontinuance. The SSE shall also notify the servicing accounting office and shall advise that office of the expected charge for the incomplete investigation, if any. The SSE shall contact OPM, if necessary, to resolve any subsequent question as to the charge for an incomplete investigation.

g. Completion of investigations and documentation.

(1) OPM will send all reports of investigation to the SSE identified by the SOI code on the SF-85, SF-85P, or SF-86. The SSE shall review all reports and shall provide the applicant or employee with the opportunity to respond to unfavorable information, as required by paragraph 202a, whenever the reports raise issues which may warrant taking unfavorable action against the person investigated.

(2) With each completed investigation, OPM will send a certification of investigation. When the results

have been reviewed and all adjudication has been completed, an SSE official shall sign the certification and forward it to the HRMD, which shall then file it on the permanent side of the employee's OPF. If the investigation was conducted on an applicant who is not subsequently hired, the SSE shall retain the certification with the reports of investigation.

304. ADDITIONAL SSE INVESTIGATION. Following receipt of a completed report of investigation from OPM, it may be necessary for the SSE to conduct an additional investigation before the HRMD or the SSE can make a suitability or security determination.

a. Criteria for opening an investigation.

(1) The SSE shall open an investigation 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 SSE has determined that the subject of investigation is still an employee or under active consideration for employment.

(2) The SSE shall not open an investigation:

(a) Solely to conduct an interview with an employee or applicant, or to conduct brief, followup 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; i.e., 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.

(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. When it is necessary to open an investigation, the SSE will conduct it according to procedures in the latest edition of Order 1600.20, Civil Aviation Security Investigations Handbook. If an investigation is not necessary, the SSE may interview the subject in person or send a letter or memorandum to him/her to fulfill the due process requirements prescribed in paragraph 202a.

c. Documentation. If there is a need for substantial investigative work in addition to an interview with the employee or applicant, then all of the investigative results, including the interview, should be reported in a report of investigation (ROI). If there is no need for an investigation, then the SSE shall prepare a memorandum to the personnel security file to document the results of an interview. Any written statement from the subject shall also be included in the file. The SSE shall prepare a memorandum to the file to document the results of any additional checks conducted.

305. PERSONNEL SECURITY RECORDS.

a. Personnel security files (PSF).

(1) When required. SSE's shall establish PSF's for all employees in special-sensitive and critical-sensitive positions, and for employees in other positions when there are reports of investigation or other personnel security materials warranting retention. They shall also establish PSF's for applicants when investigations have been initiated or reports of investigation obtained. It is not necessary to maintain a PSF on every employee, although an SSE may retain in a folder under a person's name personnel security or other documents, such as those related to identification media, that it is required to keep. Documents such as FAA Form 1600-54, Notification of Personnel Security Action, and FAA Form 1600-25, Security Termination Statement, may also be kept in alphabetical order in separate files.

(2) PSF contents. When it is established, the PSF shall contain, as applicable:

(a) FAA Form 1600-54, Notification of Personnel Security Action.

(b) SF-85, Questionnaire for Nonsensitive Positions.

(c) SF-85P, Questionnaire for Public Trust Positions.

(d) SF-85P-S, Supplemental Questionnaire for Selected Positions.

(e) SF-86, Questionnaire for National Security Positions.

(f) FAA Form 1600-25, Security Termination Statement.

(g) Reports of investigation completed by OPM and other agencies. National Agency Check and Inquiries (NACI) reports containing only minor unfavorable information, or information so old as to be insignificant in any future suitability or security adjudications, as well as those NACI reports which contain no unfavorable information, may be destroyed. At its discretion, the SSE may maintain a summary of the minor unfavorable information or a note that the results contained no unfavorable information. Such notations may assist in future adjudications or in processing waiver requests when the NACI information is not immediately available from OPM.

(h) ROI's completed by FAA.

(i) A copy of the OPM case transmittal or other OPM form documenting final adjudicative action.

(j) Copies of all pertinent correspondence, including that to or from OPM, another Government agency, the operating office, the HRMD, or the applicant or employee.

(k) Appropriate forms or memoranda documenting temporary or interim security clearances.

(l) A record of all disclosures or reviews of information contained in the PSF by persons outside the SSE.

(3) Nonselected Applicants. SSE's shall retain all PSF's on nonselected applicants for a period of 1 year from the date of nonselection unless they contain FAA ROI's. In those cases, the PSF's shall be retained for 5 years.

(4) Transfer of PSF's.

(a) Forwarding to another SSE. When an employee transfers within FAA from the jurisdiction of one SSE to another, the losing SSE shall forward the PSF to the gaining SSE.

(b) Forwarding to another DOT administration. When an employee transfers to another DOT administration, the losing SSE shall forward the PSF to the Office of Security and Administrative Management, M-70.

b. Separated employees. When employees separate from FAA and do not transfer to another DOT administration, their PSF's and other personnel security records shall be retained and destroyed as follows:

(1) PSF's containing significant personnel security or suitability information shall be retained in accordance with the latest edition of Order 1350.15, Records Organization, Transfer, and Destruction Standards, except that the SSE's may transfer these files to the Federal Records Center after 1 year following termination of employment.

(2) PSF's not containing significant personnel security or suitability information and not containing an FAA ROI shall be retained for 30 days following termination of employment unless the employee:

(a) Is on military or other leave status;

(b) Is expected to be re-employed within 5 years; or

(c) Is known to be involved in administrative action or an appeal which may result in restoration to duty.

(3) PSF's containing an FAA ROI shall be retained for 5 years following termination of employment.

(4) Regardless of when PSF's may be destroyed, SSE's shall retain FAA Forms 1600-25 for at least 1 year following termination of employment.

(5) SSE's shall retain other personnel security correspondence and records in accordance with the latest edition of Order 1350.15.

c. Protection of Personnel Security Records. Personnel security records contain sensitive, highly privileged, and, in some cases, classified information. All FAA personnel shall carefully protect these records in their handling, transmittal, storage, and release.

(1) Investigative information obtained under a pledge of confidence shall be controlled in accordance with the restrictions which the investigating agency has placed on it. Such restrictions normally preclude divulging it to the subject of the investigation.

(2) OPM reports of investigation may be disseminated to authorized agency officials on a strict need-to-know basis. SSE's are responsible for deciding on the extent of dissemination. They may furnish summaries or extracts of investigative reports in lieu of disseminating the reports themselves.

(3) Medical reports included as part of an investigation shall be carefully controlled to ensure that the information they contain is disseminated only to persons who need it for security or suitability adjudication. These records shall be released to operating office managers only through aviation medical officials, who shall interpret the medical information to those management officials who have a need to know.

(4) Reports of investigation, PSF's, or other records which contain classified information shall be protected in accordance with the latest edition of Order 1600.2, Safeguarding Controls and Procedures For Classified National Security Information And Sensitive Unclassified Information.

(5) All PSF's, reports of investigation, personal history statements (including SF's 85, 85P, 85P-S, and 86), and other personnel security records and documents which contain information of a personal or privileged nature shall be protected, transmitted, stored, and destroyed in accordance with the latest editions of FAA Order 1600.2, and Order 1280.1. No employee shall have unrestricted access to any such records on himself or herself, and employees shall have access to PSF's only as provided by paragraph 305d below.

(a) As a minimum, these records shall be considered "For Official Use Only." It is not necessary to mark individual documents and records "For Official Use Only" as long as they are retained in the PSF. If these records are transmitted outside the PSF, they shall be individually marked "For Official Use Only."

(b) All reports of investigation shall be stored in a combination locked cabinet or safe, or other equally secure area. No such report shall be placed in an OPF.

(c) ACO-300 shall maintain all personnel security records on regional and center SSE managers and ACO-1 shall ensure proper security for all such records concerning the ACO-300 manager. Upon request, ACO-300 shall maintain the records on persons directly responsible for regional and center personnel security programs.

(6) All SSE personnel must ensure need to know before releasing reports of investigation, or extracts or summaries of these reports, to anyone outside the SSE. Persons outside the SSE who review reports of investigation shall sign FAA Form 1600-12, Investigative Record Review, acknowledging that they understand their obligation to protect the information. Individuals reviewing

investigative information pertaining to themselves need not sign such an acknowledgment.

d. Employee review of PSF's. Upon request, an SSE shall provide an employee the opportunity to review his or her PSF. The employee may also, in writing, authorize a representative to review it. The SSE shall do the following when complying with a request for a PSF review:

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

(2) Remove any report of investigation completed by another agency, such as OPM, the Defense Investigative Service (DIS), or the Federal Bureau of Investigation (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), that the FAA is not authorized to release it directly to the employee or representative, and that he or she should contact the investigating agency directly in order to request a copy.

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

(4) If the employee works at Washington headquarters, a regional headquarters, or a center, permit review only at the SSE.

(5) If the employee works at any other location, send only a certified true copy of the PSF to the employee's facility, retaining the original in the SSE. Enclose the copy in an envelope addressed to the employee and marked, "TO BE OPENED BY ADDRESSEE ONLY," and transmit the envelope according to the requirements in Order 1280.1.

(6) When the review takes place at the SSE, permit the employee or representative to review the PSF only under the direct observation of an SSE employee. Provide the employee or representative a reasonable amount of time to review the file and ensure that he or she does not withdraw any documents or pages from it.

e. Privacy Act requirements. In responding to requests under the Privacy Act for disclosure of information in PSF's and/or reports of investigation, FAA personnel shall follow all requirements of the latest edition of Order 1280.1. However, no report of investigation completed by another Federal agency shall be released in response to a Privacy Act request without the consent of that agency. FAA is not authorized to release such a report outright, as that is the prerogative of the agency that prepared it. If an individual asks for a copy of his or her PSF, and the PSF contains another agency's report of investigation, the person shall be told that the PSF contains the report, which agency prepared it, and that the FAA is not authorized to release it without the other agency's consent. In such a case, the FAA personnel responding to the request shall follow the procedures stated in the latest edition of Order 1280.1 concerning records that originated outside FAA. In the case of an OPM report of investigation, and because OPM has requested this procedure, the individual should be told to contact OPM directly to ask for a copy.

f. FAA personnel receiving third party inquiries shall follow the procedures for responding to them that are stated in the latest editions of Orders 1200.23 and 1280.1.

(1) A third party inquiry coming in under the Privacy Act only must have a signed statement by the first party to whom the record pertains granting the FAA permission to release it to the specific third party before FAA personnel may do so.

(2) If a third party request does not include a signed statement from the first party to whom the record pertains, and if the record requested is specifically part of the Privacy Act system of records and identifies the individual by name, Social Security number, routing symbol, or other specific identification, the request shall be logged in and answered under the provisions of the Freedom of Information Act (FOIA).

(3) If the information for a third party request is found in general records not identified by the individual's name, Social Security number, routing symbol, or other specific identification, FAA personnel shall respond to the request under the provisions of the FOIA.

(4) If the request concerns a deceased individual, FAA personnel shall respond to it under the provisions of the FOIA.

g. Agreements to release personnel security records. Without the concurrence of ACS or the appropriate SSE, no FAA employee shall enter into any collective bargaining agreement or any agreement with an individual requiring the FAA to release any personnel security record. Under no circumstances shall an employee enter into any agreement requiring the FAA to release a report of investigation completed by another Federal agency.

h. IPPS and personnel action forms.

(1) SSE's and HRMD's shall enter into the IPPS 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, which maintains and manages the IPPS. All required information shall be entered promptly and all personnel with responsibility for entering information shall ensure that the data maintained in the system are complete, accurate, and current.

(2) The sensitivity or risk level designation entered into the IPPS for each position shall be that shown on all personnel action forms. In any case where it does not, such as on an SF-52, the designation shall be entered using the coding shown in paragraph 506.

(3) Office of CAS Operations (ACO) shall represent the FAA in all discussions with OST concerning the data to be entered into the IPPS 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.

306. VISIT CLEARANCE REQUESTS.

a. The SSE shall process all requests for visit clearances received from other agencies or private companies and shall provide the appropriate offices with necessary information regarding visitors' security clearances.

b. The SSE shall process visit clearance requests to other agencies and private companies, certifying clearances on DOT Form 1630.5, Visit Clearance. Operating offices shall complete items 1 through 15 on this form before forwarding it to the SSE, and should do so as far in advance of the proposed visit as possible to allow the SSE sufficient time to process it. Clearances shall be certified 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 shall certify a security clearance to another agency or to a company.

307.-399. RESERVED.

CHAPTER 4. PERSONNEL SUITABILITY/SECURITY STANDARDS AND CRITERIA

400. RELATIONSHIP BETWEEN SUITABILITY AND SECURITY.

a. Suitability means fitness or eligibility for employment and refers to identifiable character traits and past conduct which are sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate efficiency and effectiveness. Suitability is distinguishable from a person's ability to fulfill the 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 an individual can reasonably be expected to promote the efficiency of the Federal service. Potentially disqualifying suitability factors are listed in paragraph 401.

b. Security relates to requirements for an individual occupying a specific position to have access to classified information. A security determination focuses on the question of whether or not access to such information is clearly consistent with the interests of the national security. Paragraph 402 contains the standard and criteria specified in Executive Order (E.O.) 10450 and E.O. 12968, which shall be used in making a security determination.

c. In processing applicants for employment, a security determination under E.O. 10450 and/or E.O. 12968 will usually be made subsequent to a favorable suitability adjudication. Therefore, a Human Resource Management Division (HRMD) may favorably adjudicate a background investigation or information the applicant has provided and find the person suitable for employment in a specific sensitive position; but the servicing security element (SSE) may then determine that the person should not have access to classified information. In the case of an employee, however, neither a suitability adjudication nor a security determination is contingent upon the other. For example, a security determination may result in reassignment or removal from a position under the provisions of Chapter 11, Adverse Security Actions, even if the servicing HRMD has made no

suitability determination. Also under those provisions, a security determination that an employee may not be granted a security clearance would prevent promotion or reassignment to a sensitive position.

d. Except as stated below, employees with at least 1 year of continuous FAA service in their current period of employment, or with at least 1 year of service and no break in such service of more than 1 year, are not subject to suitability determination by their HRMD. They are, however, subject to disciplinary and removal actions under the provisions of FAA's Personnel Management System when an investigation develops information warranting such action. As exceptions, the HRMD retains 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.

401. PERSONNEL SUITABILITY STANDARD AND CRITERIA.

a. Suitability Standard. A suitability adjudication is an assessment of past and present conduct which may indicate future actions with adverse impact on the efficiency of the service. The assessment is made to decide whether there is a reasonable expectation that the employment or continued employment of a person either would or would not promote the efficiency of the service. In making this determination the adjudicator considers whether the conduct of the person indicates a potential for behavior which 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. In determining potential impact on the efficiency of the service, two issues must be considered: (1) whether the conduct in question indicates a potential for inadequate or reduced performance of specific duties; and (2) 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. When making a suitability determination, the adjudicator may consider any of the following reasons as a basis for finding an individual unsuitable for employment with FAA. A person would not be suitable for employment or continued employment when, because of these factors, the potential for adverse impact on effective performance of the person or others, or on the agency's ability to carry out its responsibilities, is such that there is a reasonable expectation in the mind of the adjudicator that the employment or continued employment of the person would not promote the efficiency of the service. These criteria are as follows:

(1) Misconduct or negligence in prior employment which 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 which suggests that 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. In making a suitability determination, the adjudicator shall consider the following factors to the extent he/she deems pertinent to the individual case:

(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.

402. PERSONNEL SECURITY STANDARD AND CRITERIA.

a. Security Standard. The granting of access to classified information to any person shall be clearly consistent with the interests of the national security. In making this determination, the adjudicator assesses past and present conduct and considers whether or not the granting of such access conforms to this standard. Conduct relating to any of the criteria listed below is grounds for denying access to classified information if the conduct indicates 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. SSE's shall grant this eligibility only when doing so is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of the national security.

b. Criteria. E.O. 12968 states that eligibility for access to classified information shall be granted only to persons whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment; freedom from conflicting allegiances and potential for coercion; and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. E.O. 10450 enumerates the following criteria which shall be considered 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 (hereinafter referred to as organizations) 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 in applying the security standard and criteria:

(1) In granting access to classified information there shall be no discrimination on the basis of race,

color, religion, sex, national origin, disability, or sexual orientation.

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

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

403. COORDINATING PERSONNEL SECURITY INFORMATION. Human resource management officials and all supervisors in the FAA shall furnish to their SSE any information they receive concerning employees or applicants under their jurisdiction which may affect their suitability for employment or their holding of a security clearance because of the standards and criteria stated in paragraphs 401 and 402.

404.-499. RESERVED.

CHAPTER 5. POSITION SENSITIVITY AND RISK LEVEL DESIGNATION AND CONTROLS

500. POSITION SENSITIVITY AND RISK LEVEL DESIGNATION. All FAA positions and FAA contractor positions must be designated as to their level of risk in terms of suitability and access to automated information systems (AIS), and level of sensitivity in terms of national security.

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

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

501. RESPONSIBILITY FOR POSITION SENSITIVITY AND RISK LEVEL DESIGNATIONS. The servicing security element (SSE), working with other management officials, is responsible for designating the risk or sensitivity level of every position within its jurisdiction. All new position descriptions shall be coordinated with the SSE before a sensitivity or risk level is designated and the SSE shall approve any changes in a position's sensitivity or risk level designation. Designations may be by class, group, or categories of positions, when appropriate, or may be by an individual position when circumstances warrant doing so. The Investigations Division (ACO-300) shall work with other SSE's and with headquarters offices and services as necessary to ensure uniform designations for positions

common in more than one region or center. Appendix 3, Position Risk and Sensitivity Level Designation Process, lists minimum sensitivity levels for certain positions.

502. RISK LEVELS. There are three position risk levels, as follows:

a. Low Risk. These are positions which have potential for impact involving duties of limited relation to the agency mission with program responsibilities which affect the efficiency of the service. This level includes positions which have limited impact on AIS.

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

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

503. SENSITIVITY LEVELS. There are three sensitivity levels for designating positions with regard to national security:

a. Noncritical-sensitive (NCS). These are positions with potential for causing serious damage to the national security.

b. Critical-sensitive (CS). These are positions with the potential for causing exceptionally grave damage to the national security.

c. Special-sensitive (SS). These are positions which an agency determines 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).

504. POSITION SENSITIVITY AND RISK LEVEL DESIGNATION PROCESS.

a. SSE's shall use the risk level designation process outlined in appendix 3 to ensure that the FAA designates positions uniformly and consistently. This process includes the criteria for designating risk levels based on AIS duties and responsibilities. SSE's shall use the national security criteria for determining sensitivity levels in conjunction with the risk level designation process to ensure proper designation of national security positions.

b. All positions requiring access to classified information are sensitive positions and shall be designated at one of the three sensitivity levels. Appendix 3 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 and it may not be necessary to apply all of the specific designating procedures in appendix 3. Similarly, essentially identical positions may require only occasional case-by-case analysis. Even when risk levels may appear to be obvious, the appendix 3 procedures should be applied on at least a random basis to ensure proper designations.

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

505. OFFICIAL RECORD OF POSITION RISK AND SENSITIVITY DESIGNATION. Position risk and sensitivity level designation shall be documented on FAA Form 1600-59, Position Designation Record, contained in appendix 3. The

Human Resource Management Division (HRMD) shall maintain this form unless the SSE agrees to do so. Even if the HRMD keeps it, the SSE shall maintain a copy of every Form 1600-59 for sensitive positions. The Form 1600-59 may also be maintained electronically in lieu of retaining hard copies.

506. CODING OF POSITION RISK AND SENSITIVITY LEVELS ON PERSONNEL DOCUMENTS. The following coding of position risk and sensitivity levels is required for Governmentwide use on appropriate personnel documents such as the Standard Form 50, Notification of Personnel Action, and SF-52, Request for Personnel Action. It shall be used to record a position's level in the Integrated Personnel and Payroll System (IPPS). AIS positions, as determined according to appendix 3, paragraph 5c, shall be identified by the letter "C" after the numerical coding.

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

507.-599 RESERVED.

CHAPTER 6. PERSONNEL INVESTIGATION REQUIREMENTS

600. 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 a person holding the position, govern the type of investigation required. Chapter 3, Personnel Security Operations, Responsibilities, and Records, and Appendix 5, Forms Required for Investigations, contain specific guidance for initiating required investigations.

601. TYPES AND SCOPE OF BACKGROUND INVESTIGATIONS.

a. The Office of Personnel Management (OPM) will conduct the following investigations for the FAA:

(1) National Agency Check (NAC)

(2) National Agency Check and Credit (NACC)

(3) National Agency Check and Inquiries (NACI)

(4) National Agency Check, Inquiries, and Credit (NACIC)

(5) Minimum Background Investigation (MBI)

(6) Limited Background Investigation (LBI)

(7) Background Investigation (BI)

(8) Single Scope Background Investigation (SBI)

(9) Reimbursable Suitability/Security Investigation (RSI)

(10) Periodic Reinvestigation (PRI)

(11) Periodic Reinvestigation for Single Scope Background Investigation (PRIS)

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

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

b. Minimum Coverage. All investigations will cover the most recent 3 years of a person's life. They 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.

c. Personal Interview. OPM will conduct one or more interviews of the person who is the subject of the investigation in all SBI, BI, LBI, Upgrade, PRIS, and PRI cases.

d. Credit Searches. OPM will conduct credit searches as part of the NACC, NACIC, MBI, LBI, BI, SBI, PRI, SGI, BGI, LGI, SDI, BDI, and LDI.

e. Expanded Coverage. OPM will expand all background investigations in scope and coverage as necessary to resolve an issue.

f. Extra Coverage.

(1) If it is appropriate to the position, the FAA may request extra background investigation coverage of the following attributes. OPM investigators will then ask persons they interview additional questions about the subject in order to cover them:

(a) Managerial/supervisory attributes, which include 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, which include ability to meet and deal with all types of people, diplomacy, tact, personal appearance, and speaking ability.

(c) Law enforcement attributes, which 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, which 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 which might discredit the United States should the person be stationed in a foreign country.

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

602. BASIC INVESTIGATIVE REQUIREMENTS. Outlined below are the minimum investigative requirements for all positions within the FAA:

a. Special-sensitive position. A person in a special-sensitive position shall have a completed SBI. The investigation shall be completed, evaluated, and favorably adjudicated for both suitability and security before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611. If the person will be required to hold a clearance for access to Sensitive Compartmented Information (SCI), an SBI is required before the clearance can be requested; and an SBI is also required before a final Top Secret clearance can be granted. However, the person may be placed in the position on the basis of a waiver pending completion of an SBI or SGI.

b. Critical-sensitive position. A person in a critical-sensitive position shall have a completed BI or SBI. The investigation shall be completed, evaluated, and favorably adjudicated for both suitability and security before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611. If the person will be required to hold a Top Secret clearance, an SBI is required before the final clearance can be granted. However, the person may be placed in the position

with a completed BI or a waiver pending completion of an SBI or SGI.

c. Noncritical-sensitive position. A person in a noncritical-sensitive position shall have a completed NACIC or higher level investigation. The investigation shall be completed, evaluated, and favorably adjudicated for both suitability and security before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611 or the person already has a completed NAC. The SSE shall also conduct a subject interview as described in paragraph 602n below. If the person has a completed NACI, it is only necessary to initiate a credit check and conduct the subject interview before the person is placed in the position.

d. High-risk position. A person in a high-risk position shall have a completed BI or SBI. The investigation shall be completed, evaluated, and favorably adjudicated before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611.

e. Moderate-risk position.

(1) A person in a moderate-risk position shall have a completed NACI or higher level investigation. The investigation shall be completed, evaluated, and favorably adjudicated before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611 or the person already has a completed NAC.

(2) A person in a moderate-risk position with fiduciary responsibilities shall have a completed NACIC or higher level investigation. Positions with fiduciary responsibilities include, but are not limited to, contracting officers, contract specialists, cashiers, 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. The investigation shall be completed, evaluated, and favorably adjudicated before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611 or the person already has a completed NAC. If the person has a completed NACI, it is only

necessary to initiate a credit check before the person is placed in the position.

f. Low-risk position. An NACI is the investigation required for a person in a low-risk position. This investigation shall be initiated within 14 days after the person is placed in the position. Upon completion, the NACI shall be evaluated and adjudicated as soon as possible.

g. Periodic Reinvestigations (PRI and PRIS). A PRIS shall be completed on each incumbent of a special-sensitive position, and on each incumbent of a critical-sensitive position for which the person is required to hold a Top Secret clearance, within 5 years from the date of the last SBI, BI, or PRIS. A PRI shall be completed on each incumbent of a critical-sensitive position with no Top Secret clearance requirement, and on each incumbent of a high-risk position, within 5 years from the date of the last BI or PRI. The SSE shall review the personnel security file and the Official Personnel Folder (OPF) as part of the PRI. In addition, a NACC and local law enforcement agency checks shall be completed on each person holding a Secret clearance within 10 years from the date of the last investigation or reinvestigation.

h. Credit checks for fiduciary positions. A credit check shall be conducted on all persons employed in positions with fiduciary responsibilities at least once every 5 years, regardless of other investigation requirements that may apply. If a person is being placed in one of these positions and no preplacement investigation is required, or if such a requirement is waived, a credit check shall be initiated as soon as possible, but no later than 14 days after placement. If a credit check has been conducted within the last 5 years as part of another investigation, a new one is not required.

i. Upgrade Investigations. The appropriate Upgrade Investigation (SGI, BGI, or LGI) may be conducted when an MBI, LBI, or BI has been 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 than the one he or she currently occupies. This investigation is in lieu of the required investigation and shall be completed,

evaluated, and favorably adjudicated before the person is placed in the position, unless this requirement is waived in accordance with paragraph 611.

j. Update Investigations. The appropriate Update Investigation (SDI, BDI, or LDI) may be conducted in lieu of the required investigation whenever an LBI, BI, or SBI has been completed within the past 5 years, the same level investigation is now required, and the person has had a break in Federal service of more than 12 months.

k. Investigations on former Federal employees. The investigation required for a position shall be conducted on any former Federal employee who has had a break-in-service in excess of 12 months. If the person has had no break in service in excess of 12 months, no new investigation is required unless a periodic reinvestigation requirement applies. In determining continuity of service, any one or a combination of the following employments may be credited the same as Federal employment:

(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 a security clearance granted by a Government agency. Any period of time during which the clearance was not in effect would constitute a break in service.

(3) Employment by the District of Columbia Government.

l. Changes in risk or sensitivity level. When the risk or sensitivity level of a position changes, an incumbent may remain in the position, but any new investigation required for the new risk or sensitivity level must be initiated within 14 days of that change.

m. Movement from a public trust position to a national security position. An employee moving from a public trust to a national security position shall complete a Standard Form (SF) 86, Questionnaire for National Security Positions, which the SSE shall review before placement. If the employee has received the required investigation for the

national security position, no reinvestigation is required unless the time elapsed since the previous investigation necessitates updating, or unless information disclosed on the newly completed SF-86 or other special circumstances justify additional investigation.

n. Subject interviews for noncritical-sensitive positions.

(1) Before a person enters a noncritical-sensitive position or is granted a security clearance, the SSE shall conduct a subject interview. The interview may be conducted telephonically when the applicant or employee is not readily available for one in person at the SSE. If an interview is not feasible, the SSE may have OPM conduct an MBI to meet the investigative requirement for the position.

(2) The interviewer shall review the applicant's or employee's SF-86; Optional Form (OF) 306, Declaration for Federal Employment; and employment application prior to conducting the interview. The subject interview should 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. The interviewer should use the SF-86 questions as a guide in conducting the interview and should ask the subject about any information furnished on the SF-86, OF-306, or employment application that is not entirely favorable.

(3) The SSE shall document the date and results of the interview in writing, to include a summary of any information the subject provided that was not completely favorable. The documentation shall also include the subject's explanation about any information furnished on the SF-86 or employment application that is not entirely favorable.

o. Incomplete investigations. An investigation received from OPM which is substantially complete, even if not entirely complete, may be adjudicated for both suitability and security if the SSE determines that the outstanding portion is not likely to affect a final adjudication or help to resolve any issues. Such an

investigation may be considered complete for the purpose of meeting a preplacement investigation requirement.

p. Military Personnel and Medical Records Checks. When there is evidence that an air traffic control specialist applicant has had prior military service, the person's name, branch of service, date and place of birth, Social Security number, and separate service number, if applicable, shall be sent to the FAA representative at the National Personnel Records Center, St. Louis, Missouri. The FAA representative shall review the person's military records and provide the results to the requesting SSE. These records shall also be reviewed whenever requested by FAA aviation medical personnel for other applicants who must meet aviation medical standards, and the results sent to the requesting division through the appropriate SSE. In addition, an SSE may request the military records check on any person as necessary to help resolve any suitability or security issues raised during the investigative process. If the SSE believes that a person's records are not in St. Louis, it shall request them directly from the military organization holding them.

603. SPECIFIC REQUIREMENTS: SPECIAL-SENSITIVE POSITIONS.

Case Circumstances	Investigation/Action Required
a. Candidate with no prior investigation.	SBI completed prior to placement.
b. Candidate with prior SBI completed within past 5 years, and no break in service of 1 year or more.	Review prior investigation, current records, and personal history statement. No SDI necessary unless needed to resolve a suitability or security issue.

Case Circumstances	Investigation/Action Required
c. Candidate with prior SBI eted within past 5 years, but break in service of more than 1 year.	Review prior investigation, current records, and personal history statement, and completion of SDI before placement.
d. Candidate with prior SBI completed more than 5 years ago (with no updating investigation), but no break in service.	SBI. May be post-placement.
e. Candidate with prior SBI completed more than 5 years ago (with no updating investigation) and any break in service.	SBI completed prior to placement.
f. Candidate for position with BI completed within past 5 years.	SGI completed prior to placement.
g. Candidate for position with LBI, MBI, NACI, or NAC.	SBI completed prior to placement.
h. Candidate is incumbent of another special-sensitive position whose last investigation was completed 5 or more years ago.	PRIS completed prior to placement.

604. SPECIFIC REQUIREMENTS: CRITICAL-SENSITIVE POSITIONS.

Case Circumstances	Investigation/Action Required
a. Candidate with no prior investigation.	SBI or BI completed prior to placement.

b. Candidate with prior SBI completed within past 5 years and no break in service of 1 year 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 1 year 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 SBI or BI completed within past 5 years, but break in service of more than 1 year.	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 SBI or BI completed more than 5 years ago (with no investigation), but no break in service.	PRIS if Top Secret clearance required; otherwise, PRI. May be post-placement.
f. Candidate with prior SBI or BI completed more than 5 years ago (with no updating investigation), and any break in service.	SBI or BI completed prior to placement.

g. Candidate with LBI completed within past 5 years.	SBI completed prior to placement if Top Secret clearance required. Otherwise, BGI completed prior to placement.
h. Candidate with MBI, NACI, or NAC.	SBI or BI completed prior to placement.
i. Candidate is incumbent of critical-sensitive or high-risk position whose last investigation was completed 5 or more years ago.	Initiate PRIS or PRI. May be completed post-placement.

605. SPECIFIC REQUIREMENTS: NONCRITICAL-SENSITIVE POSITIONS.

Case Circumstances	Investigation/Action Required
a. Candidate with no prior investigation.	NACIC and subject interview completed prior to placement.
b. Candidate with prior SBI, BI, LBI, MBI, or NACIC and subject interview completed within the past 5 years and no break in service of more than 1 year.	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 SBI, BI, LBI, MBI, or NACIC and subject interview, but break in service of more than 1 year.	New NACIC and subject interview completed prior to placement.

Case Circumstances	Investigation/Action Required
d. Candidate with NACI.	Review prior investigation, current records, and personal history statement. Credit check and subject interview completed prior to placement.
e. Candidate with NAC.	NACIC and subject interview completed prior to placement.
f. Candidate is incumbent of noncritical-sensitive position whose last investigation was more than 5 years ago.	Review prior investigation, current records, and personal history statement. Credit check and/or subject interview if not previously conducted. No additional investigation necessary unless needed to resolve a suitability issue.

606. 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 SBI or BI completed within past 5 years, and no break in service of 1 year or more.	Review prior investigation and current records. No new investigation necessary unless needed to resolve suitability issue.
c. Candidate with prior SBI or BI completed within past 5 years, but break in service of more than 1 year.	Review prior investigation, current records, and personal history statement. BDI completed prior to placement.

Case Circumstances	Investigation/Action Required
d. Candidate with prior SBI 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, NACI, or NAC.	BI completed prior to placement.
h. Candidate is incumbent of critical-sensitive or high-risk position whose last investigation was completed 5 or more years ago.	Initiate PRI. May be completed post-placement.

607. 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, NACIC completed prior to placement.

Case Circumstances	Investigation/Action Required
b. Candidate with prior SBI, BI, LBI, MBI, NACIC, or NACI completed within the past 5 years and no break in service of more than 1 year.	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 SBI, BI, LBI, MBI, NACIC, or NACI, but break in service of more than 1 year.	New NACI completed prior to placement. If position has fiduciary responsibilities, NACIC completed prior to placement.
d. Candidate with NAC.	NACI initiated prior to placement. If position has fiduciary responsibilities, NACIC initiated prior to placement.
e. Candidate is incumbent of noncritical-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.

608. 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, BI, SBI, and no break in service of more than 1 year.	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 SBI, but break in service of more than 1 year.	NACI initiated no later than 14 days after placement.
d. Candidate with NAC.	NACI initiated no later than 14 days after placement.

609. 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 Associate Administrator for Civil Aviation Security (ACS). An LBI shall be the minimum level investigation conducted on all persons employed in ACS and subordinate offices. All ACS personnel in positions designated special-sensitive or critical-sensitive shall be subject to the investigation required for their level.

610. EXCEPTIONS TO INVESTIGATIVE REQUIREMENTS.

a. Exempt Positions.

(1) Certain low-risk positions are exempt from the investigative requirements provided FAA conducts at least two reference checks on the applicant to ensure that the employment of the person is clearly consistent with the efficiency of the service and the interests of national security. This exception shall not be viewed as a prohibition from processing the person under the normal investigative requirements. Persons appointed without

investigation shall not have access to classified information or to areas restricted for security reasons.

(2) The exempt positions are:

(a) 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.

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

b. Detailed Positions. Individuals occupying permanent positions who are detailed formally or informally into special-sensitive, critical-sensitive, noncritical-sensitive, high-risk, or moderate-risk positions must meet the normal investigative requirements prior to the detail if the detail is to be in excess of 120 days. If access to classified information is required, the person must have the investigation required for the clearance. If the detail is to a special-sensitive, critical-sensitive, or high-risk position and will be for less than 120 days, the SSE shall review the prior investigation, OPF, Personnel Security File, and a current SF-86 or SF-85P, Questionnaire for Public Trust Positions, and SF-85P-S, Supplemental Questionnaire for Selected Positions, as applicable. If a detail originally scheduled for 120 days or less is unexpectedly extended for another period of 120 days or less, the individual may continue in the position without meeting the normal investigative requirements. However, no person may be continued in a series of details in excess of 240 days unless the required investigation is in progress or the requirement is waived in accordance with paragraph 611.

c. Individuals occupying noncritical-sensitive and moderate-risk positions under previously existing requirements. Employees occupying noncritical-sensitive and moderate-risk positions who were investigated under requirements in effect prior to the date of this order and who do not meet the current minimum investigative requirements for positions at these levels may remain in their positions, or be placed in other positions in the same

job series and at the same risk or sensitivity level, without further investigation.

611. WAIVER OF PREPLACEMENT INVESTIGATIVE REQUIREMENTS.

a. Criteria.

(1) Executive Order 10450 requires that waiver of the preplacement investigative requirements on persons entering special-sensitive, critical-sensitive, or noncritical-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. DOT has established the same criteria for high-risk and moderate-risk positions. The Office of the Secretary (OST) has given ACS authority to grant waivers for noncritical-sensitive and moderate-risk positions; and, in some circumstances, for special-sensitive, critical-sensitive, and high-risk positions. Only OST may grant waivers for special-sensitive, critical-sensitive, and high-risk positions when ACS does not have delegated authority to do so.

(2) Prior to appointing a person to a sensitive or public trust position, and prior to making a firm starting date commitment to a person to begin working in such a position, the responsible Human Resource Management Division (HRMD) or operating office appointing official shall obtain authorization from the SSE and assurance that either the preplacement investigative requirements have been met or that OST or the SSE has granted a waiver. If, through clerical or other error, a person has been permanently appointed to a sensitive or public trust position without first meeting the investigative requirements, the HRMD or operating office shall contact the SSE.

b. Request and Processing Procedures.

(1) Operating office request and actions.

(a) The operating office shall submit a written request to the SSE for a waiver of a preplacement investigative requirement. This request shall include:

1 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;

2 The position's title, grade, and location;

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

4 If the person has been chosen for a sensitive position, the level of security clearance required, a 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.

(b) The operating office should submit the waiver request as soon as possible, allowing at least 3 weeks for processing for critical-sensitive and high-risk positions.

(c) No office shall make a firm starting date commitment to any applicant until a waiver has been granted or the investigative requirement has been met.

(d) The operating office should advise the applicant of the need to obtain a waiver; the importance of promptly submitting all required forms and furnishing the SSE all information requested; and, for critical-sensitive and high-risk positions, the SSE's need to contact the applicant for an interview.

(2) SSE Processing.

(a) Special-sensitive, critical-sensitive, and high-risk positions. For waiver requests for these positions, the SSE shall do the following:

1 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.

2 Obtain and review the candidate's completed SF-86 or SF-85P, as appropriate; SF-85P-S, if applicable; OF-306; and employment application.

3 Conduct 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. The subject shall also be asked if there is anything in his/her background which could raise any questions of personal character or loyalty to the United States. The interviewer should use the questions on the SF-86 or SF-85P, and the SF-85P-S, if applicable, as a guide in conducting the interview and should ask the subject about any information furnished on the SF-86, SF-85P, SF-85P-S, OF-306, or employment application that is not entirely favorable. The interview may be conducted telephonically when the candidate is not readily available for one in person at the SSE.

4 Conduct a credit check.

5 Conduct a check of the subject's current or most recent former employer.

6 If the candidate is a current or former FAA employee, review the OPF (current employee) and Personnel Security File (PSF), if available, and conduct a check of the Investigations Subsystem of the Civil Aviation Security Information System (CASIS) or other appropriate automated system for record of any FAA investigation. If the person is currently employed outside the SSE's area of responsibility, contact the appropriate SSE to accomplish OPF and PSF reviews.

7 Conduct a check of the current or former employing agency's security office (for current and former Federal employees only), if other than FAA.

8 Initiate the required investigation.

9 If the operating office's request contains sufficient justification, and if the SSE knows of no significantly unfavorable information regarding the applicant, prepare a transmittal memorandum to the Investigations Division (ACO-300) containing the following information:

(aa) Nature of waiver request; i.e., from (operating office identification), to place (name of applicant) into a (position sensitivity or risk level).

(bb) If FAA employed, subject's current security clearance, if any, and basis; and title and grade level of subject's present position. In addition, state the results of a review of subject's OPF and PSF.

(cc) If not FAA employed, type, date, and results of any previous investigation(s). If the review of a previous investigation cannot be accomplished within a reasonable period of time, so stipulate. In addition, indicate results of telephonically conducted check with subject's present or most recent employer.

(dd) Date and 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 SF-86, SF-85P, SF-85P-S, or employment application that is not entirely favorable.

(ee) The date the investigation forms were forwarded to OPM, and attach, as appropriate, a copy of subject's SF-86 or SF-85P, SF-85P-S, if applicable, and employment application.

(ff) The results of credit search and any local agency checks.

(gg) The servicing security element's recommendation for approval.

(hh) As an attachment, the request from the operating office.

(b) Noncritical-sensitive and moderate-risk positions.

1 For waiver requests for these positions, the SSE shall do the following:

(aa) 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.

(bb) Obtain and review the applicant's completed SF-86 or SF-85P, as appropriate; SF-85P-S, if applicable; and employment application.

(cc) If candidate is an FAA employee, review PSF and check the appropriate automated system for record of any FAA investigation.

2 The SSE may then approve the waiver request if it is satisfied that the request is justified and that the available information raises no significant security or suitability issues. The SSE should then give the HRMD permission to place the person in the noncritical-sensitive or moderate-risk position.

3 If the candidate provides information on the SF-86, SF-85P, SF-85P-S, or employment application showing any of the following, the SSE should not approve the waiver unless it has checked with the appropriate law enforcement agency and/or previous employer and is satisfied that the information raises no significant security or suitability issues:

(aa) Any arrests, charges, convictions, or incarceration within the last 5 years.

(bb) Any drug-related arrests, regardless of when they occurred.

(cc) More than one arrest, regardless of when they occurred.

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

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

4 Before granting a waiver, the SSE shall resolve 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 due regard to the nature, extent, and recency of the conduct. The SSE should interview the applicant as necessary to resolve any issues.

(c) Optional Checks. For special-sensitive, critical-sensitive, noncritical-sensitive, high-risk, or moderate-risk positions, the security element may conduct appropriate local agency checks that are readily available. For current or former Federal employees, the security element may wish to conduct a check of OPM's Security Investigations Index (SII), especially if information from a former agency's security office appears incomplete.

(3) ACO-300 processing and notification of decision.

(a) ACO-300 shall promptly review each waiver request from a regional or center SSE for sufficiency of justification and inclusion of all required information. In the absence of any significantly unfavorable information, ACO-300 may grant the waiver and notify the SSE of its approval. If the request contains any significantly unfavorable or questionable information, ACO-300 shall either return it to the SSE as disapproved or transmit it and all appropriate documentation to the Office of Security (M-70), OST, requesting a reply back to ACO-300. Upon receipt of a reply, ACO-300 shall notify the appropriate SSE.

(b) Only OST may grant waivers for special-sensitive, critical-sensitive, and high-risk positions when

ACO-300 is the SSE. When that is the case, ACO-300 shall transmit the request and all appropriate documentation to M-70.

612. SPECIAL PROCEDURES FOR ACCELERATED HIRING.

a. The Office of CAS Operations (ACO) and the Office of Human Resource Management (AHR) may jointly enter into agreement with particular operating offices to establish procedures for accelerated hiring of applicants into specific safety-critical positions. Individual SSE's and their corresponding HRMD's may also enter into these agreements. The procedures under such an agreement may permit applicant hiring following basic qualifications determinations and limited initial security investigation. If the position requires applicants to meet certain medical qualifications, the Office of Aviation Medicine (AAM) will normally also be a party to the agreement. Each involved organization will conduct part of the process which shall be satisfactorily completed before HRMD's or operating offices may 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 before the FAA commits to hiring them. The procedures may be used for noncritical-sensitive and moderate-risk positions, and are an alternative to a waiver of the preplacement investigative requirement processed in accordance with paragraph 611.

b. When ACO, AHR, AAM, and an operating office agree to apply accelerated hiring procedures to a particular category of positions, they shall also agree on the specific security checks to be conducted before ACO or a particular SSE may give an HRMD security approval for hire. At a minimum, the checks shall consist of the following:

(1) ACO review of a completed employment application and a completed SF-85P or SF-86, whichever the position requires.

(2) A check of the applicant's fingerprints by the Federal Bureau of Investigation for a possible record.

(3) Checks with state and/or local law enforcement agencies covering those areas where the

applicant has worked or lived for a significant period of time during the most recent 5 years.

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

d. ACO may issue implementing instructions for the security processing of applicants under these procedures, and may do so jointly with AHR and other concerned offices. These instructions may specify, for example, that operating office personnel interviewing applicants shall review the employment application and the SF-85P or SF-86, as appropriate, and the SF-85P-S, if applicable, and make an initial determination as to whether or not an applicant may continue to be processed for hiring prior to completion of the required investigation.

e. An applicant shall not be hired under these procedures prior to completion of the required investigation if he or she admits any of the following on the employment application, SF-85P, SF-85P-S, or SF-86, or if the checks conducted reveal any of the following:

(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 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. No HRMD or operating office shall commit to hire any applicant being processed under these procedures without specific approval from ACO or an SSE.

g. Once the checks are completed, and ACO or an SSE has given approval to hire an applicant, ACO or the SSE may initiate the required investigation at any time; or, at the latest, within 14 days following the date on which the individual enters on duty. Results of the checks completed under these procedures shall be furnished to OPM with the required investigative forms.

h. If ACO or an SSE does not give approval for hire based on review of forms or results of checks conducted, no HRMD or operating office shall commit to hiring the applicant until the required investigation has been completed and favorably adjudicated for both suitability and security.

613.-699. RESERVED.

CHAPTER 7. STANDARDS AND PROCEDURES FOR USING PREVIOUS INVESTIGATIONS

700. GENERAL.

a. Some applicants for FAA employment and some newly hired employees, especially those persons transferring from other Government agencies, will have already been investigated by another Federal department or agency. Servicing security elements (SSE) shall use these investigations when practicable to reduce the number of investigations which FAA requests from the Office of Personnel Management (OPM), thereby reducing investigative costs and delays in waiting for investigations to be completed.

b. In reviewing an employment application, an SF-86, Questionnaire for National Security Positions; an SF-85P, Questionnaire for Public Trust Positions; or an SF-85, Questionnaire for Nonsensitive Positions, a personnel security officer should be alert to any information indicating that the applicant may have had a previous investigation. Such information would include recent Federal employment; military service, including service with the National Guard or reserves; employment with a Government contractor where the person might have held a security clearance; and a claim by the person that he or she has had a previous investigation and/or a security clearance.

c. When a previous investigation is readily available, the SSE should review it prior to giving a Human Resource Management Division (HRMD) or operating office permission to employ the person in a sensitive (special-sensitive, critical-sensitive, or noncritical-sensitive) or public trust (high-risk or moderate-risk) position. If possible, the SSE shall obtain a copy of the investigation for the person's Personnel Security File (PSF).

d. If a previous investigation is not readily available, the SSE should obtain as much information as possible about it before giving an HRMD or operating office permission to employ the person in a sensitive or public trust position. Sources of this information can include the agency which conducted the investigation, an employing agency security office, or an agency which granted the

person a security clearance. The SSE shall request a copy of the investigation and review it as soon as possible.

e. An investigation which another Federal agency conducted on an FAA applicant or employee, and which is of the same type and scope as the one required for the FAA position, is sufficient to meet the investigative requirements provided that it was conducted within the past year or that the applicant or employee has had no break in service in excess of 1 year since the investigation was completed. Except where there is substantial information indicating that an individual may not meet the suitability and/or security standards and criteria stated in chapter 4, such an investigation shall be accepted by the FAA. Any higher-level investigation than the one required for the position also meets the requirements.

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

701. OBTAINING AND REVIEWING PREVIOUS INVESTIGATIONS.

a. Office of Personnel Management (OPM). OPM maintains the Security Investigations Index (SII), an index of investigations conducted by OPM and certain other Federal agencies. An SSE shall check this index whenever there is an indication that OPM or another agency has conducted an investigation. The SSE may 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 the SSE can do that through a direct data link to FIPC. In written and telephonic requests, the SSE must provide the Security Office Identifier (SOI) which OPM has assigned to it.

(1) National Agency Check and Inquiries (NACI) Investigations. The method of documenting NACI's depends on when they were completed. When sending a completed NACI to an agency, OPM furnishes a certificate which an agency

security officer or specialist signs and which then is placed in an employee's Official Personnel Folder (OPF). If an FAA applicant or employee previously worked at another agency, this certificate in the OPF provides sufficient documentation that the NACI was completed on the date shown. Prior to instituting this procedure, OPM returned a copy of the person's employment application stamped either "Processed under 3(a) of E.O. 10450," or "Results furnished to requesting agency." Either of these stamps on an employment application in an applicant's or employee's OPF also provides sufficient documentation that an NACI was completed. An employment application stamped "Processed under 3(a) of E.O. 10450" indicates that the NACI results were favorable. An employment application stamped "Results furnished to requesting agency," or a certificate showing completion of an NACI, indicates that OPM did not adjudicate the results, but instead sent them to the agency for adjudication. In these cases, the SSE shall check with whatever sources are available to determine whether or not the NACI revealed any information raising security or suitability issues. These sources may include FIPC or the appropriate agency security office.

(2) Other investigations. When an SII check or other documentation reveals that OPM previously conducted another type of investigation, the SSE shall obtain and review a copy of that investigation. The SSE may request it from OPM by submitting OFI Form 79B, or electronically, if the SSE can do so.

b. Department of Defense (DOD).

(1) DOD indexes its investigations in the Defense Central Investigations Index (DCII), maintained by the Defense Investigative Service (DIS). These include investigations on military personnel, DOD civilian employees, and DOD contractor personnel. When requesting a check of this index, the SSE shall prepare and send to DIS a letter formatted as shown in figure 1 at the end of this chapter. DIS will then check the DCII and provide the results to ACO-300. It will also furnish a copy of any report of investigation on file. ACO-300 will then transmit the information and/or report to the SSE.

(2) The Defense Industrial Security Clearance Office (DISCO), an office of DIS, grants security clearances to DOD contractor employees. An SSE may conduct name checks with DISCO and obtain investigation and security clearance information by calling DISCO in Columbus, Ohio, at 614-692-2265. FAA's facility code is "FAA." Copies of investigations conducted for DISCO clearances may be requested through DCII.

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

d. Other Federal agencies. Other Federal agencies have authority, either by law or through agreement with OPM, to conduct their own investigations pursuant to Executive Order 10450. These agencies include the Department of State, Central Intelligence Agency, Peace Corps, U.S. Information Agency, U.S. Secret Service, Internal Revenue Service, U.S. Customs Service, and U.S. Postal Service. 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, the SSE shall 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 the agency will not release a copy of an investigation, but will permit review at an office in the Washington, D.C., area, ACO-300 shall assist the SSE by reviewing the report, documenting the results, and providing the information to the SSE. If there is any indication that a copy of an investigation might be on file at OPM, FIPC, the SSE may request a copy as it would for an OPM investigation. OPM will furnish a copy of another agency's investigation if it has it on file and if it meets current OPM criteria for release.

702. SAMPLE LETTER FOR DCII CHECKS. Figure 1 shows the format for a letter to request DCII checks.

Figure 1. SAMPLE LETTER FOR DC11 CHECKS

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

Attn: DO960

Dear Sir:

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

Name	DPOB	SSN

Mail results to:

Attn: (Name - Personnel Security Officer)
Federal Aviation Administration
Investigations Division, ACO-300
800 Independence Avenue, SW.
Washington, DC 20591

1. Purpose Code: 06

2. Accreditation: XE023

Thank you for your cooperation in this matter.

Sincerely,

cc: ACP-300

703.-799. RESERVED.

CHAPTER 8. SUITABILITY ADJUDICATION

800. GENERAL. As stated in paragraph 400a, the focus of a suitability adjudication is on whether the employment or continued employment of an individual can reasonably be expected to promote the efficiency of the Federal service. This chapter prescribes basic suitability adjudication procedures for FAA. Appendix 6, Suitability Adjudication Procedures, contains more detailed procedures for adjudicators to follow. Suitability adjudication is separate from security adjudication under Executive Orders 10450 and 12968, the procedures for which are in Chapter 9, Security Adjudication.

801. ADJUDICATION RESPONSIBILITIES.

a. Within FAA, Human Resource Management Division (HRMD) managers are assigned all suitability adjudication authority for both applicants and employees. They may designate subordinates as adjudicators. Adjudicators shall be designated in writing, shall meet the requirements of paragraph 301b of this order, and shall be thoroughly familiar with current laws, regulations, and criteria pertaining to suitability adjudications.

b. HRMD responsibility and authority for suitability adjudication extend to those employees who have not had at least 1 year of continuous FAA service, and to certain employees under other conditions as specified in paragraph 400d. Other employees are subject to disciplinary and removal actions under the provisions of FAA's Personnel Management System.

802. ADJUDICATION REFERRAL.

a. The first step in determining a person's suitability for FAA employment is the review and referral process involving:

(1) HRMD or operating office review of a person's application and application-related information received or developed by the HRMD or operating office to identify any potentially disqualifying suitability issues.

(2) Referral of an application in a case with a potentially disqualifying issue to a qualified HRMD adjudicator for a suitability determination.

b. This process occurs prior to initiating an investigation during initial consideration of an application.

c. Reviewers shall refer to an adjudicator any application containing an indication of any of the following, regardless of the date of occurrence:

(1) A statutory debarment issue, as listed in Appendix 7, Statutory Debarment Issues.

(2) An other-than-honorable military discharge.

(3) A loyalty or terrorism issue.

(4) Evidence of dishonesty in the application or examination process (e.g., falsification of application).

d. Reviewers shall refer applications when there is an indication of one or more occurrences of any of the following issues within the past 3 years. These issues may also involve delinquency or misconduct in employment, including military service:

(1) Pattern or abuse of alcohol.

(2) Pattern or abuse of illegal drugs.

(3) Rape, sexual assault, or other criminal misconduct.

(4) Dishonest conduct.

(5) Financial irresponsibility pattern.

(6) Disruptive or violent behavior.

(7) Rioting or violent behavior.

(8) Destruction of property.

(9) Felony conviction.

(10) Illegal use of firearms or other weapons.

803. INVESTIGATIONS, PROCESSING, AND SUITABILITY/SECURITY ADJUDICATION.

a. When a trained adjudicator is able to review an application and related documents and make an unfavorable suitability determination based on clearly disqualifying investigation of the applicant. The adjudicator shall use the procedures in appendix 6 as a guide in making this determination unless it can be made based on a statutory debarment issue specified in appendix 7.

b. If there are unresolved suitability issues and/or the adjudicator cannot determine that the applicant is clearly suitable or unsuitable, the HRMD shall consult with the servicing security element (SSE) regarding the type of investigation necessary to resolve the issue(s). The HRMD and/or the SSE shall then initiate the investigation following the procedures in paragraph 303 of this order. The SSE may conduct a limited inquiry to resolve an issue, such as by obtaining court, credit, or other record information, or may decline to investigate pending completion of the required investigation by OPM.

c. In many cases suitability issues will not be evident until the required background investigation is completed or obtained by FAA, either while a person is still an applicant or after being hired. The SSE will receive all investigative reports from OPM and in some cases will receive reports of investigation completed by other agencies. As stated in paragraph 304, the SSE will sometimes conduct an additional investigation. The SSE shall also provide a person the opportunity to respond to unfavorable information when required by paragraph 303g.

d. While investigating issues involving employee conduct, SSE's may also receive information which could warrant an unfavorable suitability determination. As paragraph 202a requires, the SSE shall provide the employee an opportunity to respond to the unfavorable information.

e. When the SSE has information which may warrant an unfavorable suitability determination, it shall forward all reports and pertinent information to the HRMD for adjudication. The SSE may forward any reports of investigation to the HRMD, but is not required to do so when they contain no unfavorable information or information that under the procedures in appendix 6 could not reasonably be expected to result in an unfavorable suitability determination. However, the SSE shall forward any reports or other information to the HRMD which might raise a question about an individual's qualifications for a particular job, even if they raise no suitability or security issue.

f. When the subject of an investigation is an FAA employee and the SSE forwards investigative information to the HRMD, it shall also send a copy to the operating office.

g. The SSE shall 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 shall also notify the HRMD that it has done so.

h. The HRMD, in consultation with the SSE and with the operating office in the case of an employee, shall make all suitability determinations. It shall coordinate with AAM or its Aviation Medical Division in regard to any medical issues. The HRMD shall consult with the Office of the Chief Counsel (headquarters cases) or Assistant Chief Counsel (regional and center cases) prior to making a nonsuitability determination.

i. If a person is an applicant for a sensitive position, the SSE may, if warranted, deny granting any security clearance required for the position. In doing so, the SSE shall follow the procedures in Chapter 11, Adverse Security Actions, in addition to providing the HRMD with all information necessary to make a suitability determination. The SSE may take this action even if the HRMD has not made a suitability determination; and the HRMD may make a suitability determination even if the SSE has not completed all of the actions required under chapter 11. Per

paragraph 1102d(2)(a), an applicant denied a clearance required for a position shall not be appointed to the position.

j. If a person is an employee in a sensitive position, the SSE may, if warranted, revoke any security clearance required for the position, provided that it does so following the procedures in chapter 11. It shall also provide the HRMD with all information necessary to make a suitability determination. The SSE may take this action even if the HRMD has not made a suitability determination; and the HRMD may make a suitability determination even if the SSE has not completed all of the revocation actions required under chapter 11.

804. SUITABILITY ADJUDICATION PROCESS.

a. Suitability adjudication is a three-level process consisting of basic suitability adjudication, position sensitivity adjudication, and position performance adjudication.

(1) Basic suitability adjudication is the first level of suitability adjudication and is an assessment of conduct as it affects a person's suitability for any position at FAA. At this level an HRMD applies the suitability standard and criteria in paragraph 401 of this order and adjudicates issues in and of themselves, without particular reference to their impact on employment eligibility for a specific position. As in each step of the adjudication process, the conduct of the person as it may adversely affect his or her performance, or the ability of the agency to perform its mission, is subject to careful evaluation under screening standards that are designed to promote uniform and equitable decisions. No HRMD shall take action to disqualify a person from FAA employment unless it has first established an adverse connection, or nexus, between a person's conduct and either the person's performance in any position or the agency's ability to perform its mission. Such a nexus shall be one where the HRMD reasonably expects that the person's employment would not promote the efficiency of the service.

(2) Position risk adjudication, the next step in the adjudication process, is applied to persons rated

suitable at the basic suitability adjudication level who are being considered for employment, or retention in employment, in specific positions. The HRMD assesses 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. In adjudicating conduct, the HRMD views 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) Position Performance Adjudication, the final step in the adjudication process, applies to persons who have been rated suitable at the first two levels. The HRMD assesses 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. Appendix 6 contains specific procedures for adjudicating suitability at each of the above levels.

805. DOCUMENTATION AND NOTIFICATION.

a. An HRMD making a suitability adjudication shall clearly document it. In any case where there are serious issues, whether the determination is favorable or unfavorable, the documentation shall contain a clearly written rationale stating that the individual'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. The HRMD shall maintain this record for at least 2 years from the date of the adjudication.

b. When the HRMD has determined that an individual is not suitable, it shall notify the person in writing, stating the nature of the proposed action and the specific, detailed reasons for it. If the HRMD has found the individual unsuitable as the result of either position risk adjudication or position performance adjudication, the notification should tell the person that he or she has been found unsuitable for employment with FAA in any position at a specified risk level, or in a specific position, as applicable. The notification shall also include specific

statements about any due process rights afforded the individual based on his or her status.

c. In any case where the HRMD proposes a nonsuitability determination, it shall maintain copies of all documentation pertinent to the adjudication, including letters or memoranda of proposed action; written challenges, replies, or documentation supplied by the individual; and a written summary of any oral response. The HRMD shall maintain this documentation for at least 2 years from the date of the final decision in the case. Any adverse personnel action resulting from an unfavorable suitability determination shall be in accordance with the FAA's Personnel Management System.

d. FAA is required to 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) Form OFI-79A, Report of Agency Adjudicative Action on OPM Personnel Investigations, accompanies all completed OPM reports of investigation and shall be completed and returned to OPM whenever the instructions on the form say to do so.

(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. Whichever form OPM sends for this purpose shall be completed and returned to OPM whenever the instructions on the form say to do so.

(3) Whenever OPM requires the return of an OFI-79A or other form, and the SSE is sending reports of investigation and other pertinent information to the HRMD, the SSE shall include the OPM form with the reports. Upon completion of final adjudicative action, the HRMD shall complete the form and return it to the SSE for forwarding to OPM. When the individual is applying for or employed in a sensitive position, the HRMD shall coordinate with the SSE before completing the form.

(4) If the SSE makes an adverse security determination which precludes any HRMD suitability adjudication, it shall complete the applicable OFI form and return it to OPM. The SSE shall also forward a copy of the completed form to the HRMD.

(5) In the case of an unfavorable suitability or security adjudication, which may warrant OPM action to debar the person from Federal employment, the division returning either the OFI-79A or other form shall also include copies of:

(a) Reports of any investigation conducted by FAA or another agency which OPM may not already have.

(b) Any letter or memorandum proposing action, any response from the individual, and any documents relating to an appeal.

(c) Any other information or documents which would assist OPM in determining if debarment from Federal employment is warranted.

806.-899. RESERVED.

CHAPTER 9. SECURITY ADJUDICATION

900. GENERAL. E.O. 10450, Security Requirements for Government Employment, requires that an agency make a security determination as to whether the employment of a person in a sensitive position is clearly consistent with the interests of the national security. E.O. 12958 and E.O. 12968 require that a determination be made concerning whether the person is eligible for access to classified information. Servicing security elements (SSE) are responsible for adjudicating all pertinent information and making these determinations. Chapter 10, Access Authorizations, contains more specific criteria and procedures for granting access to classified information. Appendix 12, Security Adjudication Guidelines, contains specific guidelines for determining eligibility for access to classified information.

901. RESPONSIBILITY FOR SECURITY ADJUDICATIONS.

a. The SSE is responsible for security adjudication for all employees and applicants for positions under its jurisdiction, except for the positions of regional administrator, deputy regional administrator, center director and deputy director, and SSE manager. The Investigations Division (ACO-300) shall make the security adjudications for persons in these positions, except that the Office of Security and Administrative Management (M-70), Office of the Secretary, in consultation with the Director of CAS Operations (ACO-1), shall be responsible for adjudications involving the ACO-300 manager. If an SSE manager so requests, ACO-300 shall adjudicate cases on those SSE personnel directly responsible for administering the personnel security program, such as the appropriate branch manager, the personnel security officer, and/or a personnel security specialist.

b. All cases involving the Associate Administrator for Civil Aviation Security (ACS-1), the Deputy Associate Administrator for Civil Aviation Security (ACS-2), ACO-1, ACO-2, and the ACO-300 manager shall be referred to M-70 for security adjudication.

c. Cases which raise significant questions regarding a person's loyalty to the United States and cases where the

SSE manager concludes that a person has been coerced, influenced, or pressured to act contrary to the interests of the national security shall be forwarded to ACO-300 for referral to M-70, which will then refer them to the Federal Bureau of Investigation (FBI). Any other cases may be forwarded to ACO-300 for advisory opinions.

902. CASE ADJUDICATION PROCEDURES.

a. During initial review of any report of investigation or of any information received which raises a security issue, the SSE adjudicator shall:

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

(2) Determine if there are any significant discrepancies between activities claimed on an SF-85, SF-85P, SF-85P-S, SF-86, 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 ACO-300.

b. The SSE shall obtain additional information as needed to adjudicate the case. It may request the Office of Personnel Management (OPM) to conduct additional investigation if an OPM report appears to be inconclusive or incomplete, or to conduct a Reimbursable Suitability Investigation to resolve an issue raised in a National Agency Check and Inquiries Investigation (NACI) or Minimum Background Investigation (MBI). The SSE may also, however, initiate an FAA investigation to resolve any issues when warranted as stated in paragraph 304. By personal interview or interrogatory, the SSE may question an applicant or employee about discrepancies relating to applications or security forms, but may not allow the person to amend such forms to eliminate the discrepancies.

c. All issues in question (except loyalty cases) shall be assessed 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, may impair the security interests of the United States demonstrates a national security risk. The standard and criteria to be used in this assessment are those stated in paragraph 402. The guidance in appendix 12 shall be used in all determinations of eligibility for access to classified information.

d. The SSE shall 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. If the SSE believes that the granting of a security clearance is not clearly consistent with the interests of the national security, the applicant or employee must be denied a security clearance, or any clearance which the person has must be revoked. In the case of an employee who already has a clearance, the SSE shall immediately suspend the person's access to classified information pending completion of the revocation process. (See Chapter 11, Adverse Security Actions.)

903. TIMELINESS OF ADJUDICATIONS. In the interests of national security, the FAA, and the individual involved, the SSE shall adjudicate cases promptly. In cases requiring security adjudication based on an OPM investigation, and when required by OPM, the SSE shall return the OPM Form OFI 79A, which accompanies the completed reports, within 90 days from the date of receipt of the material or upon final adjudicative action. OPM requires use of this form to report the action taken.

904. RECORDS TO BE MAINTAINED.

a. The SSE shall maintain a record of all security adjudications, to include the following:

(1) A copy of the case transmittal form and OFI Form 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 the SSE proposes an adverse security action, it shall maintain, at a minimum, an administrative due process file consisting of the documents mentioned in paragraph 904a and the following:

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

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

(3) A copy of any report of investigation from OPM, another agency, or the FAA.

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

c. When the individual is an applicant and does not become an FAA employee, the file created when an adverse action is proposed shall be retained for at least 2 years from the date of the final decision in the case. If no adverse action is proposed on an applicant who is never hired, the SSE shall keep the record of the adjudication for at least 1 year from the date of the adjudication. If the person is or becomes an FAA employee, the SSE shall include the above documents in the Personnel Security File (PSF).

905.-999. RESERVED.

CHAPTER 10. ACCESS AUTHORIZATIONS

1000. GENERAL. Access authorizations are certifications by servicing security elements (SSE) in accordance with provisions of E.O. 12958 and E.O. 12968 that persons are found to be sufficiently trustworthy to be allowed access on a need-to-know basis to classified national security information at specified levels. These authorizations are generally called security clearances. SSE's may grant them for access to classified information at the Confidential, Secret, and Top Secret levels. A clearance is usually granted after the required investigation is completed and the SSE has made a favorable security adjudication. Especially tight controls are imposed in processing Top Secret access authorizations and requests for access to Sensitive Compartmented Information (SCI). Access authorizations are terminated when no longer required. SSE's may grant interim clearances under specified conditions in which urgent need warrants the risk of not waiting for completion of the required investigation. DOT does not have authority to grant access to SCI, but the Director of Central Intelligence may grant such access to an FAA employee when necessary for the employee to perform his or her duties.

1001. REQUEST PROCEDURES.

a. The SSE shall grant a security clearance only upon specific written request from the employee's supervisor or a manager for whom the employee works. This request shall specify the reason that a clearance is necessary and the level of classified information to which the employee will need access.

b. If the employee will not need access to classified information for a period of time exceeding 6 months, the supervisor or manager shall request a temporary clearance for the required amount of time.

c. When requesting an interim clearance, the supervisor or manager shall 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.

d. When appropriate, and in lieu of submitting a separate request for each employee needing a clearance, a supervisor or manager may submit a request for clearances that covers an entire group of employees, such as all of those persons 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. Such a request shall then be sufficient for the SSE to grant clearances to all employees in the specified group(s). Position sensitivity designations should be reviewed as clearances are requested in order to ensure that positions have the appropriate sensitivity levels required and that these levels are adjusted as necessary.

e. E.O. 12968 requires that an agency limit the number of employees that it determines are eligible for access to classified information to the minimum required for the conduct of agency functions. Supervisors and managers shall request security clearances for employees only when there is a demonstrated, foreseeable need for access. The SSE shall evaluate 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. Upon the SSE's request, an operating office shall provide information necessary to confirm that an employee needs access to classified information at the level specified. If there is any dispute regarding the need for a clearance that the operating office and the SSE cannot resolve, ACO shall make the final determination of need.

f. A security clearance shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access to classified information and such access can reasonably be prevented.

1002. INTERIM CLEARANCES.

a. In exceptional circumstances where an employee must perform official functions requiring access to classified information prior to completion of the required investigation, the SSE may grant the employee temporary eligibility for access. This type of access is called an

interim clearance and may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of this access. This process shall not be used in lieu of a waiver or as a means to place an employee in a sensitive position without the required background investigation.

b. Upon determining that they are needed and justified, SSE's may grant interim clearances for access to Confidential and Secret information. Only the Office of Security and Administrative Management (M-70), OST, may grant interim Top Secret clearances.

c. Any one of the following may serve as the basis for the SSE to grant an interim Confidential or Secret clearance:

(1) 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.

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

(a) The individual has not had more than a 1 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;

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

(c) The SSE reviews the individual'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) Confirmation of a completed NAC which another Government agency used to grant the person a security

clearance for employment as or for a Government contractor, provided that:

(a) Not more than 1 year elapsed between the date that the clearance was last in effect and the beginning date of the person's FAA employment; and

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

d. The SSE shall not grant an interim clearance without reviewing the Standard Form (SF) 86, Questionnaire for National Security Positions, used to initiate the required investigation and conducting a subject interview.

e. As a matter of practice, M-70 rarely grants interim Top Secret clearances and does so only in exceptional cases. As much of the required investigation as possible shall be completed before this level of interim clearance is requested from M-70. An SSE receiving a request for an interim Top Secret clearance shall, upon determining that it is justified, forward it to ACO-300. The SSE shall include with the request copies of the SF-86 used to initiate the investigation, all available investigative information, and any other pertinent information. ACO-300 shall forward the request to M-70.

f. The SSE shall 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, the SSE, after checking on the status of the investigation and the information developed to date, may extend the period of time that the clearance remains in effect. A final clearance supersedes an interim clearance.

g. Upon being granted an interim clearance, the employee shall complete and sign the SF-312, Classified Information Nondisclosure Agreement, and receive the appropriate briefing. The SSE shall also 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. The SSE shall immediately terminate an interim clearance if the

investigative results do not warrant the granting of a final clearance.

1003. FINAL CLEARANCES.

a. An SSE may grant a final clearance when the required investigation has been completed and adjudicated and all other pertinent official records have been reviewed and evaluated. The SSE may also grant the clearance when OPM has sent FAA a substantially complete investigation, even though a minor portion is still pending, if in the adjudicator's opinion the completed portion clearly supports a favorable adjudication and the pending information is unlikely to raise a material issue or help to resolve one.

b. The investigative requirements for final clearances are:

(1) Confidential or Secret. National Agency Check, Inquiries, and Credit (NACIC) or higher level investigation with no subsequent break in service in excess of 1 year and completion of subject interview.

(2) Top Secret. Single Scope Background Investigation (SBI) with no subsequent break in service in excess of 1 year. In using a combination of other investigations, the adjudicator must determine that together they provide investigative coverage equivalent to that of an SBI.

1004. TEMPORARY CLEARANCES.

a. Temporary eligibility for access, referred to as a temporary clearance, may be granted 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.

b. The SSE may grant a temporary clearance to an individual who has met the requirements for an interim or final clearance, except that only M-70 may grant a temporary Top Secret clearance if the person does not have a current Background Investigation (BI) or SBI. When necessary, the SSE shall forward a request for a temporary Top Secret clearance to M-70 through ACO-300.

c. The SSE shall review a current, signed SF-86 from the individual before granting a temporary clearance.

d. The SSE shall grant a temporary clearance for a period of time not to exceed 6 months; but, if circumstances warrant, may then extend it for an additional period of time not to exceed a total of 1 year. The SSE shall establish a fixed date or event for expiration of the clearance. The access granted shall be limited to information related to a particular project or assignment.

e. When an individual is being granted a temporary clearance for access to another agency's classified information, that agency must concur before the FAA grants the access. The SSE shall take appropriate steps to ensure that the other agency concurs with the release of its classified information to an employee with a temporary clearance.

1005. CLEARANCE GRANTING PROCEDURES AND DOCUMENTATION.

a. Basic procedures.

(1) Personnel security officers and adjudicators shall make determinations regarding the granting of security clearances and shall use FAA Form 1600-54, Notification of Personnel Security Action, to document clearances granted. The Integrated Personnel and Payroll System (IPPS) normally produces this form but it may also be produced manually.

(2) Upon receipt of Form 1600-54, the SSE shall ensure that it accurately shows the following information:

(a) Level and date of clearance.

(b) Investigative basis and date of investigation.

(c) Position sensitivity.

(d) Date of last update investigation, if the employee is in a critical-sensitive or special-sensitive position.

(3) The personnel security officer or designated representative shall sign and date the Form 1600-54.

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

(5) The employee's supervisor shall give or arrange for the required security briefing and shall have the individual sign the SF-312, which is an agreement not to disclose to any unauthorized person any classified information the employee has access to during the time that he or she holds a security clearance and at all times thereafter. The supervisor or person providing the briefing shall sign as a witness to the employee's signature on the SF-312. The employee shall also sign the Form 1600-54, acknowledging that he or she has been granted a security clearance at the specified level.

(6) A person only needs to sign an SF-312 once, regardless of how many times he or she is granted a clearance. SSE's shall record in the IPPS those employees from whom the FAA has received a signed SF-312. If a person being granted a clearance has previously signed the SF-312, the SSE shall so inform the operating office.

(7) The operating office shall return the completed original Form 1600-54 and the SF-312, if applicable, to the SSE and shall retain Copy 2.

(8) The SSE shall retain the original of the Form 1600-54. It shall send to the Human Resource Management Division (HRMD) both Copy 3 and the SF-312 for placement in the employee's Official Personnel Folder (OPF).

b. Temporary and interim clearances.

(1) An employee being granted an interim or temporary clearance is required to sign the SF-312 and receive a security briefing. The SSE may document the clearance in a memorandum to the operating office in lieu of completing the Form 1600-54. It shall retain a copy of this memorandum in the PSF.

(2) Whenever an employee has been granted an interim or temporary clearance, the SSE shall convey that fact to any other agency that considers affording the employee access to its information. The SSE should include this information on DOT Form 1630.5, Visit Clearance, when processing a visit clearance request as stated in paragraph 306b.

c. Security briefings.

(1) Security briefings shall be given to all persons authorized access to classified information to ensure that they fully understand the requirements and procedures for protecting it, the specific hazards that may be expected, what to do if a compromise occurs, and their continued obligations after their clearances are terminated. (Refer to Appendix 8, Security Briefing Guidance for Access to Classified Information.)

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

1006. TERMINATING ACCESS AUTHORIZATIONS.

a. Administrative termination. The SSE shall administratively terminate an employee's security clearance whenever his or her FAA employment is terminated for any reason or when duty changes occur which eliminate the need for the clearance. When the latter situation exists, the employee's supervisor shall request termination of the clearance or reduction in the level of clearance, if appropriate. Clearance termination or reduction in level may require reassessment of the sensitivity level of the employee's position or redesignation of the position as nonsensitive.

b. Clearance suspension.

(1) Suspension of a clearance, also known as administrative withholding, is appropriate when a significant question of security fitness arises. Suspension

is warranted, for example, when the SSE receives information indicating possible gross misconduct, criminal conduct, substance abuse, or a serious breach of integrity.

(2) Clearance suspension is a temporary action and shall be in effect only while a question of security fitness is 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 may reinstate the clearance whenever it believes that this action is consistent with the interests of national security, even though the employee is still participating in a rehabilitation or similar program. However, the SSE is not required to do so when other FAA offices have determined that the employee is fit for duty. The SSE shall make every effort to complete all investigations expeditiously and obtain information necessary to make a final determination regarding an employee's clearance; and, when appropriate, shall reinstate a suspended clearance as soon as possible. When the SSE determines that a clearance should be revoked, it shall promptly begin the procedures to do so.

(3) When suspending clearances, SSE's shall ensure adherence to the clearance suspension procedures contained in Chapter 11, Adverse Security Actions.

(4) An SSE shall fully coordinate a clearance suspension with the employee's supervisor. While it is not necessary to inform the operating office in detail of the reason for a suspension, the SSE shall notify the office in writing that the clearance has been suspended and shall ensure that the employee is notified. As stated in paragraph 1102a, a clearance suspension exceeding 10 days requires written notice to the employee.

c. FAA Form 1600-25, Security Termination Statement. All persons vacating a sensitive position must sign FAA Form 1600-25, which constitutes a security debriefing. The official conducting the debriefing shall sign the form

as a witness. The completed form shall be returned to the SSE, which shall retain it for at least 1 year. This statement is not required when an employee transfers to another sensitive position within the FAA or when a clearance is suspended, but only when employment with FAA ends, a temporary clearance expires, or the individual permanently transfers to nonsensitive duties.

1007. 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 Sensitive Compartmented Information (SCI) are contained in Director of Central Intelligence Directive 1/14.

b. The Department of Energy (DOE) and the Nuclear Regulatory Commission establish access requirements for programs governed by the Atomic Energy Act of 1954, as amended. Order DOT 1630.2, DOT Personnel Security Program, Chapter XII, contains specific instructions regarding DOE Restricted Data clearances.

c. Order DOT 1630.2, Chapter XIII, contains procedures for obtaining North Atlantic Treaty Organization (NATO) access authorizations.

d. SSE's shall process requests for special access authorizations through ACO-300.

1008.-1099. RESERVED.

CHAPTER 11. ADVERSE SECURITY ACTIONS

1100. GENERAL. This chapter prescribes procedures which FAA personnel shall follow upon receipt of information about an employee or applicant which may result in an adverse security action. Such actions include denial, suspension, or revocation of a security clearance for access to classified information.

1101. PRELIMINARY ACTIONS.

a. Upon receipt of information which raises questions concerning the personnel security fitness of an individual, the personnel security officer shall immediately assess the security factors involved and shall recommend to the servicing security element (SSE) manager suitable action to ensure that national security interests are protected.

b. In making a recommendation, the security officer shall consider such factors as the conclusiveness and seriousness of the information developed, the employee's access to classified information, and the opportunity the position affords the employee to commit acts contrary to national security interests.

c. Under this chapter the SSE may suspend a security clearance. It may also recommend that the Director of Civil Aviation Security Operations (ACO-1) revoke or deny a security clearance.

d. The SSE and/or ACO shall consult with the Office of the Chief Counsel (headquarters cases) or Assistant Chief Counsel (region and center cases) prior to taking any action under this chapter which may result in an appeal under the FAA Appeals Procedure.

1102. SECURITY CLEARANCE DENIAL, SUSPENSION, AND/OR REVOCATION.

a. Suspension. If a decision is made to suspend a security clearance temporarily pending investigation to determine if revocation of the clearance is warranted, and the suspension exceeds 10 days, the SSE shall notify the employee in writing that it has suspended the clearance and

why, to the extent consistent with the interests of national security.

b. Post Suspension. After the security clearance is suspended, but prior to a determination on whether to reinstate or revoke it, management may, in its sole discretion: Restrict the employee to the nonsensitive duties of the position, temporarily reassign the employee to a nonsensitive position with the same grade and pay, or place the employee on administrative leave with pay. Administrative leave should be considered only if the other options are not viable.

c. Denial or Revocation.

(1) If, upon recommendation from the SSE, ACO-1 decides to deny or revoke a security clearance, it shall notify the individual in writing, to the extent consistent with the interests of national security, that the clearance is being denied or revoked and why. The explanation for the decision shall be as comprehensive and detailed as the national security interests of the United States and applicable laws permit. ACO-1 shall also notify the individual in writing that:

(a) The individual has 30 days from the date of the notification to submit a written response to ACO-1 with any supporting documentation, and/or to request the opportunity to appear personally before an ACO or SSE adjudicative authority;

(b) The individual may request an extension of the response time, but must do so in writing to ACO; and the granting of any extension is subject to ACO's discretion;

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

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

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

(2) If the employee or applicant submits a timely response, that response and any supporting documentation timely submitted shall be considered before making a final decision. If the individual asks to appear in person to respond to the denial or revocation decision, ACO shall provide that opportunity, at Government expense, and shall allow the individual to present any documentary or physical evidence as part of the response. All such evidence shall be considered before making a final decision. ACO shall make a written summary or recording of any such personal appearance and place it in the individual's personnel security file. The final decision shall be in writing and, in the case of a denial or revocation, shall notify the individual that:

(a) He or she may appeal the decision to the Personnel Security Review Board chaired by the Office of Security and Administrative Management (M-70), Office of the Secretary; and

(b) The review request must be in writing and must be submitted to M-70 within 30 days from the date of the final decision.

(3) The Personnel Security Review Board is established as required by Section 5.2(a)(6) of E.O. 12968, Access to Classified Information, and adjudicates final appeals originating in any DOT administration.

d. Post Denial or Revocation.

(1) After the procedures outlined in 1102c have been completed and a security clearance has been revoked, the SSE shall provide the HRMD and/or the operating office all information necessary to take appropriate action under the FAA's Personnel Management System. Such action may include removing the employee or permanently reassigning the employee to a nonsensitive position. When an employee is removed, the HRMD shall inform the SSE.

(2) After the procedures outlined in 1102c have been completed and a security clearance has been denied:

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

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

1103. EMPLOYMENT OF INDIVIDUALS PREVIOUSLY SEPARATED FOR SECURITY REASONS. No person who has been separated from employment with any department or agency of the U.S. Government under any Federal security program (such as 5 U.S.C. Sections 7531-33, E.O. 9835, or E.O. 10450) may be employed in the FAA without prior approval of the Secretary and determination by the HRMD that the factors leading to the separation are not currently disqualifying for FAA employment. When employment of such a person is proposed, the personnel security officer concerned shall obtain complete information regarding the basis for the separation, ensure appropriate investigation of the person's subsequent activities, ascertain whether the HRMD has determined that the person is eligible for FAA employment, and obtain any other information the Secretary needs to decide whether or not the person's employment is clearly consistent with the interests of national security.

1104.-1199. RESERVED.

CHAPTER 12. ACCESS TO AUTOMATED INFORMATION SYSTEMS

1200. GENERAL.

a. Under Office of Management and Budget Circular Number A-130, Management of Federal Information Resources, dated December 12, 1985, agencies must establish and manage personnel security policies and procedures to ensure an adequate level of security for Federal automated information systems (AIS). The Office of Personnel Management prescribes guidance for agency policies and procedures for AIS security which apply to all Federal employees. Policies established and maintained by agencies are to include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those persons having access to sensitive data.

b. The Computer Security Act of 1987 (Public Law 100-235) requires Federal agencies to identify each computer system that contains sensitive information and to prepare a plan for the security and privacy of each such system. P.L. 100-235 defines sensitive information as any information which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive data at FAA also include proprietary data.

c. FAA Order 1600.54, FAA Automated Information Systems Security Handbook, establishes FAA's AIS security program and provides detailed guidance to ensure that an appropriate level of AIS security is implemented throughout FAA's data processing activities.

d. Personnel security is an integral part of AIS security in order to ensure sufficient protection for AIS and their data. Chapter 5, Position Sensitivity and Risk Level Designation and Controls, and Appendix 3, Position

Risk and Sensitivity Level Designation Process, contain procedures for designating position risk levels commensurate with duties and responsibilities involving AIS. This chapter contains personnel security requirements and procedures for AIS access. Because of the nature of AIS and the ease with which large amounts of data can be retrieved, manipulated, and deleted, access requirements are in some cases more stringent than for the same level of data contained in records systems outside AIS.

1201. ACCESS REQUIREMENTS.

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

b. Level I data. Any employee granted access to an AIS containing Level I data, classified national security information, shall first have the appropriate level security clearance.

c. Level II data.

(1) Any employee granted access to that portion of an AIS containing Level II data shall first have at least a completed National Agency Check (NAC). Level II data are sensitive but unclassified data.

(2) An employee may be appointed to a sensitive or public trust position requiring AIS access to Level II data without the required investigation, provided that the preappointment investigative requirement is waived in accordance with paragraphs 611 or 612. The investigation will normally have been initiated by the time the employee enters on duty. In such a situation, and in order to avoid unnecessary delays in allowing the employee to perform all of his or her duties fully, the servicing security element (SSE) shall notify the operating office as soon as major portions of the NAC are completed and favorably adjudicated. Major portions would include the Security Investigations Index (SII) check, the Federal Bureau of Investigation name check, and the fingerprint check. In the case of unclassifiable fingerprints, a records check by name only is acceptable for this purpose. Unless the investigation has

revealed unfavorable information not previously known and favorably adjudicated, the SSE need not wait for other portions of the NAC, such as the Defense Central Investigations Index (DCII) check, to be completed before granting AIS access. While an NAC is in progress on an employee awaiting Level II access, the SSE shall periodically inquire of OPM, either electronically or by telephone, as to its status. It shall do so as often as is reasonable to ensure that there is not undue delay in adjudicating for access once major portions of the NAC are complete.

d. Level III data. For an employee in a position requiring AIS access only to Level III data, those which are unclassified and nonsensitive, there are no investigative requirements beyond those otherwise associated with the position.

1202. PROCEDURES.

a. When a person is appointed to a position identified as an AIS position for which Level I or II access is required, the SSE shall notify the operating office as to whether or not the employee meets the investigative requirements for access to the applicable level(s) of information in an AIS. If Level I access is required and the employee does not have the required security clearance, AIS access shall await at least the granting of an interim clearance that would allow access to the level of classified information the AIS contains. If Level II access is required and the employee does not have a completed and favorably adjudicated NAC, the SSE shall expedite completion of the NAC and notify the operating office when the requirement has been met. Advance reports of NAC's shall be requested when possible.

b. For access to Level II data, the SSE shall use the suitability criteria for adjudicating results of an NAC. When unfavorable information is developed which the SSE determines precludes granting AIS access pending completion of the investigation, the SSE shall coordinate with the operating office management regarding the delay in granting access.

c. No employee on whom the required investigation has been completed shall be denied access to any level of data in an AIS based on information developed during the investigation without being provided due process as specified in paragraph 202a.

d. When the required investigation has been completed, the results of the suitability adjudication process shall determine whether or not the employee receives access to Level II data.

1203.-1299. RESERVED.

CHAPTER 13. FOREIGN ASSIGNMENTS AND TRAVEL

1300. GENERAL. Special safeguards are required to protect the national interest and national security information when FAA personnel and representatives are given foreign assignments or perform official foreign travel. For this purpose, a "foreign" location means outside the 50 states, the District of Columbia, Puerto Rico, the Canal Zone, 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. FAA personnel 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.

1301. 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 a mission through permanent change of station must hold Secret clearances.

(2) All foreign positions shall be designated at least critical-sensitive, and persons selected for these positions shall have at least a completed and favorably adjudicated Background Investigation (BI) prior to transfer to the foreign location.

(3) When an employee is being assigned to a foreign duty location, the SSE shall transmit the security clearance data to the appropriate DOS regional security officer (RSO) or post security officer (PSO). The SSE may do so either by electronic message directly to the RSO or PSO or by providing the data to the Personnel Security/Suitability Division, Employee/Contractor Branch (DSS/ICI/PSS/EC), Bureau of Diplomatic Security, Department

of State, Washington, DC, 20520, for transmission to the post.

b. Personal service contract (PSC) personnel. U.S. citizens who are family members of U.S. personnel stationed in foreign countries, and who are technically PSC employees under arrangements made through DOS, are not required to hold security clearances if their employment will not require them to have access to classified information or to sensitive areas at locations which receive, process, or store classified or other foreign policy or operationally sensitive information or material. A National Agency Check and Inquiries (NACI) is the minimum required investigation for these positions. The SSE is responsible for granting any security clearances necessary for persons in these positions.

c. Temporary duty (TDY).

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

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

(3) There is no requirement that an employee on TDY to a foreign location have a security clearance. However, DOS regulations prohibit an employee on TDY who does not have a clearance from having unescorted access to U.S. Government facilities. While there is no specific clearance requirement to visit FAA offices located in foreign countries, provided access to classified information is not required, an employee requiring access to an office located in an embassy or embassy annex must be escorted if he or she does not have at least a Secret clearance.

(4) When an employee is scheduled for TDY to a foreign location, the operating office should determine whether or not a clearance will be required for the work the employee will be doing and/or to avoid major inconvenience due to lack of unescorted access to FAA or other Government agency offices. In making this determination, the office

should consider such factors as the nature of work to be performed; the extent, nature, and location of contacts with FAA and other Government officials; and the length of the TDY. In many cases, not being allowed unescorted access for one visit to an office or embassy in a foreign location will cause an employee no significant inconvenience.

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

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

(7) SSE's shall transmit clearance data for employees going on TDY, as necessary, as stated in paragraph 1301a(3) above.

d. International conferences.

(1) Head of a delegation. Any FAA employee selected to head a delegation from the United States to an international conference on other than a one-time basis shall be subject to a 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 help represent FAA at an international conference, the FAA office arranging for the advisor's services shall contact its SSE at least 3 weeks prior to the date that the delegation is scheduled to

depart. The SSE shall then determine if an NAC has already been conducted on the industry representative, as may be the case, for example, if the person holds a Government security clearance or is a military reservist. If an NAC has not been completed, the SSE shall furnish the responsible office the forms for the person to complete. The office shall then ensure that they are completed and returned to the SSE, after which the SSE shall process the NAC. An 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 shall ensure in advance that it requests the SSE to process any special clearance(s) required. The office should ask about clearance requirements when making the visit arrangements and provide its request to the SSE at least 3 weeks in advance of the visit to allow time for processing.

1302.-1399. RESERVED.

CHAPTER 14. SECURITY CLEARANCES AND AUTHORIZATIONS FOR ALIENS

1400. GENERAL. Aliens shall be identified as either foreign nationals or as immigrant aliens. (See definitions in Appendix 1, Glossary.) Foreign nationals are not eligible for FAA security clearances but may be granted Limited Access Authorizations. When special compelling circumstances warrant a broader "need-to-know," they may be processed for DOT security clearances. The Director, Office of Security and Administrative Management (M-70), Office of the Secretary, is authorized to grant Limited Access Authorizations and security clearances to noncitizens. This authority is not further delegated.

1401. INVESTIGATIVE REQUIREMENTS FOR ALIENS. A Background Investigation (BI) which 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.

1402. PROCEDURES FOR LIMITED ACCESS AUTHORIZATIONS.

a. When the servicing security element (SSE), after consultation with the Office of Civil Aviation Security Operations (ACO), has determined that specific classified information is releasable to the alien concerned, the office proposing use of the alien's services shall submit a request for a Limited Access Authorization for him or her. The request shall identify the information involved and the level of its classification. The requesting office shall 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 request, accompanied by the forms required for a BI, shall be directed through the SSE and ACO to M-70, which will arrange for the investigation. When the investigation has been completed and adjudicated, M-70 will notify the requesting office through ACO and the SSE.

c. Persons to whom Limited Access Authorizations are granted are subject to the same security briefing and debriefing requirements as for a security clearance.

1403. PROCEDURES FOR IMMIGRANT ALIEN SECURITY CLEARANCES.

a. When employment of an immigrant alien in a sensitive position is desired and use of a Limited Access Authorization is impracticable, the office proposing use of his or her services shall submit a request for the processing of a security clearance. The request shall explain why the clearance is needed and shall state the specific tasks or projects on which the person will be working.

b. The requesting office shall determine that the 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 shall ensure that the person has valid immigrant alien status.

d. The request, accompanied by the forms required for a BI, shall be directed through the SSE and ACO to M-70, which will arrange for the investigation. When the investigation is completed and favorably adjudicated, M-70 will notify the requesting office through ACO and the SSE.

e. M-70 may issue an interim Secret or Confidential clearance to an immigrant alien based on the completion of a favorable National Agency Check (NAC) pending completion of the BI. When the investigation is completed, M-70 may 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 clearance shall be revoked and the person shall be considered to have reverted to foreign national status. M-70 may authorize extension of the time limit if it concludes that the delay is due to reasons beyond the person's control.

1404. APPROVAL FOR VISITS BY FOREIGN NATIONALS CLEARED BY OTHER AGENCIES. No FAA office shall accept security clearances for foreign nationals granted by other U.S. Government agencies for visits, conferences, or other purposes without approval from M-70. The office involved shall present justification to and request approval from M-70 through the SSE and ACO.

1405.-1499. RESERVED.

CHAPTER 15. NATIONAL EMERGENCY PERSONNEL SECURITY PROCEDURES

1500. PURPOSE. This chapter provides authority and procedures for planning and conducting personnel security operations in FAA under national emergency conditions, under a major attack upon the United States, and under lesser national emergency conditions which make it impossible or impracticable to follow normal personnel security procedures.

1501. ACTIVATION OF STANDBY PROCEDURES.

a. The following standby procedures shall be activated FAA-wide without further justification if there is a major attack upon the United States which causes serious disruption of all types of communication.

b. These procedures shall be activated FAA-wide upon receipt of notice from the Secretary of Transportation that the Office of Personnel Management (OPM) has temporarily deferred or discontinued conducting the investigations required by E.O. 10450.

c. These procedures shall be activated within prescribed FAA organizations or in specific geographical areas which the Assistant Secretary for Administration, DOT, so specifies, based on a decision that 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.

1502. STANDBY PROCEDURES: MODIFICATION OF INVESTIGATIVE REQUIREMENTS. The Secretary of Transportation delegates special authority needed to continue personnel security operations under national emergencies. Upon notification that these standby procedures have been activated, the following deviations from normal personnel security investigative requirements are authorized:

a. Authority to fill sensitive positions. FAA personnel security officers may authorize filling of

special-sensitive, critical-sensitive, and noncritical-sensitive positions for a limited period without the required preplacement investigation, provided that they:

(1) Obtain such existing investigations and/or conduct such investigation as may be practicable under the circumstances to afford the maximum feasible protection of national security interests;

(2) To the extent practicable under the circumstances, complete as many of the requirements for waiver of preplacement investigations, specified in paragraph 611, as possible; and

(3) Initiate the required investigations as soon as conditions permit, furnishing to OPM any investigative information already developed.

b. Authority to defer investigation for nonsensitive positions. FAA personnel security officers may authorize that the National Agency Check and Inquiries (NACI) investigation for nonsensitive positions be deferred and require only such investigation that they determine is feasible under the circumstances.

c. Authority to grant clearances on modified investigative requirements. FAA personnel security officers shall evaluate information developed in interim investigations using the personnel security standards and criteria contained in this order and shall record their determinations. On the basis of the interim investigations, they may 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. These clearances shall be superseded and discontinued when the required investigations are completed and adjudicated.

1503. REQUIRED PLANS FOR PERSONNEL SECURITY OPERATIONS DURING A NATIONAL EMERGENCY. Plans for personnel security operations under national emergency conditions shall provide for the following:

a. Designation and training of primary and alternate personnel 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 prepositioning 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.

1504.-1599. RESERVED.

APPENDIX 1. GLOSSARY

Access. The ability and opportunity to obtain knowledge of classified information.

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

Appointing/approving official. The individual delegated the authority to effect appointments, reassignments, promotions, separations, or similar personnel actions regarding FAA employees or applicants.

Background investigation. Any personnel investigation conducted to meet personnel security program requirements.

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

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.

Contracting officer. An official who has authority to enter into and/or administer contracts and make determinations or findings with respect to those contracts.

Contractor employee. A person employed as or by a contractor, subcontractor, or consultant to the FAA.

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.

FAA employee. Any person employed directly by the FAA.

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

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

Integrated Personnel and Payroll System (IPPS). An automated information system for documenting and retaining personnel, budget, training, labor relations, civil rights, and security data on present and former DOT employees.

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

Limited Background Investigation (LBI). An investigation consisting of an NAC, 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.

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.

Local Agency Check (LAC). A check of records at a state or local law enforcement agency.

Minimum Background Investigation (MBI). An investigation consisting of a National Agency Check and Inquiries (NACI), a credit search, and telephone inquiries to follow up on written inquiries not returned.

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

National Agency Check and Inquiries (NACI). An investigation consisting of an NAC, written inquiries, and record searches covering specific areas of a person's background during the most recent 5 years.

National Agency Check, Inquiries, and Credit (NACIC). An investigation consisting of an NACI and a credit search.

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

National security position. A position involving Government activities concerned with the protection of the national security.

Operating office. A line of business, an office or service in headquarters, or a division level organization in a region or center.

Periodic Reinvestigation - SBI (PRIS). An investigation updating a Single Scope Background Investigation (SBI) and consisting of personal interviews of the subject and sources, an NAC, credit search, and written inquiries and record searches covering specific areas of a person's background during the most recent 5 years.

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

Personnel 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.

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.

Personnel security adjudicator. An individual in the servicing security element (SSE) who conducts security adjudication.

Personnel security coordinator. An employee of an operating office assigned to coordinate personnel security functions among his or her organization, its SSE, and its Human Resource Management Division.

Personnel security officer. A specifically appointed individual within an SSE who is primarily responsible for management and operation of the personnel security program.

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

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

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

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

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

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

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

Selecting Official. The supervisory official within an operating office who has the authority to decide on the selection of individuals or to propose adverse action against individuals under his/her supervisory jurisdiction.

Servicing security element (SSE). The headquarters, region, or center organizational element which is responsible for providing security services to a particular activity.

Single Scope Background Investigation (SBI). An investigation consisting of an NAC, 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.

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

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

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

Upgrade Investigation (UGI). An investigation consisting of an NAC, 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.

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.

APPENDIX 2. PERSONNEL SECURITY COORDINATOR RESPONSIBILITIES

The responsibilities of personnel security coordinators are as follows:

1. Be familiar with the policies and requirements of this order.

2. Maintain liaison for their organization with their Human Resource Management Divisions (HRMD) and their servicing security elements (SSE).

3. Assist the SSE in determining the risk or sensitivity level of each position in their 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. Assist their organization's management in arranging for briefings when employees are granted security clearances, and debriefings when employees leave or their clearances are terminated.

6. Maintain security clearance rosters on personnel in their organizations.

7. Promptly notify their SSE regarding visits by employees of their organization to other FAA facilities and to other agencies when security clearance certifications will be required prior to the visits.

8. Advise their SSE regarding proposed details of persons to their organization whenever the details are to sensitive or public trust positions; and notify their SSE when such details end.

9. Assist their organization's management in notifying their SSE about any questionable employee conduct or activity which would raise a security or suitability issue.

10. Promote within their organization an understanding of the personnel security program's purpose and requirements.

11. Keep the head of their organization informed of substantive problems affecting their implementation of the personnel security program.

12. Recommend to the SSE any new or modified procedures or policies believed to be in their organization's best interest.

APPENDIX 3

POSITION RISK AND SENSITIVITY LEVEL DESIGNATION PROCESS

1. General. The process specified in this appendix provides a systematic way of uniformly designating position risk and sensitivity levels. The following paragraphs explain how to determine general risk criteria for placement of FAA programs and positions; how to apply suitability, automated information systems (AIS) and national security criteria for designating positions; and how to determine a final risk or sensitivity level. They also contain specific program placements for offices and divisions at the regional level and minimum risk and sensitivity level requirements for certain FAA positions.

2. FAA Form 1600-59. FAA Form 1600-59, Position Risk/Sensitivity Level Designation Record (figure 1), is explained in paragraph 505 of this order. It shall be used to record, as applicable, the specific steps in the designation process as outlined in this appendix.

3. Sensitivity level designation.

a. As stated in paragraphs 500 and 504 of this order, all positions requiring access to classified information, and therefore having national security duties, are sensitive positions and shall be designated as either noncritical-sensitive, critical-sensitive, or special-sensitive. Listed below are the minimum sensitivity levels for positions requiring access to specific levels of classified information. The level of access which makes a position sensitive shall be recorded as a final adjustment factor (block IV) on the FAA Form 1600-59.

(1) Positions requiring access to Confidential or Secret information shall be designated at least noncritical-sensitive.

(2) Positions requiring access to Top Secret information shall be designated at least critical-sensitive.

(3) Positions requiring access to Sensitive Compartmented Information (SCI) shall be designated special-sensitive.

b. All clerical positions at the branch level and below in the Office of the Associate Administrator for Civil Aviation Security (ACS), including regional and center Civil Aviation Security Divisions, shall be designated at least noncritical-sensitive. All other ACS positions shall be designated at least critical-sensitive, regardless of the level of access to classified information that may be required. When applicable, these criteria shall be recorded as final adjustment factors on the FAA Form 1600-59.

c. When it is apparent that the risk level criteria described below would not affect a sensitivity level determination that is based on access to classified information or employment in ACS, the designation process need not consist of anything other than recording on the FAA Form 1600-59 the reason(s) for the designation. For example, if a position requires access to SCI, it will automatically be special-sensitive regardless of other risk factors involved.

4. Risk level designation. The risk level designation process consists of designating each agency program for its impact and scope as related to the efficiency of the service, 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.

a. Program placement. Procedures for determining program placement are as follows:

(1) 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 shall be one of the following:

(a) Accounting for, auditing, or disbursement of public funds;

(b) Administrative, regulatory, or policy control over public and/or private programs or operations;

(c) Protection of the national security;

(d) Enforcement of Federal laws; or

(e) Protection of life or property.

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 Governmentwide, to all sectors, with primary focus on the public sector Governmentwide.	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				

(2) 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.

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

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

b. Position risk points and tentative risk level. In determining position risk points, the position's duties and responsibilities shall be considered in the context of the program and the risk the position has for damage or abuse to the program. The procedure requires a determination of the degree of impact on the program of each of five risk factors and the assignment of points to each risk factor. The sum of the risk points and the program placement combine to determine the tentative risk level. Specific procedures are as follows:

(1) 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.

(2) 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.

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

(4) 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 B

RISK FACTOR DESCRIPTIONS

DEGREE	DEGREE OF PUBLIC TRUST: The consensus of confident expectation for honesty, integrity, reliability, responsibility, or justice placed in a position.	FIDUCIARY MONETARY RESPONSIBILITY: Authority or ability to obligate, control, or expend public money or items of monetary (bonds, etc.) value.	IMPORTANCE TO PROGRAM: Impact the individual position has, due to status, in or influence on the program as a whole, either individually or collectively.	PROGRAM AUTHORITY: Ability to manipulate authority or control the outcome or results of all or key portions of a program or policy.	SUPERVISION RECEIVED: 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 in the 7 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 reivew of policy and major operational considerations 5 of work by superior, with some knowledge 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 issues by superior with technical 3 program expertise.
LIMITED: Potential for damage not meeting above criteria.	1	1	1	1	Close Technical: 1 Continuing review of all phrases 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	34-36
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 AND TYPE OF BACKGROUND INVESTIGATION

c. 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.

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

(a) Special investigative or criminal justice duties.

(b) Control of an automated monetary system (key access entry).

(c) Few-of-a-kind positions with special duties, such as special assistant to the Administrator.

(d) 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.

(e) Any other factors believed relevant, provided they are documented.

(2) 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:

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

(b) 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.

(3) **Final adjustment.**

(a) Any decisions on adjustment should be made only after careful analysis of positions in terms of any uniqueness or uniformity factors that may apply. The persons designating positions shall document all adjustment factors on FAA Form 1600-59.

(b) In order to ensure uniformity and consistency in risk level designations, ACO-300 shall assist regions and centers as necessary in reviewing position descriptions for positions common in more than one region or center. When doing so, ACO-300 shall coordinate with headquarters offices and services as needed, particularly for straightlined organizations.

5. AIS positions.

a. Risk level criteria for positions involving access to AIS are an integral part of risk and sensitivity level designation. In addition to any public trust or national security criteria that may apply, the following criteria shall apply to any position with AIS duties and responsibilities:

(1) High risk. Includes any position at the highest level of risk to an AIS. This is to include positions in which the incumbent is responsible for the planning, direction, and implementation of an AIS security program; has a major responsibility for the direction, planning, and design of an AIS, 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 AIS security programs, including direction and control of risk analyses and/or 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 AIS which 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 an AIS of (1) dollar amounts of $10 million per year or greater or (2) lesser amounts if the activities of the individual 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/or 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. Includes positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of an AIS, and whose work is technically reviewed by a higher authority at the high-risk level to ensure the system's integrity. Such positions may involve:

(a) Responsibility for systems design, operation, testing, maintenance, and/or 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/or 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 AIS and not just to information contained in a personal computer or local area network. The nature, extent, and volume of the information shall be considered in applying this criterion.

2 Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less then $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. Includes all AIS positions not falling into one of the above risk levels.

b. As positions with AIS duties and responsibilities may also involve determinations under the procedures in paragraph 4 of this appendix, the higher of the levels determined applying both that paragraph and this one shall be used as the final risk level. If the position is sensitive because of national security responsibilities, a determination of high risk under the AIS criteria shall result in a designation of at least critical-sensitive. Adjustments due to AIS criteria shall be recorded on Form 1600-59 as final adjustment factors.

c. Positions in the following job series shall be designated as AIS positions and coded as such as stated in paragraph 506 of this order: 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 AIS responsibilities, such as personnel responsible for AIS security, shall also be designated as AIS positions. Duties involving use of a computer or access to an AIS, by themselves, do not automatically make a position an AIS position.

6. MINIMUM LEVELS FOR CERTAIN POSITIONS. Because of uniqueness, special responsibilities, or the need for uniformity throughout the FAA, positions in the following categories shall be designated at least at the risk levels shown, regardless of the level determined under the other criteria and procedures of this appendix. The coding corresponds to that shown in paragraph 506 of this order.

Category of Position	Position Risk Level (Code) Shall be at Least
a. Executive System or a comparable pay level.	6
b. Executive Development Program.	6
c. Employee responsible at the national headquarters level for the development and/or approval of national plans, policies, or programs for continuity of FAA operations during national emergencies.	6
d. Manager responsible for the conduct of accident investigations and/or the enforcement standards through the certification/inspection process.	5
e. Division or comparable level manager at a region or center, or an office or service director at headquarters.	6
f. 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.	6

Category of Position	Position Risk Level (Code) Shall be at Least
g. Imprest fund cashier or alternate cashier responsible for a fund in excess of $20,000.	6
h. Imprest fund cashier or alternate cashier responsible for a fund in excess of $2,000 but no more than $20,000.	5
i. 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.	6
j. 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.	5
k. Budget officers in headquarters, regions, and centers.	6

Category of Position	Position Risk Level (Code) Shall be at Least
1. Budget analysts in headquarters, regions, and centers.	5
m. Employee 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.	6

7. REGIONAL LEVEL PROGRAM PLACEMENTS. To ensure uniformity throughout the FAA in designating positions common in more than one region, program placement designations for offices and divisions at the regional level, as described in paragraph 4a of this appendix, should be as follows unless circumstances unique to a region dictate that a program should be at a higher level. To the extent that these programs exist at centers on a scale comparable to that of a region, the stated levels would apply there as well.

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	Limited
l.	Public Affairs	Moderate
m.	Regional Administrator and immediate staff	Moderate
n.	Regional Operations Center	Moderate
o.	Resource Management	Limited
p.	Security	Moderate

8. REGIONAL LEVEL POSITIONS. The following are some positions common in most regions which should be designated at least at the levels shown. Other criteria and procedures in this appendix may require a higher level designation or designation as a sensitive position. Regional considerations may also dictate that a position warrants a higher designation because of other duties unique to that position in a particular region. Regions should 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 506 of this order.

Position	Risk Level (Code)
a. Air Traffic:	
(1) Air Traffic Control Specialist (Center), GS-9	1

(2) Air Traffic Control Specialist (Terminal), GS-9 5

(3) Air Traffic Control Specialist (Flight Service Station), GS-9 1

(4) Air Traffic Assistant, GS-7 1

b. Aircraft Certification:

(1) Manager, Technical Support Staff, GM-14 1

(2) Aerospace Engineer, GS-12/13/14 5

(3) Aerospace Engineer, GS-11 and below 1

(4) Aviation Safety Inspector, GS-12 and above 5

(5) Aviation Safety Inspector, GS-11 1

c. Airports:

(1) Manager, Planning, Programming Capacity Branch, GM-15 5

(2) Manager, Airports District Office, GM-14/15 5

(3) Program Officer, GS-13 5

(4) Airport Certification Safety Inspector, GS-13 5

(5) Program Analyst, GS-12 1

d. Airway Facilities:

(1) Engineer, GS-12 and above (all disciplines) 5

(2) Airway Transportation Systems Specialist, GS-11 and above 5

(3) Engineering Technician, GS-11 and above 5

(4) Electronics Technician, GS-11 and above 5

(5) Electronics Technician, GS-9 and below 1

(6) Systems Management Office Manager, GS-15 5

(7) Program Support Unit Manager, GS-14 5

e. Assistant Chief Counsel:

(1) General Attorney, GS-11/12/13/14 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 1

h. Flight Standards:

(1) Aviation Safety Inspector, GS-12/13/14 5

(2) Aviation Safety Inspector, GS-11 1

i. Human Resource Management:

(1) Employment Branch Manager 1

(2) Personnel Staffing, Position Classification, Employee Development, Employee Relations, and Labor Relations Specialists 1

(3) Drug Program Coordinator, GS-12 5

(4) Assistants and Clerical personnel working with the employee drug program 5

(5) Employee Relations Specialist (Employee Assistance Program) 5

j. International Affairs: International Aviation Specialist, GM-14 5

k. Logistics: All positions, unless other criteria in this appendix apply 1

l. Public Affairs:

(1) Public Affairs Specialist 5

(2) Writer/Editor 1

m. Regional Administrator and Support Staff: Secretary to Deputy Regional Administrator 5

n. Regional Operations Center: Regional Duty Officer 5

o. Resource Management:

(1) Supervisory Computer Systems Analyst, GS-12 and above 6

(2) Computer Specialist, GS-9 5

(3) Computer Assistant, GS-7 1

p. Security: Other criteria apply to all positions

APPENDIX 4. PERSONNEL SECURITY FORMS

Form Number	Form Name, National Stock Number, Unit of Issue, Supply Source
SF-85	Questionnaire for Nonsensitive 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.
OFI 79, 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 5. FORMS REQUIRED FOR INVESTIGATIONS

1. General. This appendix specifies the forms to be submitted to the Office of Personnel Management (OPM) to initiate personnel security investigations, and contains additional instructions for their completion and submission.

2. Required forms. The risk or sensitivity level of the position which a person occupies, or for which he or she is under consideration, determines which forms OPM requires for an investigation. The specific type of investigation being requested does not affect which forms are needed. The required forms are as follows:

a. Low-risk positions:

(1) Standard Form (SF) 85, Questionnaire for Nonsensitive Positions, if the person is a Federal employee or applicant.

(2) SF-85P, Questionnaire for Public Trust Positions, if the person is a contractor employee or applicant.

(3) 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.

(4) SF-87, Fingerprint Chart, if the person is a Federal employee or applicant.

(5) FD-258, FBI Fingerprint Chart, if the person is a contractor employee or applicant.

(6) Employment application, if the person is a Federal employee or applicant and the investigation is in conjunction with an appointment action.

(7) Optional Form (OF) 306, Declaration for Federal Employment.

b. Moderate-risk and high-risk positions:

(1) SF-85P, Questionnaire for Public Trust Positions.

(2) SF-86A, Continuation Sheet for Questionnaires SF-86, SF-85P, and SF-85, 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.

(3) SF-85P-S, Supplemental Questionnaire for Selected Positions, if OPM has granted the FAA approval to use the form for the position in question.

(4) SF-87, Fingerprint Chart, if the person is a Federal employee or applicant.

(5) FD-258, FBI Fingerprint Chart, if the person is a contractor employee or applicant.

(6) Employment application, if the person is a Federal employee or applicant and the investigation is in conjunction with an appointment action.

(7) OF-306, Declaration for Federal Employment.

c. Noncritical-sensitive, critical-sensitive, and special-sensitive positions:

(1) SF-86, Questionnaire for National Security Positions.

(2) SF-86A, Continuation Sheet for Questionnaires SF-86, SF-85P, and SF-85, 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.

(3) SF-87, Fingerprint Chart.

(4) Employment application, if the investigation is in conjunction with an appointment action.

(5) OF-306, Declaration for Federal Employment, if the investigation is in conjunction with an appointment action.

3. Additional required information for contractor employees: When FAA requests an investigation on a contractor employee or applicant, OPM may request answers to additional questions to supplement those on an SF-85 or SF-85P. As necessary, ACO-300 shall transmit to the servicing security elements (SSE) information about these OPM requirements.

4. Completion of forms.

a. All forms shall be typewritten or clearly printed.

b. All forms shall be completed following any instructions that accompany them. The SSE and/or the Human Resource Management Division (HRMD) shall accept only complete forms, with all required information shown. Forms are not acceptable unless signed and dated.

c. Forms which require a person to list employment, education, and/or residence history are not acceptable unless they 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 shall account for all periods of time within the past 7 years.

d. The employee or applicant shall completely answer all questions on a form, even if he or she previously furnished some of the information requested, such as employment history, on a form that was used to conduct an earlier investigation. Only the SSE may make exceptions to this requirement, and then only with OPM's consent.

e. The following requirements apply to the amendment of forms already provided to an HRMD or SSE:

(1) If an HRMD or SSE employee reviewing a form observes that it is not properly completed, he or she may return it to the person being investigated to provide all required information. HRMD's and SSE's should follow this procedure whenever possible. If the person being investigated is not at the same location as the SSE or HRMD and circumstances do not allow sufficient time to return it to him or her, the HRMD or SSE official may 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) Certain items on an SF-85, SF-85P, SF-85P-S, or SF-86 may be amended only by the person being investigated or by an HRMD or SSE official through use of OPM Form FIPC 391, Certification of Amended Investigative Form. The form lists the items to which this requirement applies. An amended SF-85, SF-85P, SF-85P-S, or SF-86 is not acceptable unless the person being investigated has initialed and dated all changes to any specified items or unless an HRMD or SSE employee has certified the changes on the FIPC 391.

(3) Changes the HRMD or SSE makes to items other than those specified on the FIPC 391 shall be verified by the initials of the person making the change, the date when the change was made, and the Security Office Identifier (SOI) or Submitting Office Number (SON) code.

(4) Under no circumstances shall anyone other than the person being investigated alter or amend any information that the person is required to furnish on an investigative form unless the change or addition is certified as stated above. Changes include re-dating a form or a release of information portion of a form.

f. Fingerprints for the SF-87 and FD-258 shall be taken only by a person trained to do so. Both the person being printed and the person taking the prints shall sign the form. The person taking the prints shall note in the appropriate block any missing fingers and any scars.

g. The SF-85, SF-85P, SF-85P-S, and SF-86 shall not be submitted to OPM unless they have been signed and dated within the previous 120 days. If a completed form is over 120 days old, the person who completed it may re-sign it, re-date it, and make any necessary changes to make it acceptable for submission.

5. Originals and copies. For all of the forms except the employment application and the OF-306, the SSE shall submit the original of the form only. For all investigations on

Federal employees and applicants, it shall submit a copy of the latest available employment application.

6. Additional documents.

a. If the FAA has conducted any kind of preliminary investigation, such as local law enforcement checks or a portion of a National Agency Check (NAC), the SSE shall furnish the investigative results to OPM with the other required forms.

b. When requesting a Reimbursable Suitability Investigation (RSI), the SSE shall send to OPM a request memorandum and any new or additional information developed that was not available to OPM when it completed the original investigation.

7. Where to submit forms. All forms required for the requested investigation, and any additional documentation, as appropriate, shall be submitted in one package to OPM, Federal Investigations Processing Center (FIPC), Boyers, Pennsylvania 16018.

APPENDIX 6

SUITABILITY ADJUDICATION PROCEDURES

A. GENERAL.

(1) FAA personnel shall use the procedures in this appendix as a guide when adjudicating suitability as prescribed in Chapter 8, Suitability Adjudication, and when applying the suitability standard, criteria, and additional considerations listed in paragraph 401.

(2) Adjudicators are not required to follow precisely the procedures listed in paragraphs E, F, and G of this appendix. They are based on the Office of Personnel Management's (OPM) adjudication procedures, which OPM has used to ensure consistency and fairness in its adjudications and which have resulted in many determinations that have been sustained when appealed. Adjudicators shall use good judgment in all adjudications, especially in any cases where they wish to depart from the procedures in this appendix. They shall be able to demonstrate that whatever procedures they use are fair to applicants and employees, sufficiently protect the FAA's interests, and result in adjudications that are consistent when applied to different individuals under similar circumstances.

(3) In suitability adjudication, adjudicators shall consider only those factors and issues pertinent and relevant to a person's suitability. They shall not allow other factors, such as a person's qualifications or agency hiring pressures, to influence their decisions.

B. APPLYING SUITABILITY CRITERIA. Suitability adjudicators shall consider the following when applying the suitability criteria listed in paragraph 401b.

(1) **Misconduct or negligence in prior employment which 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.** The misconduct or negligence need not have resulted in dismissal from employment. If dismissal occurred, the

adjudicator should place primary emphasis on the act or conduct which prompted the dismissal rather than on the mere fact of dismissal.

(2) **Criminal or dishonest conduct related to the duties to be assigned to the person or to that person's service in the position or the service of other employees.**

(a) In reviewing criminal conduct, the adjudicator should give primary consideration to the nature of the conduct, evidence of rehabilitation, and the effect such conduct may have on the efficiency of the service. The facts and circumstances of the behavior should be considered in all adjudications, even when the person was not formally convicted of a criminal offense, as in situations when charges were dropped or when a court placed the person on probation without rendering a verdict. The facts and circumstances should also be considered in those cases when a record of a conviction has been expunged or a pardon granted. An exception would be a presidential or gubernatorial pardon granted on the basis of the person's innocence. When an applicant for employment is under indictment or formal criminal charges for an offense requiring referral under the provisions of paragraph 802, that person may not be considered for employment until a disposition is made of the pending charges.

(b) Dishonest conduct includes an act indicating deliberate disregard for the rights of others (generally through lies, fraud, or deceit) for the benefit of the applicant or employee; or for the benefit of other persons (e.g., offer or acceptance of a bribe, falsification of records, willful disregard for the truth, theft, issues relating to non-material falsification).

(3) **Intentional false statement or deception or fraud in examination or appointment.** Examples (not all-inclusive): Falsifying an application or appointment document, impersonation in examination, collusion in examination, assuming the identity of a person who is eligible for employment, altering the grade score on an OPM notice of rating, altering discharge information on military discharge documents, and altering college transcripts to qualify for a position requiring specific educational attainment.

(4) **Refusal to furnish testimony required by civil service rules.** Civil Service Rule 5.4 requires all employees and all applicants for positions covered by civil service rules to provide to OPM, the Merit Systems Protection Board (MSPB), and the Special Counsel of MSPB, upon request, information, testimony, documents, and material about matters inquired of under the civil service laws, rules, and regulations. Authority to invoke this rule is reserved to OPM, MSPB, and its Special Counsel. Failure to comply with an OPM requirement may be disqualifying, provided the person was aware of the Rule 5.4 requirement.

(5) **Alcohol abuse of a nature and duration which suggests that 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.** Current, continuing abuse will ordinarily be disqualifying. Abuse may manifest itself in poor employment records, debts, domestic difficulties, or convictions for offenses against the law. A clear, lengthy break in a pattern of abuse and strong evidence that the abuse will not occur again is required before the conduct can be considered nondisqualifying.

(6) **Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation.** Current or recent use or possession will ordinarily be disqualifying. Any pattern is also disqualifying unless there is a clear, lengthy break since the last occurrence.

(7) **Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force.** Traitorous acts are disqualifying. Knowing membership in, with specific intent to further the aims of, an organization which unlawfully practices acts of force or violence to prevent others from exercising their rights under the Constitution or law, or which seeks to overthrow the Government by unlawful or unconstitutional means is disqualifying. Peaceful protest in and of itself is not disqualifying. In some situations, conduct that is disqualifying will also involve a statutory bar to employment.

(8) **Any statutory or regulatory bar which prevents the person's lawful employment in the position in question.** Refer to appendix 7.

C. ADDITIONAL CONSIDERATIONS. To the extent deemed pertinent to an individual case, suitability adjudicators shall consider the following when applying the additional considerations listed in paragraph 401c:

(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.** The greater the extent to which the level of authority and responsibility associated with the position affects the efficiency of the service, the more serious the misconduct becomes as a potentially disqualifying issue.

(2) **The nature and seriousness of the conduct.** Refer to paragraph E.

(3) **The circumstances surrounding the conduct.** Full facts and circumstances are essential in each case to ensure justice to the individual and protection of the Government's interests.

(4) **The recency of the conduct.** The more recent the conduct is, the greater the potential for disqualification.

(5) **The person's age at the time of the conduct.** In general, adjudicators should treat an offense committed as a minor as being less serious than the same offense committed as an adult, unless it is very recent, is part of a pattern, or is particularly heinous. In regard to juvenile crimes, a juvenile offender is one who committed an act in violation of a law, regulation, or ordinance before his or her 18th birthday and the offense for which charged was finally adjudicated in a juvenile court or under a youth offender law. Adjudicators shall apply a more flexible standard when adjudicating a particular case if the person either:

(a) Committed an offense prior to his or her 18th birthday and the offense was adjudicated in a juvenile court; or

(b) Up to the age of 26 had a conviction set aside under the Federal Youth Correction Act or similar state authority.

(6) **Contributing societal conditions.** Adjudicators shall consider these conditions in cases involving relatively minor issues.

(7) **Absence or presence of, or efforts toward, rehabilitation.** Clear, affirmative evidence of rehabilitation is required for a favorable adjudication. Mere efforts toward rehabilitation are insufficient.

D. OPM ISSUE RANKINGS. When OPM completes an investigation, it assigns a ranking (A, B, C, or D) based on the seriousness of any issues raised. OPM's rankings, descriptions, and potential as a basis for disqualification are as follows:

(1) "A" - Minor: Conduct or issue which, standing alone, would not be disqualifying, under suitability, for any position.

(2) "B" - Moderate: Conduct or issue which, standing alone, would probably not be disqualifying, under suitability, for any position.

(3) "C" - Substantial: Conduct or issue which, standing alone, may probably be disqualifying, under suitability, for any position.

(4) "D" - Major: Conduct or issue which, standing alone, would be disqualifying, under suitability, for any position.

E. BASIC SUITABILITY ADJUDICATION.

(1) In basic suitability adjudication, the adjudicator determines whether there is an issue or combination of issues that would clearly disqualify the person from any position at the FAA. This adjudication requires identification of suitability issues and characterization of those issues relative to seriousness, frequency of occurrence, and elapsed time since occurrence. Depending upon the recency of an issue, and its frequency of

occurrence, the adjudicator is expected to either upgrade or downgrade its relative seriousness during the adjudicative process. Only after according these factors adequate consideration would the adjudicator take any warranted action.

(2) The adjudicator should proceed with adjudication in the following manner:

(a) Characterize the level of seriousness of each issue using chart A as a guide and any ranking OPM has assigned to an issue in a completed investigation.

(b) For each issue, determine the date (month and year) the conduct or incident occurred. In the case of a current, ongoing issue, such as current drug use, the date would be the current month.

(c) For each issue, determine a control date, as follows:

1. If the person is an applicant who has filed directly with the FAA, the control date is the date the Human Resource Management Division first considered the application.

2. If the person is an investigated applicant or employee, the control date is the date he or she signed the Standard Form (SF) 85, Questionnaire for Nonsensitive Positions; SF-85P, Questionnaire for Public Trust Positions; or SF-86, Questionnaire for National Security Positions.

3. If the person is an employee, the control date is the date the conduct was first identified as an issue.

(d) For each issue, determine the elapsed time between the occurrence and the control date.

(e) If there are multiple issues in the same case, and if necessary, upgrade the most serious issue according to frequency. This step is based on the premise that multiple issues raise a more serious suitability question. "A," "B," or "C" issues may be upgraded if they

are repeated issues or if they occur in connection with another issue or issues. As a guide:

1. If there are two issues occurring within 36 months prior to the control date, or two occurrences of the same issue within that time, raise the most serious issue once (e.g., "A" to "B").

2. If there are three or more issues occurring within 36 months prior to the control date, or three occurrences of the same issue within that time, raise the most serious issue twice (e.g., "A" to "C").

(f) If there was no suitability upgrade, downgrade an issue, if necessary, to take into account its recency. As a guide:

1. Do not downgrade any issue that occurred within the 36 months prior to the control date.

2. Downgrade by one letter any issue that occurred between 37 and 72 months prior to the control date (e.g., "B" to "A," "C" to "B"). An "A" issue occurring more than 36 months prior to the control date would become a non-issue.

3. Downgrade by two letters, if possible, any issue that occurred between 73 and 108 months prior to the control date (e.g., "C" to "A," "D" to "B"). A "B" issue occurring more than 72 months prior to the control date would become a non-issue.

4. If there are no issues that occurred within 108 months prior to the control date, any issue that occurred more than 108 months ago should not be considered for adjudication unless that issue results in a statutory debarment. (Refer to appendix 7.)

(g) Make a final basic suitability determination, using the following as a guide:

1. If at this point the most serious issue is at the "A" level, following any upgrading or downgrading, the potential for disqualification (i.e., not hiring an

applicant or removing an appointee or employee) is minimal. An adjudicator should normally not take such an action.

2. If the most serious issue is at the "B" level, disqualification is possible, depending on the recency and circumstances of the conduct, although not required. The adjudicator should carefully take into account the applicable suitability criteria and additional considerations, if any, in paragraphs B and C above.

3. If the most serious issue is at the "C" level, the adjudicator should probably rate the person as unsuitable, subject to any applicable considerations in paragraph C above. Any decision to hire an applicant with a "C" issue should clearly be warranted as being in the best interests of the FAA.

4. If the most serious issue is at the "D" level, the adjudicator should rate the person as unsuitable.

F. POSITION RISK ADJUDICATION.

(1) When a person has been rated suitable at the basic suitability adjudication level, and is in or is applying for a position that is other than a low risk position, the suitability ranking of the most serious actionable issue may be upgraded as follows:

(a) For positions at the moderate-risk and noncritical-sensitive levels, the adjudicator may raise the ranking of the issue by as much as one letter (e.g., "A" to "B," "C" to "D").

(b) For positions at the high-risk, critical-sensitive, and special-sensitive levels, the adjudicator should raise the ranking of the issue by one letter.

(2) Following any upgrading because of the position's risk or sensitivity level, the adjudicator should proceed with adjudication as stated in paragraph E(2)(g) above.

(3) The adjudicator should give due regard for the position's risk or sensitivity level in making a determination during this step in the process, especially in cases which may appear to be "borderline." However, the

adjudicator should take no action to disqualify a person from appointment or continued employment based on the position's risk or sensitivity level unless an adverse connection or nexus between the particular conduct and the person's performance of high risk, moderate risk, or sensitive duties, or the FAA's ability to perform its mission, is established and sustained, indicating that the person's employment could reasonably be expected not to promote the efficiency of the service.

G. POSITION PERFORMANCE ADJUDICATION.

(1) This step in the adjudication process occurs following favorable adjudication at the basic suitability and position risk levels. The adjudicator determines whether a person's conduct indicates a potential for behavior which would interfere with, prevent, or otherwise adversely affect:

(a) The person's performance in the position applied for or employed in;

(b) The performance of duties and responsibilities of other persons in the Government should the person be employed in that position; or

(c) The ability of the FAA, DOT, or other agencies to carry out their mandated responsibilities.

(2) In assessing the relation of the conduct to performance in a specific position, the adjudicator should determine:

(a) Whether the conduct or issue(s) would result in, or indicates a potential for, improper or inadequate performance or reduced efficiency by the person or others of specific duties and responsibilities; and

(b) Whether the conduct or issue(s) indicates any immediate or long-term risk to the efficiency of the service or abuse of the public trust by the person in carrying out the position's responsibilities.

(3) If the answer is "yes" to either or both of the above questions, the issue(s) must be considered as

potentially disqualifying in terms of the person's suitability for the position in question (i.e., the person's employment or continued employment may reasonably not be expected to promote the efficiency of the Federal service).

(4) During position performance adjudication, the adjudicator should consider all issues in a case with more than one, rather than just the most serious issue, because a less serious issue may actually have more of a nexus impact, or potential impact, on the person's performance in the specific position. As in the previous steps in the adjudication process, the adjudicator should carefully take into account the applicable suitability criteria and additional considerations, if any, in paragraphs B and C above.

H. FINAL DETERMINATION. If the adjudicator rates a person suitable at the basic suitability, position risk, and position performance stages of the adjudication process, and there is no statutory bar to the individual's employment, the Human Resource Management Division shall consider the person suitable for employment.

CHART A

ADJUDICATIVE STANDARDS: ISSUES

1. Issues related to use or possession of intoxicants			
A	B	C	D
drunk; drunk and disorderly; liquor law violation (use or possession by minor)	drinking and driving under the influence; driving while intoxicated	illegal manufacturing/sale	pattern of excessive use as reflected in -conviction record -job performance -employment history -inability to function responsibility -medical treatment -health
2. Issues related to illegal use/possession of controlled substances or marijuana			
A	B	C	D
infrequent use/possession of marijuana; possession of marijuana paraphernalia; possession of marijuana (arrest)	frequent use/possession of marijuana; use/possession of other controlled substances; possession of drug paraphernalia; cultivating marijuana for personal use	transfer of controlled substance; possession of sale/resale; prescription fraud/forgery; sale of controlled substance; unlawful dispensing of prescription drugs; smuggling contraband into prison; regular use of controlled substance other than marijuana	pattern as in 1.; manufacturing; addiction; importing/trafficking; cultivating for sale
3. Issues related to financial responsibility			
A	B	C	D
bad check; infrequent, irregular, but deliberate delinquency in meeting financial obligations	nonsupport; judgment tax lien or other default with no attempt at restitution; illegal gambling evictions	pattern of irresponsibility as reflected in -credit history -disregard for debts -abuse of fiduciary trust	pattern as in C plus continuing, major valid liabilities

ADJUDICATIVE STANDARDS: ISSUES (CONTINUED)

4. Issues related to immoral conduct			
A	B	C	D
	indecent exposure ; prostitution; solicitation; voyeurism/peeping tom; mailing/selling/displaying obscene material; obscene phone call; indecent proposal	carnal knowledge; sodomy; bigamy/polygamy; pimping/pandering; keeping house of ill repute; contributing to delinquency/corrupting; sexual harassment; other sexual misconduct with impact on job and/or notoriety	pattern of misconduct as reflected in -conviction record -medical treatment -public knowledge child molestation; sexual assault; statutory rape; incest; beastiality
5. Issues related to honesty			
A	B	C	D
	altering; breaking & entering; forgery; fraud; possession of or receiving stolen property; black market activities (nonprofit); stealing; theft; petty theft; shoplifting; abuse of property; false statement; filing false instrument; failure to file income tax	bribery; embezzlement; grand larceny; grand theft; mail theft; burglary; robbery; perjury; false impersonation (e.g., impersonating an officer); interstate transportation of stolen goods; black market activities (with intent to profit); income tax evasion	pattern of dishonesty as reflected in -disregard for truth -conviction records -abuse of trust -employment records blackmail; counterfeiting; extortion; robbery, armed; intentional false statement or deception or fraud in examination or appointment

ADJUDICATIVE STANDARDS: ISSUES (CONTINUED)

6. Issues related to disruptive or violent behavior			
A	B	C	D
disorderly conduct; disturbing the peace; making threats; resisting arrest; abusive language; hindering prosecution	assault; damaging property; destroying property; hit & run; vandalism; criminal/malicious mischief; harassment	assault & battery; battery; manslaughter (involuntary)	pattern of violence as reflected in -conviction records -disregard for life or property -civil actions -employment records -medical records assault, aggravated; assault with deadly weapon; assault with intent to commit rape; kidnapping/abduction; murder; rape; arson; threat or assault upon public official; voluntary manslaughter; child abuse

7. Issues related to termination or forced resignation			
A	B	C	D
attitude; personality conflict	insubordination; absenteeism/attendance; rules/regulations violation	*	pattern of unemployability based on misconduct or delinquency as reflected in employment history*

*Other issues (use or possession of intoxicants, controlled substance and marijuana, financial responsibility, immoral conduct, honesty, disruptive or violent behavior, etc.) which lead to termination or forced resignation are raised on level for adjudicating purposes. For example, theft, a "B" issue by itself becomes a "C" issue if it is determined to be the reason for termination from employment.

ADJUDICATIVE STANDARDS : ISSUES (CONTINUED)

8. Issues relating to firearms/weapons			
A	B	C	D
possession unregistered firearm	possession of prohibited weapon; possession of illegal ammunition	carrying concealed weapon/firearm; carrying deadly weapon; brandishing firearm; possession of firearm by felon; possession of leaded firearm; possession of explosives	improper/illegal sale or transportation of firearm or explosive; manufacture of firearms or explosives
9. Miscellaneous issues			
A	B	C	D
vagrancy; loitering; trespassing; minor traffic violations (traffic violations not required to be admitted on SF-171/SF-86 will not be considered as issues)	traffic violations greater than "A," but less than "C", contempt of court; driving motor vehicle without owner's consent; possession of instrument of crime	vehicular homicide; refusal to furnish testimony as required by 5 CFR Sec 5.4; tampering with witness; harboring a fugitive	Hatch Act violation; mutilation/destruction of public records; engaging in riots or civil disorders; striking against Government; desertion
10. Issues subject to statutory debarment: See Appendix 7			

NOTE: For conduct not listed in this appendix, an attempt will be made to find a like or related issue, and the characterization of the listed issue should be used. If the conduct does not equate with a listed issue, but seems to relate more appropriately to a level where no issues are identified (i.e., level "A" at issues 4 and 5 or level "B" at issue 8) it might be appropriate to identify the issue at one of these level. Any uncertainty about an unlisted issue should be resolved by an experienced adjudicator.

The ranking of probation/parole violations will be determined by the nature of the issue leading to the violation. For example, a probation/parole violation for driving while intoxicated will be adjudicated at level "B" while a violation for assault with a deadly weapon will be adjudicated at level "D." Probation/parole violations that cannot be related to conduct in this appendix (e.g., failure to report to probation/parole officer) will be adjudicated at level "B."

APPENDIX 7. 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 8. SECURITY BRIEFING GUIDANCE FOR ACCESS TO CLASSIFIED INFORMATION

GENERAL.

a. Operating offices 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. This appendix has been prepared to aid offices in conducting these briefings and is not to be taken as a substitute for review of the latest edition of Order 1600.2, Safeguarding Control and Procedures for Classified National Security Information and Sensitive Unclassified Information, and other FAA and DOT orders pertaining to the handling of classified information. It also includes items mentioned in Standard Form 312, Classified Information Nondisclosure Agreement, which an employee shall sign when being granted a clearance for access to classified information as stated in paragraph 1005 of this order.

b. The following Guidance for Protecting Classified Information, written in the second person, is in the form of a sample briefing. It contains the most important information that employees need to know if they are going to have access to this information. Anyone with questions concerning the use of this guidance should consult his or her servicing security element (SSE).

GUIDANCE FOR PROTECTING CLASSIFIED INFORMATION

1. RESPONSIBILITIES. Security is an individual responsibility. You are personally responsible for the security of classified information entrusted to your care. Your servicing security element will assist you in carrying out this responsibility and you should ask that division or staff any questions you may 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 which 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 which 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 which 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 may be used to identify classified information.

d. Only information may 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 may be originally classified only to the SECRET level, and then only by the Administrator, the Associate Administrator for Civil Aviation Security, and, under emergency conditions, by regional administrators, center directors, and the Director of the Europe, Africa, and Middle East Office.

f. TOP SECRET, NATO, Communications Security (COMSEC), Restricted Data, Sensitive Compartmented Information, 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 should report the situation immediately to your servicing security element.

3. ASSURANCES NEEDED BEFORE GRANTING ACCESS TO CLASSIFIED INFORMATION. Before you give anyone access to any classified information, you must:

a. Identify the individual who desires access to the information and establish that he or she is cleared to the proper level. Personal recognition, by itself, is not 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 does not establish his or her security clearance status or "need to know." You must have either your personnel security coordinator or servicing security element 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.

a. Store classified information only in GSA-approved containers (safes) with built-in, three-way combination locks. You are not authorized to store it in other locked containers, including file cabinets that have been modified with lock bars and combination padlocks.

b. Keep a safe locked when its custodian or other person authorized access to it is not watching it continuously.

c. Use the OPEN/CLOSED sign and safe check record (Standard Form 702, Security Container Check Sheet) each

time the safe is opened or closed. If possible, someone who is not 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 at the SECRET level and above is controlled. A security control point has been established at your facility. All classified messages and documents, including file and grid copies, must be accounted for when they are received or created, and they must be returned to the security control point for destruction when there is no longer a need to keep them.

h. If your facility has a large volume of classified information, it should have a document control station with a custodian and alternate. Only these persons are authorized to receive classified material from the security control point. The custodian must maintain control records which 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.

i. Obtain a receipt for all classified documents classified at the SECRET level and above. When you are issued such a document, you must sign the original DOT F-1600.4, Classified Material Record, which the security control point retains. You will receive a copy of the form which you must file with the document in your office. Whenever you return the document to the security control point for transfer or destruction, you must bring that copy with you.

j. 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.

k. Whenever you transfer a document classified SECRET or above to another office within your facility, you must route it through the security control point for accountability.

l. Whenever you want to transmit any classified document to a location outside your facility, regardless of the document's classification level, you must route it through your security control point. If you are going to carry the document yourself, the security control point will make sure that it is properly wrapped and will advise you of all necessary procedures.

m. The receipt process is not required for CONFIDENTIAL material. However, you must take CONFIDENTIAL documents to the security control point for destruction or for transfer outside your facility.

n. Apply classification markings 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.

o. 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.

p. Do not reproduce classified information unless the security control point specifically authorizes you to do so. Normally, the security control point will reproduce it for you.

q. Do not 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 should 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. Do not 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 servicing security element. 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 servicing security element.

d. If a visitor expresses an unusual interest in information he or she is not authorized to receive, report the situation to your servicing security element.

APPENDIX 9. INVESTIGATING CONTRACTOR EMPLOYEES

1. General. This appendix states policy and procedures for the personnel security program as it relates to FAA contractor employees. It applies to persons employed as or by contractors, subcontractors, or consultants who have access to FAA facilities, sensitive information, and/or resources; and to other persons who have such access by agreement of the FAA. Appendix 11, Investigating Child Care Center Workers, contains procedures for investigation of persons working at FAA-sponsored child care centers.

2. Background. Many contractor employees are part of the FAA work force or closely support the agency's mission. Because of their FAA identification, the extent of their responsibility, and the risk levels of the positions they occupy, the FAA investigates certain contractor employees to determine their suitability for access to FAA facilities, sensitive information, or resources.

3. Authority to investigate contractor employees.

a. The Department of Justice (DOJ) rendered an opinion October 1, 1979, that Federal agencies have the authority to screen contractor employees in any reasonable manner and that such screening must be consistent with due process of law. The DOJ cited from the United States Code (U.S.C.) three statutory sources of agency authority to investigate and determine the suitability of contractor employees. These authorities are:

(1) 5 U.S.C. 301. Authorizes the head of each executive or military department to "prescribe regulations for the government of [the] department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property."

(2) 44 U.S.C. 3102. Requires each Federal agency to provide for "effective controls over the creation and over the maintenance and use of records in the conduct of current business" and in cooperation with the Administrator of the General Services Administration to "promote the maintenance and security of records deemed appropriate for preservation."

(3) 5 U.S.C. 552a(e)(9) and (10). Requires that each agency establish: (1) Rules of conduct for persons involved in the design, operation, or maintenance of any system of records; and (2) appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. The DOJ noted that U.S.C. 552a, while applicable only to systems of records containing information on individuals, does provide that agencies, consistent with their authority, shall extend the requirements of the section to Government contractors who operate such a system of records to accomplish agency functions.

b. OMB Circular A-130, Management of Federal Information Resources, requires Federal agencies to establish personnel security policies for Federal and contractor personnel as needed to ensure an adequate level of security for Federal automated information systems. These policies should include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications, as well as those persons having access to sensitive data.

4. Definition of sensitive information. P.L. 100-235 defines sensitive information as any information which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive data at FAA also include proprietary data.

5. Policy.

a. Except as stated in this appendix, the personnel security program requirements and procedures applicable to FAA employees shall also apply to contractor employees who have comparable exposure to the agency's facilities, information, or resources. No contractor employee or applicant for contractor employment shall be prevented from having access to FAA facilities, sensitive information, or resources because of information revealed in a background

investigation unless the FAA has given that person an opportunity to respond to any information used as a basis to deny such access. The servicing security element (SSE) is responsible for adjudicating the suitability of contractor employees.

b. Contracts requiring contractor employees to have access to classified information shall be prepared and processed according to the procedures contained in Appendix 10, National Industrial Security Program (NISP).

6. Responsibilities.

a. Contracting offices shall:

(1) Ensure that all new or revised contracts or purchase orders have been coordinated with the SSE for review and determination of applicable personnel security investigative requirements prior to issuance of contract solicitation.

(2) Ensure that whenever the SSE has determined that a contract or purchase order requires investigation of any contractor employees, the contract contains language sufficient to achieve this objective in an orderly and expeditious manner and language allowing FAA to deny a contractor employee access to FAA facilities, information, and/or resources if the FAA determines that that person is unsuitable.

(3) Ensure that the SSE is notified whenever a contract is issued or when the status of a contract changes (i.e., replaced, defaulted, terminated, etc.).

(4) Ensure that contractors and contractor employees (including prospective contractor employees) submit to the SSE completed forms and information for each person subject to investigation as required by the applicable contract.

(5) Ensure that a contractor employee is not allowed to work in a high- or moderate-risk position unless the SSE has received all forms necessary to conduct any required investigation and has given its approval.

(6) Ensure that the SSE is notified of any information it receives which raises a question about the suitability of a contractor employee.

(7) Ensure that any appropriate action the SSE directs is taken whenever a question has arisen regarding the suitability of a contractor employee. Appropriate action may include temporarily denying the contractor employee access to FAA facilities, sensitive information, and/or resources pending resolution of an issue raising a question of suitability.

(8) Ensure that appropriate action is taken when the SSE determines that a contractor employee is unsuitable for access to FAA facilities, sensitive information, and/or resources. Appropriate action may include excluding the contractor employee from working on any aspect of the FAA contract.

(9) Ensure that the SSE is notified whenever a contractor employee has completed work under the contract or leaves his or her position.

b. Operating offices shall:

(1) Coordinate with the SSE on all procurement requests which may involve contractors and/or contractor employees having access to FAA facilities, sensitive information, or resources. Included are situations where operating offices exercise authority to contract for or purchase services directly without significant involvement on the part of a separate contracting office. They shall also coordinate with the SSE on any proposed agreements with outside parties that would result in non-FAA personnel having such access. The purpose of this coordination is to determine whether or not any investigation requirements would apply to the contractor employees or other persons having access.

(2) Ensure that whenever the SSE has determined that persons granted access to an FAA facility under an agreement as stated in b(1) would require investigation, the agreement contains language sufficient to achieve this

objective and to allow the FAA to deny any such person access to FAA facilities, information, and/or resources if the FAA determines that the person is unsuitable.

(3) Work with the contracting office as necessary to obtain from the contractor and contractor employees all forms and information required to initiate personnel security investigations.

(4) Ensure that a contractor employee is not allowed to work in a high- or moderate-risk position unless the SSE has received all forms necessary to conduct any required investigation and has given its approval.

(5) Notify the SSE and the contracting office of any questionable conduct which might affect the suitability of a contractor employee.

c. Servicing security elements shall:

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

(2) Assist the contracting office in developing appropriate contract clauses.

(3) Ensure that contracts requiring contractor employees to have access to classified information are prepared and processed as required by appendix 10.

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

(5) Evaluate the results of personnel security investigations of contractor employees and adjudicate suitability in consultation with other offices on a need-to-know basis.

(6) Conduct or arrange for additional investigation when necessary to resolve suitability issues.

(7) Provide due process to contractor employees prior to taking any unfavorable action based on the results

of an investigation. Due process shall consist of notifying the person of the specific reasons for the proposed action and affording the person an opportunity to respond.

(8) Notify the contracting officer in writing of any contractor employee found unsuitable for access to FAA facilities, sensitive information, and/or resources and request action to deny such access.

(9) Consult with the operating office and direct appropriate action to be taken whenever any information is received which raises a question about a contractor employee's suitability.

(10) Maintain records on contractor employee personnel security investigations in an automated information system which the Office of Civil Aviation Security Operations (ACO) has approved for this purpose and maintain personnel security files, as necessary, on contractor employees.

(11) Provide the contracting officer with all DOT/FAA security directives that the contractor needs to fulfill security responsibilities under the contract.

(12) Ensure that contractor employees receive all needed security briefings.

7. Designating position risk levels.

a. The SSE, in consultation with the operating office, shall review procurement requests and contract specifications to determine the risk levels for contractor employee positions. The policies specified in Chapter 5, Position Sensitivity and Risk Level Designation and Controls, shall apply in designating positions in terms of suitability and access to automated information systems (AIS). The SSE may use the risk level designation process outlined in Appendix 3, Position Risk and Sensitivity Level Designation Process, to help ensure uniformity and consistency in these designations.

b. The SSE may designate contractor employee positions in groups or by category rather than creating records for each individual position.

c. In order to ensure uniformity throughout FAA for positions common in more than one region and/or center, the Investigations Division, ACO-300, may provide specific direction to SSE's regarding designations of particular position categories or groups.

8. Investigative requirements for contractor employees.

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

b. Specific requirements and exceptions are as follows:

(1) High-risk positions. All contractor employees in these positions shall be subject to a Background Investigation (BI). Whenever possible, this investigation should be completed and favorably adjudicated before the employee is allowed to perform the position's duties. However, the SSE may grant approval for the employee to begin work earlier, provided that it has considered the nature of the FAA facilities, sensitive information, and resources to which the employee will have access. In giving this approval, the SSE may also limit the facilities, information, and/or resources to which the employee has access pending completion of the investigation. If the BI cannot be completed before the employee must begin work on the FAA contract, the SSE shall make every effort to complete at least a check of the person's fingerprints with the Federal Bureau of Investigation's (FBI) Identification Division, or an appropriate law enforcement agency check, as soon as possible. At a minimum, a contractor employee may not perform the duties of a high-risk position until all necessary investigative forms have been submitted to the SSE. Except as stated in this paragraph, the specific investigative requirements for high-risk positions stated in paragraph 606 of this order also apply to contractor employees.

(2) Moderate-risk positions. All contractor employees in these positions shall be subject to at least a National Agency Check and Inquiries (NACI) investigation. In addition, those employees in positions with significant fiduciary responsibilities, as determined by the SSE, shall be subject to a National Agency Check, Inquiries, and Credit (NACIC) investigation. Whenever possible, the investigation shall be completed and favorably adjudicated before the employee is allowed to perform the position's duties. However, the SSE may grant approval for the employee to begin work earlier, provided that it has considered the nature of the FAA facilities, sensitive information, and resources to which the employee will have access. In giving this approval, the SSE may also limit the facilities, information, and/or resources to which the employee has access pending completion of the investigation. If the investigation cannot be completed before the employee must begin work on the FAA contract, the SSE shall make every effort to complete at least a fingerprint or appropriate law enforcement agency check as soon as possible; and, in the case of a position with significant fiduciary responsibilities, a credit check. At a minimum, a contractor employee may not perform the duties of a moderate-risk position until all necessary investigative forms have been submitted to the SSE. Except as stated in this paragraph, the specific investigative requirements for moderate-risk positions stated in paragraph 607 of this order also apply to contractor employees.

(3) Low-risk positions. Except as specified below, the minimum investigative requirement for contractor employees in these positions is a fingerprint check. Depending on the extent of access to FAA facilities, sensitive information, or resources, the SSE may require a more extensive investigation, up to and including an NACI. The SSE, after consultation with the contracting office and the operating office, may require submission of all required forms before the employee can receive the access.

(4) Temporary positions. Contractor employees in low-risk positions that are intermittent, seasonal, per diem, or temporary and who do not work on the FAA contract in excess of 180 days in either a single assignment or a series of assignments are exempt from any investigative

requirement. This exemption does not preclude investigating the person under the normal investigative requirements.

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

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

(7) Contractor personnel requiring access to classified information. When contractor employees require access to classified information and DOD investigates them under the National Industrial Security Program, as stated in appendix 10, the SSE is not required to initiate any additional investigation.

c. The provisions of Chapter 7, Standards and Procedures for Using Previous Investigations, also apply to contractor employees.

9. Initiating investigations.

a. The contracting office has the primary responsibility for ensuring that required, completed forms for investigation of contractor employees are submitted to the SSE prior to the employees receiving access to the facilities, information, or resources which make them subject to investigation. The operating office shall assist the contracting office as necessary.

b. Specific forms are required to initiate investigations for low, moderate, and high risk positions:

(1) For low risk positions requiring only a fingerprint check, the contractor employee shall be required to submit an FD-258, FBI Fingerprint Chart. For any low risk position, however, the SSE may also require submission of Standard Form (SF) 85P, Questionnaire for Public Trust Positions. This form is required to conduct a National Agency Check (NAC) or NACI.

(2) For moderate and high risk positions, the contractor employee shall be required to submit the FD-258 and an SF 85P.

(3) For any contractor employee position, the SSE may also require submission of Optional Form 306, Declaration for Federal Employment, or other form needed to comply with Office of Personnel Management (OPM) requirements. As necessary, ACO-300 shall transmit to the SSE's information about additional forms or information required to initiate investigations on contractor employees.

c. Because of the sensitive nature of the forms required for investigations, and because of Privacy Act requirements, either ACO or a particular SSE may establish procedures for contractor employees to submit the forms directly to the SSE or to the contracting office for forwarding to the SSE. These procedures shall ensure that an employee submits the forms directly to the FAA in a sealed envelope and that neither the employee's supervisor nor other company personnel have access to them.

d. When initiating only a fingerprint check, the SSE may do so directly with the FBI or, by appropriate agreement, through OPM.

(1) To conduct the check directly with the FBI, the SSE should submit the FD-258, FBI Fingerprint Chart, directly to the Identification Division, ATTN: Recording Section, Federal Bureau of Investigation, 10th and Pennsylvania Avenue, NW, Washington, DC 20537.

(2) To conduct this check through OPM, the SSE shall ensure that any necessary agreement exists between the FAA and OPM and shall follow OPM instructions in submitting the FD-258 and any other required form(s).

e. When initiating an NACI or higher level investigation, the SSE may do so through any Government agency providing this service. ACO may also establish procedures for SSE's to conduct the required investigations on contractor employees.

f. To pay for investigations, allotments of funds are made to regions, centers, and headquarters. Unless there has been a specific allotment to the SSE to pay for all contractor employee investigations for operating offices it services, each operating office shall arrange to pay the costs for investigations on those employees working under contracts for which it is responsible. While this requirement does not preclude recovering investigation costs from contractors, the operating office responsible for payment shall provide the SSE with the accounting code information necessary to have the costs charged appropriately.

10. Adjudicating investigations.

a. The SSE shall adjudicate all reports of investigation on contractor employees to determine their suitability. In those cases where the SSE believes that information developed during the course of an investigation might result in an unfavorable suitability determination, it shall consult with the contracting officer and any office with a need-to-know.

b. Following receipt of a completed report of investigative results, it may be necessary for the SSE to conduct additional investigation before making a suitability determination. In doing, so the SSE shall follow the criteria and procedures stated in paragraph 304 of this order.

c. In adjudicating contractor employee investigations, the SSE shall apply the same suitability standard and criteria used in adjudicating investigations on FAA

applicants and employees, as stated in paragraph 401 of this order.

d. Before the FAA denies a contractor employee access to its facilities, sensitive information, or resources because of information received as the result of investigation, the SSE shall provide the employee due process, an opportunity to respond to the information being considered as the basis for denying that access. The SSE may provide due process either orally during an interview with the contractor employee, or in writing. In either case, the SSE shall clearly explain the unfavorable information and provide the employee the opportunity to respond. It shall then consider any information the employee has provided before making a final suitability determination. The FAA does not have to give the employee any additional opportunity to respond to the decision.

e. In the case of an unfavorable suitability determination, the SSE shall notify the contracting office in writing. The contracting office shall then notify the contractor to remove the employee as otherwise objectionable from performance under the contract, or to take other action as the SSE directs. For example, the SSE may deny the person access to FAA facilities but may still allow him or her to work on the FAA contract at another location.

f. When providing due process and adjudicating investigative results, the SSE shall communicate with an employee directly rather than through a supervisor or other contractor official. Neither an SSE nor any other FAA employee shall disclose to a contractor information contained in an investigation on a contractor employee or the specific reason(s) for any suitability determination. Contracting offices shall ensure that contractors understand these procedures and the reasons for them.

11. Foreign nationals as contractor employees.

In general, foreign nationals may work as FAA contractor employees on unclassified contracts and may have access to FAA facilities, information, and resources under other agreements to which the FAA is a party. In any situation where the operating office and/or the SSE determine that it is in the FAA's best interest to restrict

access or work on a contract to United States citizens only, the appropriate contract or other agreement shall specify that restriction. In determining whether or not to apply this restriction in a given situation, FAA personnel shall consider the nature and extent of access, particularly in regard to sensitive or proprietary information.

12. Records on contractor employees.

a. When the SSE initiates an investigation on a contractor employee, it shall enter a record on that person into an automated information system approved by ACO. It may also enter a record on an employee to whom DOD has granted a security clearance for work on an FAA contract. The contractor employee information in the approved system shall be available to all SSE's and shall serve as the primary means by which an SSE can determine if a particular contractor employee has been investigated.

b. As appropriate, SSE's shall provide information to operating offices, facilities, personnel security coordinators, and contracting offices as to which contractor employees are allowed access to FAA facilities, sensitive information, and resources.

c. SSE's shall establish personnel security files (PSF) for contractor employees when there are reports of investigation or other personnel security records warranting retention. SSE's may use paragraph 305a of this order as a guide regarding contents of a PSF. When they establish PSF's, they shall maintain them for as long as the employees are working on an FAA contract. After that time, the SSE's shall retain their PSF's for the same lengths of time which paragraph 305b of this order specifies for separated FAA employees.

d. Personnel security records contain sensitive, highly privileged, and, in some cases, classified information. All FAA personnel shall carefully protect these records in their handling, transmittal, storage, and release. The provisions of paragraph 305c of this order also apply to personnel security records on contractor employees.

e. Upon request, an SSE shall provide a contractor employee the opportunity to review his or her PSF. The employee may also, in writing, authorize a representative to review it. When complying with a request for a PSF review, the SSE shall follow the same procedures as those for PSF's on FAA employees, specified in paragraph 305d of this order.

APPENDIX 10. NATIONAL INDUSTRIAL SECURITY PROGRAM

1. General. This appendix states policy and procedures for implementing the National Industrial Security Program (NISP) at the FAA. It implements Executive Order 12829, National Industrial Security Program; and the industrial security policies contained in the latest edition of Order DOT 1640.4, Classification, Declassification, and Control of National Security Information. These policies and procedures apply whenever contractors, contractor employees, consultants, or other persons (hereafter referred to as contractor employees) performing work for or under the direction of the FAA require access to classified information in order to perform their duties.

2. Background.

a. E.O. 12829 established the NISP on January 6, 1993. The National Security Council is responsible for providing overall policy direction for the NISP and the President has designated the Secretary of Defense as the NISP Executive Agent. The Director, Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies. By agreement between DOT and the Department of Defense (DOD), DOT authorizes DOD to act for and on behalf of DOT in providing security services for the protection of classified information that DOT releases to contractors, contractor employees, and consultants.

b. When acting as a contracting agency, DOT has the authority and responsibility and performs the functions specified for a user agency in the latest editions of the National Industrial Security Operating Manual (NISPOM) and the Industrial Security Regulation (ISR), both of which are issued by DOD. DOD grants facility clearances to contractors as needed and grants security clearances to contractor employees when necessary for access to classified information.

3. Classified contract processing procedures.

a. Whenever a proposed contract, purchase order, or consulting agreement would require persons not employed by the U.S. Government to have access to classified

information, the operating office shall include that information in a statement with the procurement request. The office shall also prepare and submit with the request a draft DD Form 254, Contract Security Classification Specification. The DD 254 shall be prepared as specified in the ISR or other DOD regulations or instructions. The office shall coordinate the draft DD 254 with its servicing security element (SSE) to ensure appropriate classification.

b. The contracting office shall review all proposed procurement actions to determine if the FAA will need to share classified information with a contractor during pre-contract negotiations. If that is the case, the contracting office shall advise the SSE and provide it with a list of prospective bidders. The contracting office shall coordinate with the appropriate Defense Investigative Service (DIS) office to determine if any prospective bidders require processing for a facility security clearance in accordance with the NISPOM, ISR, and/or other DOD regulations. The contracting office is responsible for taking action required by DOD and shall issue a DD 254, signed by the contracting officer, for each request for proposal, invitation for bid, request for quotation, or other solicitation.

c. The contracting office shall issue a completed DD 254 with the award of each classified contract, including follow-on contracts, and shall provide a copy of the form to its SSE.

d. Each classified contract or consulting agreement shall contain a security clause specifying everything that a contractor, contractor employee, or consultant has to do to ensure that the FAA and DIS can process all contractors and individuals for any needed facility or security clearances, and do so according to requirements and procedures stated in the NISPOM, the ISR, or other DOD regulations. The contract shall also specify that visit requests for classified visits shall be in accordance with the NISPOM and shall be certified by the contracting office prior to forwarding to the organization to be visited.

e. DIS will work directly with contractors, contractor employees, and consultants to grant facility clearances and to grant security clearances to individuals. In selected

cases, DIS will provide reports of investigation to the SSE. In those instances the SSE shall then adjudicate the investigations as stated in paragraph 4 and determine whether or not to grant the clearances.

f. The contracting office shall notify the SSE and DIS whenever the status of a contract changes (i.e., replaced, defaulted, or terminated).

4. Annual review of DD 254. Annually, on the anniversary date of the contract, or more often if required by the ISR or other DOD regulation, the operating office shall review the DD 254 for accuracy and currency. If changes are necessary, the operating office and the contracting office, in coordination with the SSE, shall issue a revised DD 254, preparing it as specified in the ISR or other DOD regulation. If no change is necessary, the operating office shall notify all holders of the DD 254 that it is current in all respects.

5. Visit requests. Whenever a contractor employee or consultant is required to visit an FAA facility and will be required to have access to classified information, the contracting office shall complete, certify, and process a visit request as specified in the NISPOM, the ISR, or other DOD regulation. The contracting office shall provide an information copy of a certified visit request to the SSE for the facility to be visited.

APPENDIX 11. INVESTIGATING CHILD CARE CENTER WORKERS

1. General. This appendix states policy and procedures for the personnel security program as it relates to suitability checks on child care center workers. It applies to persons working in FAA-sponsored child care centers as either employees or volunteers.

2. Background. The Crime Control Act of 1990 (Public Law 101-647), Subtitle E, Child Care Worker Employee Background Checks, authorizes criminal history background checks on child care employees either hired by or under contract to the Federal Government. In accordance with General Services Administration guidelines, the DOT Child Care Handbook states that suitability checks shall be conducted on all child care center employees and shall include criminal records and background checks.

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

a. Any applicant for work in an FAA-sponsored child care center shall be subject to a National Agency Check (NAC) investigation.

b. Human Resource Management Divisions and servicing security elements (SSE) shall coordinate with each other to ensure that before an applicant is allowed to work in an FAA child care center, either as an employee or as a volunteer, he or she completes and submits to the SSE Standard Form 85P, Questionnaire for Public Trust Positions, and Form FD-258, Fingerprint Card. The SSE's are the regional and Aeronautical Center Civil Aviation Security Divisions, the Technical Center Security Staff, and the Office of CAS Operations (ACO) at Washington headquarters. Either law enforcement officers or qualified FAA personnel may take the fingerprints. Whenever possible, however, FAA personnel shall do the fingerprinting.

c. Upon receipt of the SF-85P, an SSE specialist trained to conduct personnel security interviews shall interview the applicant and review the form. The interviewer shall 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. Section 231(c), Applicable Criminal Histories, of the Crime Control Act of 1990 states, in part, that a conviction for any of these offenses may be grounds for denying employment or for dismissal of an employee from a child care services position.

d. If the SF-85P shows that a prior security investigation has been completed within the past 5 years, the SSE shall attempt to obtain the results of that investigation.

e. Whenever the interview or review of the SF-85P reveals derogatory information, the SSE shall inform the regional, center, or headquarters child care coordinator, who shall inform the applicable board of directors and/or the director of the applicable child care center, that the applicant may not begin working in the facility until the NAC has been completed and favorably adjudicated. Derogatory information in this instance means an arrest for one of the offenses specified above or other unfavorable information raising a significant issue which may eventually result in the FAA directing that the applicant may not work in the child care center.

f. If the interview and review of the SF-85P reveal no derogatory information, the SSE shall notify the regional, center, or headquarters child care coordinator, who shall notify the board of directors and/or the child care center director, that the applicant may begin working in the facility, under continuous supervision, pending completion of the NAC. The director of the child care center shall ensure that until the NAC has been completed and favorably adjudicated, the child care worker is not left alone with children at the center.

g. The SSE shall initiate the NAC through the Office of Personnel Management (OPM). ACO shall budget for the cost of these investigations and provide each SSE with an appropriate accounting code.

h. An SSE specialist trained in suitability adjudication shall adjudicate the results of the NAC and make a suitability determination. In doing so, the

specialist shall apply the same standard and criteria used in adjudicating investigations on FAA applicants and employees, as stated in paragraph 401 of this order.

i. Before making any unfavorable suitability determination, the SSE shall provide the applicant or employee due process, an opportunity to respond to the information being considered as the basis for prohibiting the person from working at the child care center. An SSE employee trained to conduct personnel security interviews shall interview the person, clearly explain the unfavorable information, and provide the individual the response opportunity. The SSE employee shall also document the interview, including the information provided to the individual and the individual's response. The SSE shall then consider any information the applicant or employee has provided before making a final suitability determination. The SSE shall consult with the Office of the Chief Counsel in headquarters cases, and with the Office of the Assistant Chief Counsel in regional and center cases, before making a final unfavorable suitability determination.

j. The SSE shall notify the regional, center, or headquarters child care coordinator, who shall notify the board of directors and/or the child care center director, of the results of the suitability determination. In the event of an unfavorable suitability determination, the SSE shall inform the child care coordinator in writing, who shall then inform the board of directors and/or the child care center director in writing, that the applicant or employee may not work at any FAA-sponsored child care center. The SSE shall also notify the applicant or employee in writing when the suitability determination is unfavorable.

k. FAA personnel responsible for arrangements for, oversight of, and liaison with FAA-sponsored child care centers shall 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 these procedures.

APPENDIX 12. SECURITY ADJUDICATION GUIDELINES

1. General. The following adjudication guidelines, which are in effect throughout DOT, were developed by the Security Policy Board as required by E.O. 12968. They shall be used when determining whether the granting or continuation of eligibility for access to classified information is consistent with the interests of national security. Servicing security elements (SSE) shall use this guidance in all such determinations at FAA.

2. The adjudicative process.

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

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

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

(3) the frequency and recency of the conduct;

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

(5) the voluntariness of participation;

(6) the presence or absence of rehabilitation and other pertinent behavioral changes;

(7) the motivation for the conduct;

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

(9) the likelihood of continuation or recurrence.

(b) Each case must be judged on its own merits, and final FAA determination remains the responsibility of the Office of Civil Aviation Security Operations (ACO). Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security and considered final.

(c) The ultimate determination of whether the granting or continuation of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person:

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

(2) GUIDELINE B: Foreign influence;

(3) GUIDELINE C: Foreign preference;

(4) GUIDELINE D: Sexual behavior;

(5) GUIDELINE E: Personal conduct;

(6) GUIDELINE F: Financial considerations;

(7) GUIDELINE G: Alcohol consumption;

(8) GUIDELINE H: Drug involvement;

(9) GUIDELINE I: Emotional, mental, and personality disorders;

(10) GUIDELINE J: Criminal conduct;

(11) GUIDELINE K: Security violations;

(12) GUIDELINE L: Outside activities; and

(13) GUIDELINE M: Misuse of Information Technology Systems.

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

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

(1) voluntarily reported the information;

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

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

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

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

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

(f) If after evaluating information of security concern the adjudicator decides that the information is not serious

enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

GUIDELINE A

Allegiance to the United States

3. The concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to question an individual's allegiance to the United States.

4. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) 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;

(b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(c) 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

(d) involvement in activities which 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.

5. Possible mitigating conditions: Conditions that could mitigate security concerns include:

(a) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(b) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(c) 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

(d) the person has had no recent involvement or association with such activities.

GUIDELINE B

Foreign Influence

6. The concern. A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may 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.

7. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) 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;

(b) sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

(c) relatives, cohabitants, or associates who are connected with any foreign government;

(d) failing to report, where required, associations with foreign nationals;

(e) unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

(f) conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

(g) 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

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

8. Possible mitigating conditions: Conditions that could mitigate security concerns include:

(a) 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;

(b) contacts with foreign citizens are the result of official United States Government business;

(c) contact and correspondence with foreign citizens are casual and infrequent;

(d) 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

(e) foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

GUIDELINE C

Foreign Preference

9. 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.

10. Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

(a) the exercise of dual citizenship;

(b) possession and/or use of a foreign passport;

(c) military service or a willingness to bear arms for a foreign country;

(d) accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

(e) residence in a foreign country to meet citizenship requirements;

(f) using foreign citizenship to protect financial or business interests in another country;

(g) seeking or holding political office in the foreign country;

(h) voting in foreign elections; and

(i) 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.

11. Possible mitigating conditions: Conditions that could mitigate security concerns include:

(a) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

(c) activity is sanctioned by the United States; and

(d) the individual has expressed a willingness to renounce dual citizenship.

GUIDELINE D

Sexual Behavior

12. The concern. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion.[1] Sexual orientation or

[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.

preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

13. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) 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;

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

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

14. Possible mitigating conditions. Conditions that could mitigate security concerns include:

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

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

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

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

GUIDELINE E

Personal Conduct

15. 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 may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

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

(b) 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.

16. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying also include:

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

(b) 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;

(c) 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;

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

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

(f) association with persons involved in criminal activity.

17. Possible mitigating conditions. Conditions that could mitigate security concerns include:

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

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

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

(d) 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;

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

(f) 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

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

GUIDELINE F

Financial Considerations

18. 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.

19. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) a history of not meeting financial obligations;

(b) 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;

(c) inability or unwillingness to satisfy debts;

(d) unexplained affluence; and

(e) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

20. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) the behavior was not recent;

(b) it was an isolated incident;

(c) 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);

(d) 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;

(e) the affluence resulted from a legal source; and

(f) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

GUIDELINE G

Alcohol Consumption

21. 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.

22. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) 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;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

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

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

(e) habitual or binge consumption of alcohol to the point of impaired judgment; and

(f) consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

23. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) the alcohol-related incidents do not indicate a pattern;

(b) the problem occurred a number of years ago and there is no indication of a recent problem;

(c) positive changes in behavior supportive of sobriety; and

(d) 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.

GUIDELINE H

Drug Involvement

24. The concern.

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

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

(1) 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

(2) inhalants and other similar substances.

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

25. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

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

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

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

(d) 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

(e) 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.

26. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) the drug involvement was not recent;

(b) the drug involvement was an isolated or infrequent event;

(c) a demonstrated intent not to abuse any drugs in the future; and

(d) satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.

GUIDELINE I

Emotional, Mental, and Personality Disorders

27. 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 may be fully and properly evaluated.

28. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) an opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

(b) 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;

(c) a pattern of high-risk, irresponsible, aggressive, anti-social, or emotionally unstable behavior; and

(d) information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

29. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) there is no indication of a current problem;

(b) 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;

(c) 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.

GUIDELINE J

Criminal Conduct

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

31. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

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

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

32. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) the criminal behavior was not recent;

(b) the crime was an isolated incident;

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

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

(e) there is clear evidence of successful rehabilitation.

GUIDELINE K

Security Violations

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

34. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) unauthorized disclosure of classified information; and

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

35. Possible mitigating conditions. Conditions that could mitigate security concerns include actions that:

(a) were inadvertent;

(b) were isolated or infrequent;

(c) were due to improper or inadequate training; and/or

(d) demonstrate a positive attitude toward the discharge of security responsibilities.

GUIDELINE L

Outside Activities

36. 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.

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

(a) a foreign country;

(b) any foreign national;

(c) a representative of any foreign interest; and/or

(d) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

38. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities; and

(b) the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

GUIDELINE M

Misuse of Information Technology Systems

39. The concern. Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may 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.

40. Possible disqualifying conditions. Conditions that could raise a security concern and may be disqualifying include:

(a) illegal or unauthorized entry into any information technology system;

(b) illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;

(c) 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

(d) introduction of hardware, software, or media into any information technology system without

authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.

41. Possible mitigating conditions. Conditions that could mitigate security concerns include:

(a) the misuse was not recent or significant;

(b) the conduct was unintentional or inadvertent;

(c) the introduction or removal of media was authorized;

(d) the misuse was an isolated event; and

(e) the misuse was followed by a prompt, good faith effort to correct the situation.