

ORDER

1600.72A

CONTRACTOR AND INDUSTRIAL SECURITY PROGRAM



12/28/05

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

FOREWORD

This order formally documents the Federal Aviation Administration's (FAA) Contractor and Industrial Security Program, establishes and defines the policies and responsibilities for implementing the program in accordance with applicable laws and regulations, and initiates a quality assurance process that will ensure compliance with these policies.

As the FAA, our mission is to ensure safe, secure, and efficient air travel. Our ability to do this depends on the adequacy, reliability, and security of our facilities, automated systems, information, and resources.

We, along with other Federal Government agencies, have become dependent upon a growing cadre of contractors, consultants, and other individuals to support our mission. Those contractor employees, consultants, and other individuals are given the same access to our facilities, systems, information, and resources as Federal employees. Therefore, the security measures applied during the vetting process should be no less than those applied during the selection and hiring of Federal employees. This order is designed to ensure equal and fair application of security measures during the vetting process. These new policies will eliminate security weaknesses and tighten controls over the vetting of contractor employees, consultants, and other persons by ensuring appropriate risk assessments and security screenings are performed.

It is incumbent upon each associate administrator, vice president, director, manager, and FAA employee to ensure full understanding and compliance with this order since our security depends upon it.

A handwritten signature in black ink, reading "Marion C. Blakey". The signature is written in a cursive, flowing style.

Marion C. Blakey
Administrator

TABLE OF CONTENTS

| | Page No. |
|--|----------|
| FOREWORD..... | i |
| TABLE OF CONTENTS..... | ii |
| CHAPTER 1. GENERAL | |
| 1. Purpose..... | 1-1 |
| 2. Distribution | 1-1 |
| 3. Cancellation | 1-1 |
| 4. Definitions..... | 1-1 |
| 5. Authority to Change this Order | 1-1 |
| 6. Background..... | 1-2 |
| 7. Authority to Investigate Contractor Employees..... | 1-2 |
| 8. Exceptions to Requirements and Standards..... | 1-4 |
| 9. Scope..... | 1-4 |
| 10. Policies..... | 1-4 |
| CHAPTER 2. ROLES AND RESPONSIBILITIES | |
| 1. Responsibilities of the Administrator..... | 2-1 |
| 2. Responsibilities of Regional Administrators & Center Directors. . . | 2-1 |
| 3. Responsibilities of Directors of Offices & Services | 2-1 |
| 4. Responsibilities of the Office of the Assistant Administrator for Security & Hazardous Materials | 2-1 |
| 5. Responsibilities of All FAA Managers | 2-5 |
| 6. Responsibilities of the Contracting Officers (CO) | 2-6 |
| 7. Responsibilities of the Contracting Officer's Technical Representative (COTR). | 2-8 |
| 8. Responsibilities of the Operating Office..... | 2-9 |
| 9. Responsibilities of the Logistics Management Specialist (including those under airway facilities divisions) (LMS). | 2-10 |
| 10. Responsibilities of Real Estate Contracting Offices (RECO). | 2-11 |
| CHAPTER 3. CONTRACTOR AND INDUSTRIAL SECURITY OPERATIONS AND PROCUREMENT REVIEW | |
| 1. General | 3-1 |
| 2. Standards of Operation..... | 3-1 |
| 3. The Process..... | 3-1 |
| Figure 1. Contractor Security Screening Process | 3-2 |
| Figure 2. Industrial Security Screening Process | 3-3 |
| 4. Procurement Reviews | 3-4 |
| 5. Specific Review Actions..... | 3-4 |
| 6. Classified Contracts Requirements..... | 3-5 |
| 7. Post Award Actions..... | 3-5 |

| | Page No. |
|---|----------|
| CHAPTER 4. POSITION RISK/SENSITIVITY LEVEL DESIGNATIONS | |
| 1. Position Risk/Sensitivity Level Designation. | 4-1 |
| 2. Responsibility for Position Designations. | 4-1 |
| 3. Risk Levels. | 4-1 |
| 4. Sensitivity Levels. | 4-2 |
| 5. Documenting Position Risk/Sensitivity Level Designation. | 4-2 |
| Figure 3. FAA Form 1600-77. | 4-3 |
| Figure 4. Designation Codes. | 4-4 |
| 6. Sensitivity Level Designation | 4-5 |
| 7. Risk Level Designation | 4-5 |
| 8. Special Risk Level Designations. | 4-10 |
| Figure 5. Position Categories | 4-10 |
| 9. Preparation of FAA Form 1600-77. | 4-11 |
| 10. Common Contractor Positions and the Step-by-Step Procedures for Completing FAA Form 1600-77. | 4-13 |
| Figure 6. Contractor Position Risk/Sensitivity Level Designation Record (Sample). | 4-19 |
| CHAPTER 5. INVESTIGATIVE REQUIREMENTS AND INITIATION PROCEDURES | |
| 1. Introduction | 5-1 |
| 2. Types of Background Investigations. | 5-1 |
| 3. Investigative Requirements. | 5-2 |
| 4. Exemptions and Escort Requirements. | 5-4 |
| 5. Contract Janitorial, Construction, Maintenance, Property Management, & Repair Workers in Leased Facilities. | 5-6 |
| 6. Special Circumstance Investigative Requirements. | 5-7 |
| 7. Investigative Requirements for Immigrant & Non-Immigrant Aliens as Contractors. | 5-8 |
| 8. Exceptions to the Residency Requirement. | 5-10 |
| 9. Procedures for Request of a Residency Waiver. | 5-11 |
| 10. Investigative Requirements for AIS Access. | 5-12 |
| 11. Standards for Using & Obtaining Previous Investigations | 5-12 |
| 12. Process for Using & Obtaining Previous Investigations | 5-13 |
| 13. Funding for Contractor Security Screenings. | 5-14 |
| 14. Initiating and Closing Investigations. | 5-14 |
| 15. Filling Out Investigative Forms | 5-16 |
| 16. Closing & Adjudicating Investigations. | 5-18 |
| 17. Disposition of Incomplete/Closed Pending Investigations. | 5-18 |
| CHAPTER 6. SUITABILITY AND ADJUDICATION DETERMINATIONS | |
| 1. Application. | 6-1 |
| 2. Responsibility. | 6-1 |

| | Page No. |
|---|----------|
| 3. Suitability | 6-1 |
| 4. Suitability Requirements | 6-1 |
| 5. Suitability Adjudication | 6-2 |
| 6. Suitability Guidelines | 6-3 |
| 7. General Adjudication Process | 6-13 |
| 8. Issue Resolution | 6-14 |
| 9. Due Process | 6-16 |
| 10. Due Process Procedures | 6-17 |
| 11. Interim Suitability Determinations | 6-18 |
| 12. Interim Suitability Requirements | 6-18 |
| 13. Documentation & Notification | 6-19 |
| 14. Issuance of Identification (ID) Media | 6-19 |
| 15. Security Determinations | 6-20 |
| CHAPTER 7. CONTRACTOR PERSONNEL SECURITY RECORDS | |
| 1. Contractor Security Records | 7-1 |
| 2. Review of PSFs | 7-3 |
| 3. Safeguarding Records & Privacy Act Requirements | 7-4 |
| 4. Privacy Act Requirements | 7-5 |
| CHAPTER 8. NATIONAL INDUSTRIAL SECURITY PROGRAM | |
| 1. General | 8-1 |
| 2. Background | 8-1 |
| 3. Classified Contract Processing Procedures | 8-1 |
| 4. Annual Review of DD Form 254 | 8-2 |
| 5. Visit Requests | 8-2 |
| CHAPTER 9. QUALITY ASSURANCE REVIEW | |
| 1. Introduction | 9-1 |
| 2. Program Mission Statement | 9-1 |
| 3. Quality Assurance Review Standards | 9-1 |
| 4. Conducting the Quality Assurance Review | 9-2 |
| 5. Preparing the Report | 9-5 |
| 6. Findings and Recommendations | 9-5 |
| 7. Report Retention | 9-6 |
| Figure 8. Sample Quality Assurance Report | 9-7 |
| APPENDICES | |
| APPENDIX A. | |
| Glossary and Acronyms | A-1 |
| APPENDIX B. | |
| Interim Suitability Letter | B-1 |

| | Page No. |
|--|----------|
| APPENDIX C. | |
| Preparation of DD Form 254. | C-1 |
| APPENDIX D. | |
| OF 306, Declaration for Federal Employment. | D-1 |
| APPENDIX E. | |
| DOT F 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act. | E-1 |
| APPENDIX F. | |
| FAA Form 1600-74, Privacy Act Notice – Employees/Contractors. | F-1 |
| APPENDIX G. | |
| DOT F 1681, Identification Card/Credential Application. | G-1 |

CHAPTER 1. GENERAL

1. Purpose. This order establishes the Contractor and Industrial Security Program for the Federal Aviation Administration (FAA) and prescribes related policy, standards, criteria, and guidelines for security screening of contractor employees consistent with applicable laws, Executive Orders (E.O.), and Government-wide regulations to parallel the Personnel Security Program where practicable. It also furnishes servicing security elements (SSE) and other individuals assigned similar and related duties with standard procedures for implementing the directives and policies governing FAA's Contractor and Industrial Security Program. FAA Order 1600.1, Personnel Security Program, contains the policies and procedures necessary for investigation of persons working as employees or volunteers at FAA-sponsored child care services centers. FAA Order 1600.69, FAA Facility Security Management Program, contains the policies and requirements necessary for investigation of persons working as guards at our facilities.

Many contractor employees perform work that is essential for the conduct of the FAA mission. Because of their identification, the extent of their responsibility, and the risk levels of the positions they occupy, FAA investigates certain contractor employees, and other persons who have access by agreement of an FAA organization, to determine their suitability for access to FAA facilities, sensitive unclassified information, and resources.

2. Distribution. This order is distributed to all office and service directors in headquarters, offices within the Air Traffic Organization, all regions, the aeronautical and technical centers, and the security and logistics divisions in the regions and centers, with limited distribution to all logistics field offices and units.

3. Cancellation. This order cancels FAA Order 1600.72, Contractor and Industrial Security Program dated April 4, 2001, and FAA Order 1600.73, Contractor and Industrial Security Program Operating Procedures dated November 30, 2000.

4. Definitions. With respect to FAA's Contractor and Industrial Security Program, the definitions in Appendix A, Glossary and Acronyms, will apply. Contracting officers, logistics management and procurement divisions, logistics management specialists, real estate contracting offices, contracting organizations, and any other FAA component that are responsible for contracts will be hereafter referred to as logistics component. Contractor and subcontractor employees, consultants, and other persons who are not processed as visitors under FAA Orders 1600.74, Visitor Procedures for Federal Aviation Administration Facilities, will be hereafter referred to as contractor employees.

5. Authority to Change this Order. The Administrator reserves the authority to approve changes which establish or revise policy, delegate authority, or assign responsibility. The Assistant Administrator for Security and Hazardous Materials (ASH-1) can issue changes to this order as necessary to implement and manage the

program. All substantive changes will be coordinated with the Department of Transportation (DOT), Office of Security, M-40, Office of the Secretary of Transportation (OST).

6. Background. We, the FAA, use contractor employees to supplement, support, and even replace a growing segment of the Government workforce with increased emphasis on reinventing and streamlining Government processes. We utilize contractors, and contractor and subcontractor employees in support of virtually all aspects of our mission, including areas requiring access to classified national security information.

a. We must screen contractor employees to determine their suitability to work under an FAA contract in order to protect our facilities, sensitive unclassified information, and resources. We *do not* determine whom a contractor can employ, but we *do* reserve the right to restrict access to our facilities, sensitive information, and resources. A determination of a contractor employee's fitness for access to our facilities, sensitive unclassified information, and resources is known as a suitability determination and is made by a personnel security specialist (PSS) who is located in the SSE. We must also determine whether or not the use of contractor employees requiring access to classified national security information to perform under one of our contracts is in the best interest of national security. This is known as a security determination and is made by the Department of Defense (DOD).

b. With regard to classified contracts, DOT has the authority and responsibility as a contracting agency to perform the functions specified in the latest editions of the Department of Defense (DOD) National Industrial Security Program Operating Manual (NISPOM) and the Industrial Security Regulation (ISR). DOD grants facility clearances to contract companies as needed and security clearances to contractor employees when necessary for access to classified information. By agreement between DOT and DOD, DOD is authorized to act for, and on behalf of, DOT in providing security services for the protection of classified information that DOT releases to contract companies, contractor employees, and consultants.

7. Authority to Investigate Contractor Employees. Due to their affiliation, the extent of their responsibility, and the risk levels of the positions they occupy, FAA investigates contractor employees who have the same level of access to FAA facilities, sensitive unclassified information, and resources as do FAA employees in order to make suitability determinations.

a. On October 1, 1979, the Department of Justice (DOJ) rendered an opinion 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. Those 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, have the right to 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 must 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 unclassified data.

c. E.O. 12829 established the National Industrial Security Program (NISP) on January 6, 1993, to safeguard Federal Government classified information that is released to contractors, and it provides for the protection of information classified pursuant to E.O. 12958, Classified National Security Information, and the Atomic Energy Act of 1954, as revised. This E.O. appointed the Secretary of Defense as the Executive Agent for inspecting and monitoring contractors, licensees, and grantees who require or will require access to or who store or will store classified information and for determining the eligibility for access to classified information of such contractors, licensees, and grantees, and their respective employees. This order requires that the heads of all Federal agencies enter into agreements with the Secretary of Defense that establish the terms of the Secretary’s responsibilities on behalf of these agency heads. The FAA has entered into such an agreement and identified the Defense Security Service (DSS) as the primary agency responsible for conducting and adjudicating the background investigations on contractor employees and applicants, making the security determinations, and granting the security clearances for the FAA.

d. DOD Directive 5200.2, DOD Personnel Security Program, dated April 9, 1999, updated the policy and responsibilities changes to E.O. 12958 and E.O. 12968, Access to Classified Information. This directive prescribes that “the objective of any [contractor] personnel security program is that . . . contractor [employees] assigned to and retained in sensitive positions in which they could potentially damage national security are and remain reliable and trustworthy, and [that] there is no reasonable basis for doubting their allegiance to the United States.” This directive continues authorization for the publication of DOD Directive 5200.2-R, Personnel Security Program, which established uniform common adjudicative standards for contractor security background investigations.

e. DOD Directive 5220.22-M, NISPOM, January 1995, establishes investigative requirements pertaining to contractor employees and prescribes for uniform common adjudicative standards paralleling the requirements and standards for Federal Government employees set forth in E.O. 12968. The NISPOM authorizes the FAA to restrict or otherwise control contractor employee access to classified information in the interest of national security. The requirements set forth in this manual apply to the release of classified information during all phases of the contracting process to include: bidding, negotiation, award, performance, termination, and the licensing or grant process with or under the control of the FAA.

f. Other authorities and references.

(1) 5 CFR 731, Suitability.

(2) 5 CFR 736, Personnel Investigations.

(3) Public Law 100-235, Computer Security Act of 1987.

8. Exceptions to Requirements and Standards. FAA offices must submit all requests to any exception to the requirements and standards contained in this order to ASH-1 through the Office of Internal Security and Investigations (AIN-1) for approval. They must provide AIN-1 with a complete copy of the proposed office, service, center, or region order or supplement to this order that contains the exception(s) in support of the request.

9. Scope. The provisions of this order apply to persons employed as, or by contractors, subcontractors, consultants, or any other persons (not visitors) who have access to our facilities, sensitive unclassified information, and resources.

10. Policies. Contractor and industrial security policies applicable throughout the FAA are as follows:

a. Except as stated in this order, FAA will apply the Personnel Security Program policies and procedures pertaining to risk levels and investigative requirements to contractor employees and applicants who have comparable exposure (i.e., Federal employees in similar positions) to their facilities, sensitive unclassified information, and resources where practicable.

b. FAA will implement the requirements and procedures set forth in E.O. 12829 and the NISPOM, as necessary.

c. FAA will not allow a person to work under a contract unless a determination has been made on behalf of the Administrator that the person's work under the contract will promote the efficiency of the service.

d. FAA must ensure that applicants or persons who are not U.S. citizens but currently work or provide services or goods under FAA contracts within the United States have resided in the United States for 3 of the last 5 years, unless exempt from the investigative requirements in chapter 5, or a waiver of this requirement is requested and approved by AIN-1 (or designee) prior to contract award or prior to the contract employee beginning work.

e. FAA must ensure that all persons applying for work or providing services or goods under a classified contract are U.S. citizens or permanent resident aliens, except as provided for in chapter 5, paragraph 7b.

f. The FAA will not grant a person access to classified information unless that person possesses a valid need to know and has been determined to be eligible for access by DOD under DOD Directive 5200.2-R.

g. FAA will conduct appropriate background investigations on all contractor employees unless they are exempted in accordance with chapter 5, paragraphs 4, and 8d and e, as determined by the SSE. These investigations will serve as the basis for a suitability determination.

h. FAA will *not* consider a person to have been granted a security clearance for access to classified information solely on the basis of the successful completion of a required investigation.

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

j. FAA will not prevent any contractor employee or applicant from having access to its facilities, sensitive unclassified information, or resources because of information revealed in a background check unless they are given an opportunity to respond to any

information used as a basis to deny such access. FAA will give contractor employees and applicants an opportunity to explain or refute derogatory information used as the basis for any adverse action taken against them.

k. FAA may disclose investigative records and contractor personnel security files only to the extent necessary under the latest editions of FAA Order 1270.1, Freedom of Information Act Program, and FAA Order 1280.1, Protecting Privacy of Information about Individuals.

CHAPTER 2. ROLES AND RESPONSIBILITIES

1. Responsibilities of the Administrator. The Administrator ensures that FAA maintains a Contractor and Industrial Security Program consistent with applicable laws, regulations, and orders and that the use of persons performing work or providing services or supplies under a contract will promote the efficiency of the service.

2. Responsibilities of Regional Administrators and Center Directors. Regional administrators and center directors ensure implementation of and compliance with this directive in their respective regions and centers through their logistics and contracting organizations, security, and any other organization that reports directly to them as appropriate.

3. Responsibilities of Directors of Offices and Services. Directors of offices and services, including subordinates in regional and field office facilities, ensure that their subordinates understand and comply with contractor security program requirements.

4. Responsibilities of the Office of the Assistant Administrator for Security and Hazardous Materials.

a. The Assistant Administrator for Security and Hazardous Materials (ASH-1) implements the contractor security program throughout the FAA and ensures that resources needed for conducting an effective program are available and efficiently used.

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

c. Director, Office of Field Operations (AHS-1). AHS-1 is responsible for program operations and direct implementation by the servicing security element (SSE) in the regions and centers.

d. Manager, Personnel Security Division (AIN-400). Under AIN-1, AIN-400 is responsible for:

(1) Implementing and maintaining an effective Contractor and Industrial Security Program.

(2) Designating personnel security specialists who are appropriately trained to implement the personnel security responsibilities of the division.

- (3) Ensuring compliance with contractor security and suitability investigative requirements.
- (4) Ensuring that appropriate training is provided for designating position risk and sensitivity levels, and for security and suitability adjudication.
- (5) Ensuring that position risk and sensitivity levels are properly determined.
- (6) Adjudicating suitability issues, verifying security clearances, and, as necessary, coordinating the removal of contractor employees with the logistic components.
- (7) Evaluating the effectiveness of the program through quality assurance reviews and program evaluations.
- (8) Preparing security program reports for and on behalf of AIN-1.
- (9) Providing guidance and direction throughout the agency on all contractor security matters.
- (10) Performing all functions of the SSE. (Refer to paragraph 4f of this chapter.)
- (11) Granting or denying residency waiver requests for foreign nationals.

e. Managers of the Security and Hazardous Materials Divisions (AXX-700). Under the direction of AHS-1, the managers of the Security and Hazardous Materials Divisions are responsible for:

- (1) Implementing and maintaining an effective Contractor and Industrial Security Program within their area of responsibility.
- (2) Designating personnel security specialists who are appropriately trained to implement the personnel security responsibilities of the division.
- (3) Ensuring appropriate training is provided for designating position risk and sensitivity levels and for suitability adjudication.
- (4) Providing guidance to operating offices and logistics components on contractor and industrial security policies and procedures.
- (5) Overseeing the effectiveness of the Contractor and Industrial Security Program.
- (6) Ensuring that their personnel are provided training on the most current FAA-approved contracts database.

f. Servicing Security Elements (SSE). The following statements comprise a broad overview of the duties and responsibilities of the SSE. Generally, these responsibilities are assigned to personnel security specialists who are located in the SSE.

- (1) Ensuring compliance of the Contractor and Industrial Security Program policies and procedures established by this order.
- (2) Providing guidance to operating offices, logistics components, and, occasionally, the contract companies on contractor and industrial security policies and operating procedures.
- (3) Providing the logistics component with all DOT/FAA security directives that the contractor needs to fulfill security responsibilities under the contract.
- (4) Determining, in consultation with operating offices and logistics components, which contracts, purchase orders (PO), lease agreements, and memoranda of agreement (MOA), etc., require investigation of contractor employees and ensure they contain appropriate language for investigation of the proposed contractor employees.
- (5) Coordinating with operating offices and logistics components in developing appropriate personnel security clauses for contracts, POs, lease agreements, and MOAs, etc., that contain work, services, or other duties to be performed or provided by contractor employees.
- (6) Assisting operating offices and logistics components in determining whether use of foreign nationals and immigrant aliens on FAA contracts, POs, lease agreements, and MOAs, etc., is in the best interest of the agency and whether access to classified information and sensitive unclassified information is required in order for the foreign national(s) or immigrant alien(s) to perform or provide services under the contract.
- (7) Submitting all requests to waive the residency requirement for foreign nationals to AIN-1 for approval or denial.
- (8) Reviewing FAA Form 1600-77, Contractor Position Risk/Sensitivity Level Designation Record, in conjunction with the Statement of Work (SOW), and DD Form 254, if applicable, to ensure risk/sensitivity level designations are correct and appropriate, and approve or disapprove as required. Maintaining copies of all FAA Forms 1600-77 either electronically or in hardcopy format.
- (9) Receiving and reviewing investigative forms for completeness; identifying and addressing any issues or areas of concern; granting or denying interim suitability and notifying the logistics component; and initiating the required

investigation, as appropriate. If interim suitability is denied, coordinating with the contracting officer (CO) who will coordinate with the operating office in determining whether or not to initiate the investigation.

(10) Lending support to AIN-400 by reviewing, processing, and adjudicating investigative forms for contractor employees assigned to national contracts, and advising them of issues warranting action.

(11) During interim suitability and final adjudication stages, coordinating any adverse action concerning a *national* contractor employee to AIN-400 *prior* to taking any action.

(12) Verifying with the national investigations indices for prior investigations concerning contractor employees when appropriate.

(13) Notifying the logistics component and operating office (if applicable) in writing when an interim suitability determination is made, and documenting files and databases accordingly.

(14) Entering contractor employee information into the contractor database immediately upon receipt of paperwork.

(15) Initiating appropriate security screenings on contractor employees within 5 - 10 working days if all information on security forms is accurate and complete.

(16) Ensuring that all incomplete investigative forms are corrected in a timely manner.

(17) Reviewing investigative reports to determine the adequacy of the investigation; evaluating the investigative results; identifying suitability issues; and adjudicating suitability in accordance with the personnel suitability standards and criteria set forth in chapter 6, Suitability and Adjudication Determinations, of this order and in consultation with other offices on a need-to-know basis.

(18) Prior to taking any adverse action, providing due process to contractor employees either during the interim suitability phase or upon completion of the background check.

(19) Resolving suitability issues by conducting or arranging for additional investigation, and notifying the logistics component of results.

(20) Notifying the logistics component and operating office (if applicable) in writing of any contractor employee found unsuitable for access to FAA facilities, sensitive unclassified information, or resources and recommending that appropriate action be taken.

(21) Taking appropriate action when information surfaces that raises a question about a contractor employee's continued suitability; i.e., temporarily having the contractor employee removed from the contract pending the outcome of any additional investigation, suspending access to the contractor employee, etc.

(22) Reviewing security clauses for classified contracts, POs, lease agreements, and MOAs, etc., to ensure they contain language specifying that requests for classified visits be made and prepared in accordance with the DOD National Industrial Security Program Operating Manual (NISPOM).

(23) Reviewing and initialing DD Form 254, Contract Security Classification Specification (refer to Appendix C), for all classified contracts, POs, lease agreements, and MOAs, etc., to ensure appropriate classification.

(24) Maintaining records on contractor employee background investigations in an automated information system that AIN-1 has approved for this purpose.

(25) Reconciling periodic contractor employee reports (quarterly/biannually or as required by the contract) that are submitted by the contract company per contract clause requirement for persons who have access to programs, facilities, and sensitive information.

(26) Maintaining contract security files (CSFs) for contracts with a security requirement and contractor personnel security files (PSFs) for contractor employees when needed.

(27) Maintaining records of contractor-certified visit requests.

(28) Advising operating offices of all changes in costs of background investigations.

5. Responsibilities of All FAA Managers. All FAA managers are responsible for:

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

b. Identifying and reporting to the SSE any significant deviation from contractor security standards, criteria, or procedures.

c. Reporting to the SSE any information they discover that may raise a question about the suitability of a contractor employee.

d. Ensuring that proper escort procedures found in chapter 5 of this order and FAA Order 1600.69, FAA Facility Security Management Program, are followed when it is determined that a contractor employee must be escorted.

e. Budgeting for the costs of conducting contractor investigations, or coordinating with the SSE to ensure budgeting for these costs, and providing the SSE with appropriation codes as needed.

6. Responsibilities of the Contracting Officers (CO). Unless delegated, the CO is responsible for:

a. Providing the contractor with all applicable security regulations, policies, and guidance and assisting the SSE by ensuring the contractor complies with the requirements set forth in the security regulations.

b. Ensuring that the SSE receives all procurement actions with security implications during the pre-award stage.

c. Ensuring the SSE is notified whenever the status of a contract, PO, MOA, etc., is changed (e.g., renewed, terminated, etc.) or when the status of a contractor employee changes (e.g., terminates, resigns, etc.).

d. Ensuring that whenever the SSE has determined that a contract, PO, or MOA, etc., requires investigation of any contractor employee, it contains sufficient language in the security clause to achieve this objective.

e. Taking appropriate action under the contract if the SSE determines that a contractor employee is unsuitable in view of contract security clause requirements, and notifying the SSE and operating office when action is taken.

f. Ensuring that position risk/sensitivity level designations determined by the operating office (refer to chapter 4 of this order) are forwarded to the SSE on FAA Form 1600-77 for review and approval prior to any contractor employee beginning work on the contract; and retaining the original, approved FAA Form 1600-77 either electronically or in hardcopy format.

g. Working with the SSE to establish procedures for contractor employees to submit investigation forms directly to the SSE or to the CO for forwarding to the SSE. Because of the sensitive nature of these forms and Privacy Act requirements, the procedures must ensure that the forms are submitted directly to FAA in a sealed envelope and that neither the employee's supervisor nor other company personnel have access to them, unless the company established procedures which allows them to review the forms with the consent of the contractor employee.

h. Ensuring the SSE is provided with the identification of the funding line of business or operating office for background checks, and, if required, the names of the CO and COTR; and a transmittal letter by the contracting company containing the contract number, a list of the names of all proposed contractor employees, position titles, and duty location, if applicable.

i. Working with the operating office to ensure that no contractor employee has access to any FAA facilities, resources, or sensitive unclassified information until the SSE has notified them that interim suitability was granted to the individual.

j. Notifying contract companies and operating offices that interim suitability was granted or denied for a contractor employee, when this information is provided to them by the SSE.

k. Ensuring that contractor employees are following proper escort procedures when contracts call for escorting.

l. Ensuring the SSE is notified when information surfaces that raises a question about the suitability of a contractor employee while the individual is working on the contract.

m. Assisting the SSE in obtaining from the contract company, either quarterly, biannually, or as required by the contract, a listing of all contractor employees who have access to FAA facilities, resources, and sensitive unclassified information, when the SSE requests assistance. In conjunction with contract clause requirements, this list should contain the complete full name of the contractor employee, in alphabetical order, their social security number, and the contract number. Social security numbers must be omitted from reports that are provided to the CO and operating office.

n. Coordinating with the SSE and operating office to ensure all proposed contracts, POs, and MOAs, etc., requiring contractor employees needing access to classified information, contain language that clearly identifies this requirement prior to solicitation.

o. Working with the SSE and operating office to determine whether there is a need to share classified information with a contractor, consultant or other non-FAA person during pre-contract negotiations on all proposed contracts, POs, and MOAs, etc.

p. Ensuring security clauses for classified contracts, POs, and MOAs, etc., also contain language specifying that requests for classified visits be made and prepared in accordance with the NISPOM, prior to forwarding to the organization to be visited.

q. Completing and signing DD Form 254 with the award of each classified contract, PO, or MOA, etc. (Signature approval can be delegated to the operating office.)

r. Providing the SSE with a copy of DD Form 254 for their review and initialing, and sending them a copy after its been signed.

s. Coordinating with the appropriate Defense Security Service (DSS) office to determine if any prospective bidders require processing for a security clearance in accordance with the NISPOM and other applicable DOD regulations. When this is required, the CO must sign and issue a DD Form 254 for each affected screening information request.

t. Coordinating with the SSE and operating office to develop appropriate security clauses for classified contracts, POs, and MOAs, etc. Under the NISPOM and other applicable DOD regulations, ensuring that FAA and DSS processes all contractor employees for facility or security clearances, and notifies the SSE when security clearances are granted.

u. Participating in periodic evaluations of the Contractor and Industrial Security Program to ensure its effective and efficient operation and compliance with this order.

v. Ensuring the integrity of all data entered into an FAA-approved database that is used to store, track, monitor, or retrieve contract information.

7. Responsibilities of the Contracting Officer's Technical Representative (COTR):
The COTR is responsible for:

a. Notifying the SSE and CO whenever a contractor employee has completed work or leaves his or her position under a contract, PO, or MOA, etc.

b. Working with the SSE and CO on all contracts, POs, lease agreements, and MOAs, etc., as to whether or not there is an investigative requirement for individuals having access to FAA facilities, sensitive unclassified information, or resources, and ensuring that the contract contains sufficient language in the security clause to meet that objective.

c. Ensuring the SSE is provided with the identification of the funding line of business or operating office for background checks, if required; the names of the CO and COTR; and a transmittal letter by the contracting company which contains the contract number, an alphabetical list of the names of all proposed contractor employees, and duty location, if applicable.

d. Maintaining a listing of all contractor employees on their contracts, and coordinating with the SSE to ensure accuracy.

e. Determining position risk/sensitivity level designations (refer to chapter 4 of this order), along with the CO and SSE, and ensuring the designations are recorded on FAA Form 1600-77 and submitted to the SSE for review and approval prior to any contractor employee beginning work on the contract.

f. Ensuring no contractor employee has access to FAA facilities, sensitive unclassified information and resources until the SSE has notified the CO that they granted interim suitability.

g. Ensuring the SSE is notified when information surfaces that raises a question about the suitability of a contractor employee.

h. Ensuring that contractor employees are properly escorted, when required.

8. Responsibilities of the Operating Office. The operating office is responsible for:

a. Coordinating with the SSE and logistics component on all contracts, POs, lease agreements, and MOAs, etc., as to whether or not there is an investigative requirement for individuals having access to FAA facilities, sensitive unclassified information, or resources. Included are situations where operating offices exercise authority to purchase or contract for services directly without significant involvement on the part of a separate contracting office.

b. Ensuring that position risk/sensitivity level designations are forwarded to the SSE on FAA Form 1600-77 for review and approval prior to any contractor employee beginning work on the contract; and retaining an approved copy of FAA Form 1600-77 either electronically or in hardcopy format.

c. Ensuring that whenever the SSE has determined that persons to be granted access to an FAA facility, sensitive unclassified information, or resources under an unclassified contract, PO, lease agreement, or MOA, etc., would require investigation, the contract contains language sufficient to achieve this objective.

d. Determining, in consultation with the logistics component and the SSE, whether use of foreign nationals or immigrant aliens on FAA contracts, POs, lease agreements, and MOAs, etc., is in the best interest of the FAA.

e. Notifying the SSE of any questionable conduct that might affect the suitability of contractor employee.

f. Coordinating with the CO to ensure that the contract company takes appropriate action when a contractor employee is found unsuitable, and notifying the SSE when action is taken.

g. Ensuring that contractor employees are properly escorted, when required.

h. Maintaining a listing of all contractor employees working on contracts specific to their office.

i. Budgeting for the costs of conducting contractor investigations, coordinating with the SSE to ensure budgeting for these costs and providing the SSE appropriation codes as needed.

j. Maintaining records of all contractor employees granted security clearances by DSS working within their facilities. Records should be maintained as prescribed by the latest edition of FAA Order 1280.1, Protecting Privacy of Information About Individuals.

k. Reviewing all proposed contracts, POs, and MOAs, etc., to determine whether the FAA needs to share classified information with a contractor, consultant, etc., during pre-contract negotiations.

9. Responsibilities of the Logistics Management Specialist (LMS). The LMS, generally located in the Air Traffic Organization, is responsible for:

a. Ensuring that all new, modified, or renewed contracts, POs, and MOAs, etc., for which they are responsible have been coordinated with the SSE for review and determination of applicable personnel security investigative requirements prior to award.

b. Notifying the SSE and CO whenever the status of a contract, PO, MOA, etc., or a contractor employee changes which would impact personnel security requirements or access to FAA facilities, sensitive unclassified information, and resources.

c. Coordinating with the CO to ensure that the contract company takes appropriate action when a contractor employee is found unsuitable.

d. Ensuring that position risk level designations are determined (refer to chapter 4 of this order) and forwarded to the SSE on FAA Form 1600-77 for review and approval prior to any contractor employee beginning work, and retaining a copy of the approved form either electronically or in hardcopy format.

e. Coordinating with the CO and operating office in determining whether use of foreign nationals or immigrant aliens on FAA contracts, POs, lease agreements, and MOAs, etc., is in the best interest of the agency.

f. Ensuring that no contractor employee has access to any FAA facility, sensitive unclassified information, and resources within FAA until the SSE has granted interim suitability.

g. Ensuring that contractor employees are following proper escort procedures when contracts call for escorting.

h. Ensuring the SSE and CO are notified when information surfaces that raises a question about the suitability of a contractor employee.

i. Ensuring appropriate action is taken immediately upon notification that a contractor employee is determined by the SSE to be unsuitable for access to FAA facilities, sensitive unclassified information, classified information, or resources.

10. Responsibilities of Real Estate Contracting Officers (RECO): RECOs are responsible for:

a. Providing the contractor with all applicable security regulations, policies, and guidance, and ensuring the contractor complies with the requirements set forth in the security regulations.

b. Ensuring all new, modified, or renewed lease agreements containing janitorial, construction, maintenance, property management, or repair work, have been coordinated with the SSE for review and determination of applicable personnel security investigative requirements prior to award.

c. Ensuring the SSE is notified whenever the status of a contract, PO, lease agreement, MOA, etc., or contractor employee changes (i.e., replaced, defaulted, terminated, etc.) which impacts personnel security requirements or access to FAA facilities, sensitive unclassified information, and resources.

d. Ensuring that whenever the SSE has determined that a contract, PO, lease agreement, or MOA, etc., requires investigation of any contractor employee, it contains language sufficient to achieve this objective.

e. Ensuring appropriate action is taken immediately upon notification by the SSE that a contractor employee is found unsuitable for access to FAA facilities, sensitive unclassified information, classified information, or resources.

f. Requiring that the contract company take appropriate action including removal of an employee from working on an FAA contract if it is determined that the person is unsuitable and notifying the SSE when action is taken.

g. Ensuring that position risk level designations determined by the operating office (refer to chapter 4, of this order) are forwarded to the SSE on FAA Form 1600-77 for review and approval prior to any contractor employee beginning work on the contract, and retaining a copy of the approved form either electronically or in hardcopy format.

h. Working with the SSE to establish procedures for contractor employees to submit investigation forms directly to the SSE or to the RECO for forwarding to the SSE. Because of the sensitive nature of these forms, and Privacy Act requirements, the procedures must ensure that the forms are submitted directly to FAA in a sealed envelope

and that neither the employee's supervisor nor other company personnel have access to them, unless the company established procedures which allows them to review the forms with the consent of the contractor employee.

i. Ensuring the SSE is provided with the identification of the funding line of business or operating office for background checks and name of the RECO, and that all completed security packages contain a transmittal letter by the contracting company containing the contract number, an alphabetical list of the names of all proposed contractor employees, and duty location (if applicable).

j. Ensuring that no contractor employee works in any position within FAA until the SSE has granted interim suitability.

k. Notifying contract companies that interim suitability was granted or denied for a contractor employee.

l. Ensuring the SSE is notified of any information that raises a question about the suitability of a contractor employee.

m. Ensuring that contract companies provide a listing of all contractor employees who have access to FAA facilities, resources, and sensitive unclassified information on a quarterly or biannual basis, or as required by the contract.

n. Ensuring all proposed contracts, POs, lease agreements, and MOAs, etc., requiring contractor employees who need access to classified information contain language in the security clause that clearly identifies this requirement prior to solicitation in coordination with the SSE and operating office.

o. Reviewing all proposed contracts, POs, lease agreements, and MOAs, etc., to determine whether the agency needs to share classified information with a contractor, consultant or other non-FAA persons during pre-contract negotiations.

p. Coordinating with the appropriate DSS office to determine if any prospective bidders require processing for a security clearance in accordance with the NISPOM or other applicable DOD regulations. When this is required, sign and issue a DD Form 254 for each affected proposal, invitation for bid, request for quotation, or other solicitation.

q. Coordinating with the SSE and operating office to develop appropriate security clauses for classified contracts, POs, lease agreements, and MOAs, etc., to ensure that FAA and DSS can process all contractor employees for any needed facility or security clearances, and to do so according to requirements and procedures stated in the NISPOM or other applicable DOD regulations.

r. Ensuring security clauses for classified contracts, POs, lease agreements, and MOAs, etc., also contain language in the security clause specifying that requests for

classified visits be made and prepared in accordance with the NISPOM, prior to forwarding to the organization to be visited.

s. Completing and signing DD Form 254 with the award of each classified contract, PO, or MOA, etc. (Signature approval can be delegated to the operating office.)

t. Providing a copy of DD Form 254 to the SSE for their review and initialing, and sending them a copy when signed.

u. Participating in periodic evaluations of the Contractor and Industrial Security Program to ensure its effective and efficient operation and compliance with this order.

v. Ensuring the integrity of all data entered into any automated information system used to store, track, monitor, or retrieve contract information.

CHAPTER 3. CONTRACTOR AND INDUSTRIAL SECURITY OPERATIONS AND PROCUREMENT REVIEWS

1. General. This chapter outlines the process and prescribes the FAA's standards and responsibilities for conducting contractor and industrial security operations and for maintaining contractor security records.

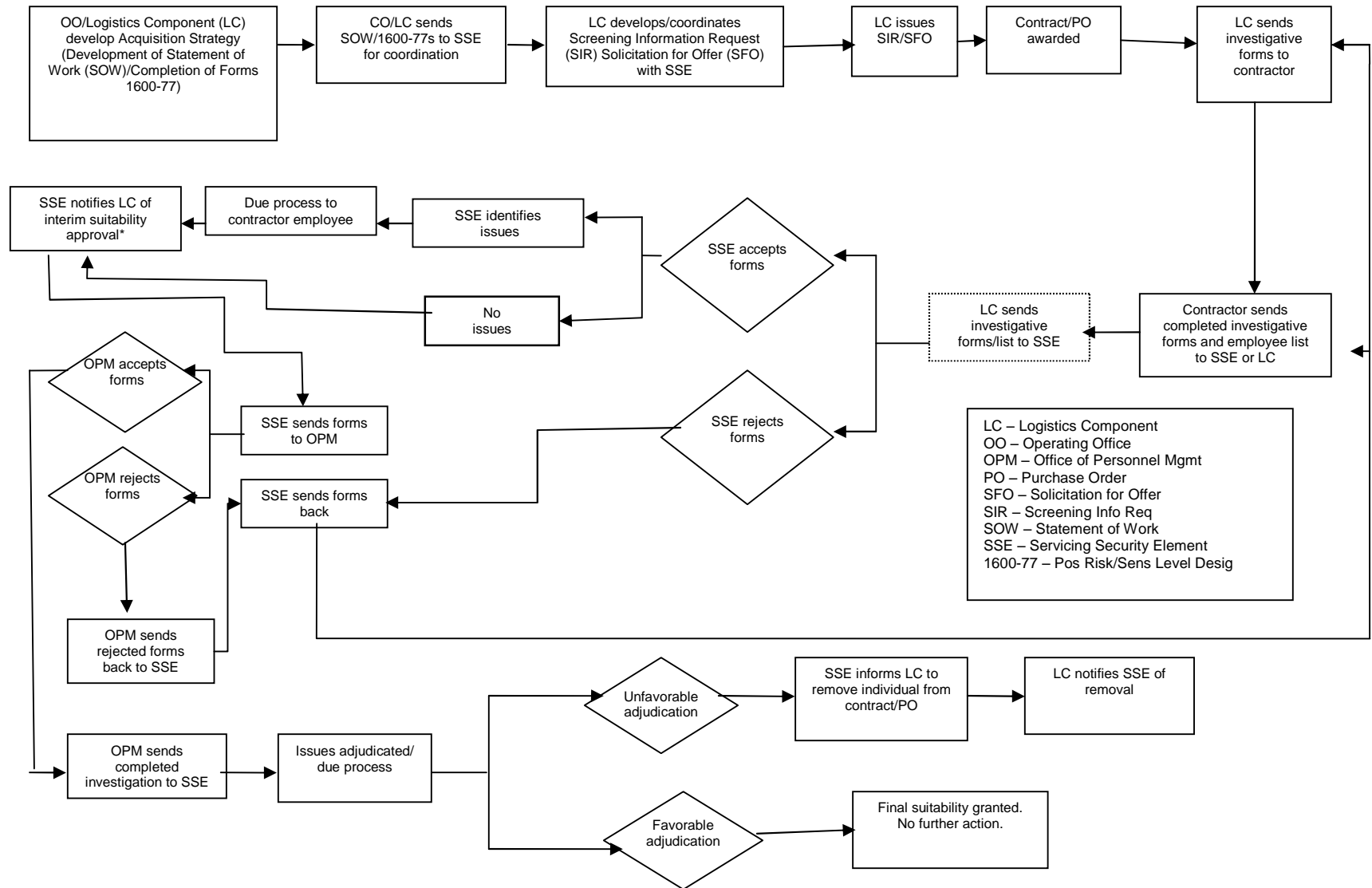
2. Standards of Operation. FAA contractor and industrial security operations must meet the following standards:

a. Organization levels will conduct and closely control the operations to ensure they comply with FAA and DOT requirements, and manage the operations in an efficient and effective manner.

b. Managers of servicing security elements (SSE) will direct contractor and industrial security operations. They can delegate responsibility for suitability adjudication to personnel security specialists (PSS) who are fully trained to evaluate reports and results of background investigations. PSSs must successfully complete the Office of Personnel Management's (OPM) security and suitability adjudication course, or an equivalent course, prior to being authorized to adjudicate cases.

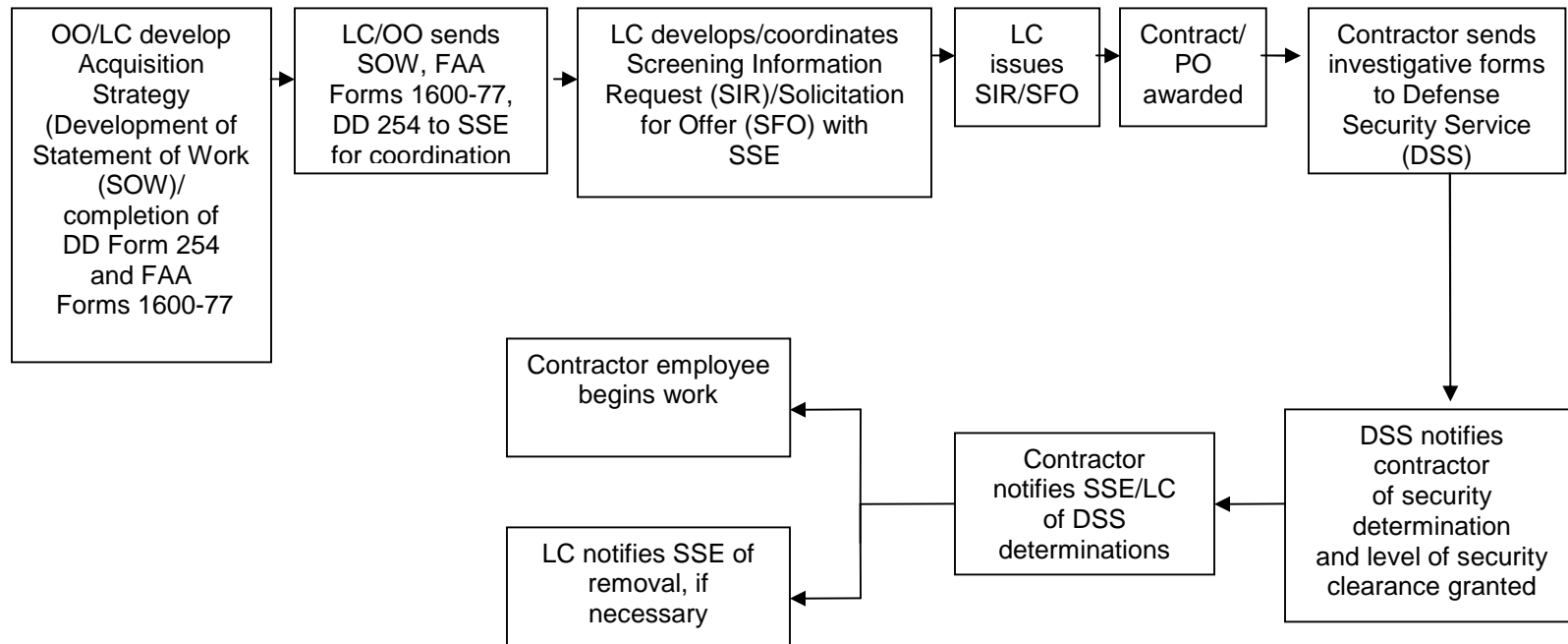
3. The Process. There is a sequential process by which suitability and security determinations are made that allow contractor employees to begin work or provide services or goods under an FAA contract. Each step is essential to the process and is conducted in a specific sequence in order for the process as a whole to succeed. For example, completion of FAA Form 1600-77, Contractor Position Risk/Sensitivity Level Designation Record, (chapter 4) determines the level and type of security screening required for each position under a given contract. If this form is completed out of sequence or is omitted altogether, then the type of investigation or security determination cannot be made. Without this information, a contractor employee cannot begin work or provide services or goods under a contract. Figure 1, Contractor Security Screening Process, illustrates each step of the process for making suitability determinations in appropriate sequential order. These steps are addressed in this and the remaining chapters of this order. Figure 2, Industrial Security Screening Process, illustrates the steps in the process for making security determinations for access to classified information in which the FAA has an active role. The background investigations for contractor employees requiring access to classified information are controlled and conducted by the Office of Personnel Management for the Defense Security Service (DSS).

Figure 1. Contractor Security Screening Process



*Interim suitability denials can be found in chapter 6.

Figure 2. Industrial Security Screening Process



DSS – Defense Security Service
 LC – Logistics Component
 OO – Operating Office
 PO – Purchase Order
 SFO – Solicitation for Offer
 SIR – Screening Information Request
 SOW – Statement of Work
 SSE – Servicing Security Element

Form 1600-77 – Position Risk/Sensitivity Level Designation
 DD 254 - Contract Security Classification Specification

4. Procurement Reviews. One way that FAA can improve the protection of security interests is by cooperation and timely exchange of information between the Office of Internal Security and Investigations, Personnel Security Division, AIN-400; regional, center, and field SSEs (AXX-700); the Vice President of Acquisition and Business Services, ATO-A; Office of Information Services (AIO); Office of Regions and Center Operations (ARC); and the regional, center, and field logistics components. These reviews identify what security screenings, if any, are required for the proposed contractor employees and precede all other operational actions relative to the Contractor and Industrial Security Program.

- a.** The logistics component must ensure that they send the PSS all procurement actions with security implications during the pre-award stage.
- b.** The PSS must review all SOWs, new contracts, modifications, and renewals of contracts with security requirements that contain work, services, supplies, or other duties to be performed or provided by contractor employees to ensure appropriate language is included to allow for the conduct of security screenings when necessary.
- c.** The PSS must work with operating offices and logistics components in determining which contracts, POs, lease agreements, and MOAs are classified or which involve access to classified information by contractor employees, and ensure that appropriate language is in the clause which clearly identifies this requirement. A completed DD Form 254, Contract Security Classification Specification, must be completed by the operating office prior to release or award.
- d.** The PSS must review all FAA Forms 1600-77 to ensure they have been properly completed, and subsequently approve the position risk or sensitivity level designations.

5. Specific Review Actions. The PSS must review all procurement actions or notification that a procurement action requires review in a timely manner. Using the following five areas as a guideline, they must determine the necessary security requirements: 1) access to classified national security information; 2) access to sensitive FAA information; 3) access to FAA telecommunications and automated information systems; 4) use of FAA-owned or leased facilities, buildings, vehicles, or other property; and, 5) escort requirement. After determining the security requirement, the PSS must:

- a.** Ensure that the security clause includes a statement that the contractor must be continuously escorted (refer to chapter 5, paragraph 4) if access is limited to FAA facilities with escort for a short period of time.
- b.** Ensure the appropriate security clause(s) are included in the Screening Information Requests/Solicitations for Offer, and check with the logistics component for the most current clause or access the logistics component database.

- c. Return review results to the logistics component, as applicable.
- d. Maintain a record of all review actions for the life of the contract.

6. Classified Contracts Requirements. Due to potential damage to the national security that can be caused by the unauthorized disclosure of classified information, the following requirements apply to classified contracts in addition to any standard security clauses that may apply. The PSS and the logistics components should work together to make sure:

- a. All classified contracts, POs, lease agreements, and MOAs, etc., contain a DD Form 254, Contract Security and Classification Specification. This form is designed to provide the contract company with the security requirements and classification guidance needed to perform under a classified contract.
- b. All classified solicitations and DD Forms 254 are coordinated by the logistics component with the PSS prior to award. (A blank DD Form 254 and detailed instructions for completing the form can be found in Appendix C.)
- c. Investigations processed under the DOD Directive 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) are:
 - (1) Submitted by the contract company to DSS.
 - (2) Conducted by DSS.
 - (3) Certified by the contract company's facility security officer and sent to the SSE, or verified by the SSE.
- d. Security clearances that are processed under the NISPOM are granted by DSS. The contract company's facility security officer should forward certification of security clearance information to the SSE for contractor employees who are assigned to work on classified contracts.
- e. If there are special security requirements (i.e., intelligence) that warrant oversight by FAA, the logistics component can establish a *carve out* that relieves DSS from contractor industrial security inspection responsibility in whole or in part, and places the responsibility on the FAA. Carve outs are normally established for special access programs and are generally a portion of an already existing contract.

7. Post Award Actions. In addition to constant communication between the PSS, logistics component, COTR, and the responsible operating office, the following actions are essential for maintaining an effective liaison.

a. The logistics component must ensure that all amendments, modifications, revisions, and renewals of existing contracts, POs, lease agreements, and MOAs, etc., *with a security requirement* are routed through the SSE for the PSS to review, even if the original document did not contain a security requirement.

(1) Logistic components do not need to send the PSS any amendments, etc., in cases where changes *do not* affect the security posture of the contract.

(2) Logistic components must submit proposed changes along with FAA Forms 1600-77 (if any positions are affected), to the PSS for their review prior to inclusion in the contract. This should be done in cases where changes *do* affect the security posture.

(3) Logistics components must notify the PSS of all expired contracts or contracts that were renewed under a new contract number.

b. The logistics component, COTR, and operating office must ensure notification is provided to the PSS when a contractor employee is terminated, changes contracts, or leaves his or her position within 5 days of the event. When received, the PSS must update the information in the Investigations Tracking System.

c. The PSS must ensure the logistics component and/or contract company and COTR are notified in writing when:

(1) interim suitability determinations (Appendix B) are made allowing contractor employees to begin work under the contract, PO, lease agreement, or MOA, etc.

(2) any contractor employee is found unsuitable for access to FAA facilities, sensitive unclassified information, and resources; and action is taken to deny such access.

CHAPTER 4. POSITION RISK/SENSITIVITY LEVEL DESIGNATIONS

1. Position Risk/Sensitivity Level Designation. All contractor positions must be designated as to their level of risk in terms of suitability; access to automated information systems (information resources), facilities, resources, and sensitive unclassified information; and the level of sensitivity in terms of national security. This is done on FAA Form 1600-77, Contractor Position Risk/Sensitivity Level Designation Record (Figure 3).

a. Risk Level Designation. Every contractor position is designated at a risk level commensurate with the public trust responsibilities and attributes of the position as it relates to the efficiency of the service. Every position where the incumbent has access to, or the responsibility for, information resources, facilities, 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 information resources or realize significant personal gain. However, there is no requirement to complete FAA Form 1600-77 if a contractor position is determined by the operating office in conjunction with the servicing security element (SSE) to have no access to FAA facilities, resources, or sensitive unclassified information.

b. Sensitivity Level Designation. Every position having access to classified national security information must be designated at a sensitivity level necessary to ensure appropriate screening under E.O. 12968. Sensitivity level designation is based on an assessment of the degree of damage that an individual occupying a particular position could cause to the national security. When it is apparent that the risk level criteria described above would not affect a sensitivity level determination that is based on access to classified information, the designation process need not consist of anything other than appropriately documenting the sensitivity level. Mention of a clearance level requirement can also be included under the final adjustment factors (refer to paragraph 7d of this chapter).

2. Responsibility for Position Designations. The operating office, coordinating with the logistics component and other management officials, is responsible for designating the risk or sensitivity levels of every contractor position within its jurisdiction that is required to have access to FAA facilities, sensitive unclassified information, and resources and classified national security information. The personnel security specialist (PSS) from the SSE is responsible for reviewing and approving contractor position risk and sensitivity level designations. Designations may be by class, group, or categories of positions, when appropriate, or may be by an individual position when circumstances warrant doing so.

3. Risk Levels. There are three position risk levels:

a. High Risk. These public trust positions 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 also includes positions that have *major* program responsibilities affecting information resources for the agency.

b. Moderate Risk. These public trust positions 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 also includes positions that have *significant* program responsibilities affecting information resources.

c. Low Risk. These positions have potential for impact involving duties of *limited* relation to the agency mission with program responsibilities that affect the efficiency of the service. This level also includes positions that have *limited* impact on information resources.

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

a. Special-sensitive. These positions involve the highest degree of trust and require access, or afford ready opportunity to gain access, to any information which is controlled under a Special Access Program as Sensitive Compartmented Information.


b. Critical-sensitive. These positions have the potential for causing *serious to exceptionally grave damage* to the national security and require access, or afford ready opportunity to gain access, up to Top Secret classified information and material as described in E.O. 12958, Classified National Security Information.

c. Noncritical-sensitive. These positions have the potential for causing *serious damage* to the national security and require access, or afford ready opportunity to gain access, to Secret classified information and material as described in E.O. 12958.

5. Documenting Position Risk/Sensitivity Level Designations.

a. As mentioned earlier, position risk and sensitivity level designations for contractor employees are recorded on FAA Form 1600-77 (Figure 3). Generally, the person most knowledgeable about the labor categories from the operating office is responsible for completing FAA Form 1600-77. The logistics component should maintain all original forms completed either electronically or in hardcopy for contractor employee positions within their area of responsibility, and copies should be kept by the operating office and SSE.

Figure 3

| | | | | |
|---|--|---|--|-------------------------------------|
|  U.S. Department of Transportation Federal Aviation Administration | CONTRACTOR POSITION RISK/SENSITIVITY LEVEL DESIGNATION RECORD | | | |
| Contract Company/Subcontractor | | Organization Code or Cost Center Contract/Solicitation Number | | |
| Purpose of Contract | Brief Position Description | | | |
| Position Title | | | | |
| If the position is a national security position (<i>security clearance required</i>) Sections I, II and III are optional. | | | | |
| RISK DESIGNATION SYSTEM | | | | |
| I. Program Placement | | | | |
| Impact on efficiency of service | Major <input type="checkbox"/> | Substantial <input type="checkbox"/> | Moderate <input type="checkbox"/> | Limited <input type="checkbox"/> |
| Scope of Operations for efficiency of service | World Wide <input type="checkbox"/> | Gov't Wide <input type="checkbox"/> | Multi-Agency <input type="checkbox"/> | Agency <input type="checkbox"/> |
| Placement | Major <input type="checkbox"/> | Substantial <input type="checkbox"/> | Moderate <input type="checkbox"/> | Limited <input type="checkbox"/> |
| II. Position Risk Points | | | | |
| a. Degree of public trust | (7-1) ----- | _____ | TOTAL POINTS: ____ | |
| b. Fiduciary responsibilities | (7-1) ----- | _____ | | |
| c. Importance to program | (7-1) ----- | _____ | | |
| d. Program authority level | (7-1) ----- | _____ | | |
| e. Supervision received | (7-1) ----- | _____ | | |
| III. Risk/Sensitivity Level | | | | |
| High Risk – 6 Moderate Risk – 5 Special-Sensitive – 4 | | Critical-Sensitive – 3 Noncritical-Sensitive – 2 Low Risk – 1 | | |
| RISK LEVEL: ____ | | | | |
| IV. Final Adjustment Factor(s), Including AIS Risk Criteria | | | | |
| | | | | |
| Level of Security Clearance Required (<i>To be filled in by the SSE</i>) | | | | |
| <input type="checkbox"/> TOP SECRET <input type="checkbox"/> SECRET <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> NONE | | | | |
| V. Final Risk/Sensitivity Level | | | | |
| Final Risk/Sensitivity Level - ____ | | | | |
| Comments: | | | | |
| VI. Automated Procurement System Entry Code | | | | |
| <input type="checkbox"/> NO ACCESS – Investigation Not Required (3) <input type="checkbox"/> YES - Background Check Required (1) <input type="checkbox"/> ESCORT Required (2) <input type="checkbox"/> CLASSIFIED (4) | | | | |
| Level of Investigation Required (<i>To be filled in by the SSE</i>) | | | | |
| <input type="checkbox"/> FP Check <input type="checkbox"/> NACI <input type="checkbox"/> ANACI <input type="checkbox"/> NACLC <input type="checkbox"/> MBI <input type="checkbox"/> LBI <input type="checkbox"/> BI <input type="checkbox"/> SSBI | | | | |
| Operating Office/CO (<i>providing input</i>) and Routing Symbol | Signature of Operating Office/CO (<i>providing input</i>) | | Date | |
| Approving Security Official (<i>Type or Print name</i>) | Signature of Approving Security Official | | Date | |

b. The following codes for position risk and sensitivity levels are required Government-wide for Federal positions; therefore, FAA must use these codes on all contractor employee documentation.

Figure 4. Designation Codes

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

c. Operating offices and logistics components must ensure that FAA Form 1600-77 is provided for all positions on contracts, purchase orders (POs), lease agreements, Memorandum of Agreements (MOAs) etc., *that have a security requirement.*

d. Operating offices and logistics components do not need to provide FAA Forms 1600-77 for positions requiring escort, however, if there is a need for one position to be used as the escort, complete an FAA Form 1600-77 which reflects that an investigation is needed. This does not alter the contract, etc., in any way from still being considered an escort-required contract.

e. Operating offices and logistics components need only provide one FAA Form 1600-77 for contracts that have similar positions as long as the risk level for these positions is the same. An example of this would be a building construction contract that has multiple positions, such as, brick layers, roofers, dry wall hangers, etc. A list of the different positions must be attached to the FAA Form 1600-77.

f. Operating offices and logistics components do not need to provide FAA Forms 1600-77 for contracts, POs, lease agreements, MOAs, etc., *that do not have a security requirement.*

g. Operating offices and logistics components must ensure that FAA Forms 1600-77 are completed for positions on contracts, POs, lease agreements, MOAs, etc., that have a security requirement but have like positions with different access. For example, a software engineer who is working at the contract company site and has limited access to an FAA facility, resources, or sensitive unclassified information, may require a lower risk level designation because of his or her limited access. However, another software engineer who has frequent access to an FAA facility, sensitive unclassified information, or resources will have a higher level of risk, therefore, the risk level designation and investigation may be different from the first software engineer, so a separate FAA Form 1600-77 is required.

6. Sensitivity Level Designation. All contractor positions within the Office of the Associate Administrator for Security and Hazardous Materials, ASH, requiring access to classified information should be designated, at a minimum as critical-sensitive. (Note: All contractor positions within ASH that do not require access to classified information should be designated, at a minimum, high risk.) For positions outside of ASH, if you are the operating office you must:

a. Designate all positions requiring access to *Confidential* or *Secret* classified information at a minimum as noncritical-sensitive.

b. Designate all positions requiring access to *Top Secret* classified information at a minimum as critical-sensitive.

c. Designate all contractor positions requiring access to *Sensitive Compartmented Information (SCI)* at a minimum as special-sensitive, regardless of other risk factors involved.

d. Designate only the sensitivity level if designation is based on access to classified information. The position risk designation process does not need to be applied. Therefore, you only need to complete the top portion of the FAA Form 1600-77 and Sections IV, V, VI, and the signature block.

7. Risk Level Designation. The risk level designation system tells you, the operating office, how to designate each contract for its impact and scope as related to the efficiency of the service, designate each position for its degree of risk to its program, and make any final adjustments necessary because of unique factors specific to certain positions, or to ensure organizational uniformity of operations. You should follow the guidance below when designating risk/sensitivity levels.

a. Program placement. You should use Chart A to determine how the contract fits into the program placement (major, substantial, moderate, or limited). In most cases, the FAA will be a *moderate* placement (refer to paragraph 8c of this chapter). Use the following procedures for determining program placement:

(1) Determine the contract'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 for the agency will be one of the following:

(a) Accounting, auditing, or disbursement of public funds. (Note: this does not mean the contract company's funds.)

(b) Administrative, regulatory, or policy control over public or private programs or operations.

(c) Protection of the national security.

(d) Enforcement of Federal laws.

(e) Protection of life or property.

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

(3) Determine the contract's impact on the program's scope of operations in terms of the efficiency of the service, choosing from one of the scopes (worldwide, Government-wide, multi-agency, or agency) listed across the top of Chart A. In most cases, the FAA contractor programs will be determined as *agency*.

CHART A

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

b. Position risk points. In determining position risk points, you must consider the duties and responsibilities of the position in the context of the FAA program and the risk the position has for damage or abuse. Use Chart B to assign risk points to each contractor position. In some instances, you may designate like positions differently based on the level of access the position has. The procedure requires you to make a determination on the degree of impact on the program of each of five risk factors and the assignment of points to each risk factor. You must:

(1) Determine the degree 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. (Column under “Supervision Received.”)

(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, however, 1 is the lowest value. For all positions in which there is limited impact, such as, a position with no fiduciary responsibility, the point value should be “1.”

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

c. Tentative risk levels. You should use Chart C to find the tentative risk level by applying the program placement determination (left column) and the total risk points (top of the chart). The sum of the risk points and the program placement combine to determine the tentative risk level.

CHART B

| RISK FACTOR DESCRIPTIONS | | | | | |
|--|--|--|---|---|--|
| | 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 technical aspects of program policy and operations. 7 |
| SUBSTANTIAL: Potential for reducing the efficiency of overall program operations, or the overall operations of major program elements or components independently, or through collective action with others. | 5 | 5 | 5 | 5 | Periodic: Ongoing spot review of policy and major operational considerations of work by superior, with some knowledge of program operations, but with minimal technical program expertise. 5 |
| 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 program expertise. 3 |
| LIMITED: Potential for damage not meeting above criteria. | 1 | 1 | 1 | 1 | Close Technical: Continuing review of all phases of work by supervisor with technical program expertise. 1 |
| POSITION RISK POINTS | | | | | |

CHART C

| II. POSITION RISK POINTS | | | | | | |
|--|---------------|--------------------|--------------------|--------------------|--------------------|----------------|
| PROGRAM PLACEMENT | 5-10 | 11-17 | 18-23 | 24-29 | 30-33 | 34-35 |
| MAJOR | LOW RISK (LR) | MODERATE RISK (MR) | MODERATE RISK (MR) | HIGH RISK (HR) | HIGH RISK (HR) | HIGH RISK (HR) |
| SUBSTANTIAL | LOW RISK (LR) | MODERATE RISK (MR) | MODERATE RISK (MR) | MODERATE RISK (MR) | HIGH RISK (HR) | HIGH RISK (HR) |
| MODERATE | LOW RISK (LR) | LOW RISK (LR) | MODERATE RISK (MR) | MODERATE RISK (MR) | MODERATE RISK (MR) | HIGH RISK (HR) |
| LIMITED | LOW RISK (LR) | LOW RISK (LR) | LOW RISK (LR) | LOW RISK (LR) | MODERATE RISK (MR) | HIGH RISK (HR) |
| POSITION RISK LEVEL AND TYPE OF BACKGROUND INVESTIGATION | | | | | | |

d. Final adjustment. Some positions, by the very nature of the duties and responsibilities of the program or the position, require designation at certain levels of risk. You can make any decision on final adjustment only after careful analysis of the position in terms of uniqueness or uniformity.

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

- (a) Special investigative or criminal justice duties.
- (b) Control of an automated monetary system (key access entry).
- (c) Certain other special duties, such as a special assistant to the Administrator or foreign nationals or immigrant aliens with unique qualities, skills, or character unobtainable elsewhere.
- (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) Access to classified information or requirement for a security clearance.
- (f) Any other factors believed relevant, provided they are documented.

(2) Uniformity. A clearly indicated need for uniformity in position designation because of authority level or program placement level may serve as a basis for making adjustments. Such a need may be for all positions within a particular program to be at

a risk level paralleling the program's placement level. This would occur in 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.

8. Special Risk Level Designations.

a. Automated information systems (information resources). Risk level designations for positions involving access to information resources are an integral part of the risk and sensitivity level designation processes. You, the operating office, must apply the following criteria when determining the risk level designations for these positions.

Figure 5. Position Categories

| POSITION CATEGORY | MINIMUM RISK LEVEL |
|--|--------------------|
| (1) Responsibility for development and administration of an information resources security program, including direction and control of risk analyses and/or threat assessments. | 6 |
| (2) Significant involvement in life-critical or mission-critical systems | 6 |
| (3) Responsibility for preparation or approval of data for input into an information resource that does not necessarily involve personal access to the system, but with relatively high risk for causing grave damage or realizing significant personal gain. | 5 |
| (4) Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from information resources of dollar amounts of \$10 million per year or greater or lesser amounts if the activities of the individual are not subject to technical review by higher authority to ensure the integrity of the system. | 5 |
| (5) Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software. | 5 |
| (6) Other positions that involve relatively high risk for causing grave damage or realizing significant personal gain. | 5 |
| (7) Responsibility for systems design, operation, testing maintenance, and/or monitoring that is carried out under technical review by a higher authority at the high-risk level to ensure the system's integrity | 5 |
| (8) Access to and/or processing of proprietary data, information protected by the Privacy Act, and Government-developed privileged information in or on a major FAA information resource (not personal computers or local area networks) involving the award of contracts. | 5 |

| | |
|--|---|
| (9) Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year. | 5 |
| (10) 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. | 5 |
| (11) All information resources positions not falling into one of the above categories/risk levels. | 1 |

b. Positions with special responsibilities or that are unique. You should be aware that there are certain positions within the FAA that are unique, have special responsibilities, or for which there is a need for uniformity. Some of these positions are: air traffic controller, weapons carrying, other safety-related position, etc. FAA has set the minimum investigative requirement for these positions at a National Agency Check with Inquiries, however, the SSE may opt to conduct a higher-level investigation.

9. Preparation of FAA Form 1600-77. As the operating office, you must use the following procedures in consultation with the logistics component and the PSS when completing FAA Form 1600-77. Other procedures may apply when completing FAA Form 1600-77 electronically.

a. Contract Company/Subcontractor Identification.

(1) Contract Company/Subcontractor. Enter the name of the contractor or subcontractor in this block.

(2) Organization Code or Cost Center and Contract/Solicitation Number. Enter the organization code or routing symbol of the office requesting the contract services and identify the office or person who can be contacted for information, if needed. Enter the contract number if available. For contracts not yet awarded, the solicitation number will suffice. Once the contract is awarded, you should change the block to reflect the contract number, or notify the PSS of the final contract number.

(3) Purpose of Contract. Provide a brief explanation of services requested, i.e., LAN support, air traffic control services, upgrade of system hardware.

(4) Position Title. Enter the title of the position whose risk designation is being determined. If the position title is not indicative of the actual work being performed, include a brief description. For example, project administrator could be the manager of an entire program or it could be a secretary or administrative officer. Be as specific as possible when entering information into this block.

(5) Brief Position Description. Provide a brief explanation of the labor category, i.e., air traffic controller who is responsible for the safety of the traveling public through the control of air traffic.

b. Section I, Risk Designation System.

- (1) Enter the impact designation determined using Chart A and the procedures outlined in paragraph 7a of this chapter.
- (2) Enter the scope of operations designation determined using Chart A and the procedures outlined in paragraph 7a of this chapter.
- (3) Enter the program placement designation determined using Chart A and the procedures outlined in paragraph 7a of this chapter.

c. Section II, Position Risk Points.

- (1) Enter the point designations determined using Chart B and the procedures outlined in paragraph 7b of this chapter.
- (2) Enter the total points.

d. Section III, Risk/Sensitivity Level. Enter the risk or sensitivity level designation determined using Chart C and the procedures outlined in paragraph 7c of this chapter.

e. Section IV, Final Adjustment Factor(s) (including AIS Risk Criteria). Enter any adjustment factors that apply determined under paragraph 7d of this chapter.

- (1) When the assessment indicates that there are unique factors associated with a contractor employee position, ensure sufficient justification is provided in this block.
- (2) Level of Security Clearance Required (To be filled in by the SSE). The PSS will check the appropriate block.

f. Section V, Final Risk/Sensitivity Level. Enter the final risk or sensitivity level and any comments. This should reflect the points in Section III along with any final adjustment factor in Section IV.

g. Section VI, Automated Procurement System Entry Code. The procurement office will check the appropriate box to indicate if there is a security requirement associated with the position, and the SSE will complete the Level of Investigation Required.

h. Level of Investigation Required (To be filled in by the SSE). The PSS will check the appropriate block based on the position risk/sensitivity level and the investigative requirements that apply in accordance with chapter 5.

i. Signature blocks. When the form is completed, the operating office or CO must sign and date it then send it to the SSE for review and approval. Once approved, the PSS,

will enter the data in sections V (Level of Security Clearance Required) and VI (Level of Investigation Required), sign (for the SSE) and date the form, and send the original to the logistics component and a copy to the operating office.

(1) If the PSS does not agree with the position risk/sensitivity level designations, he or she will contact the operating office to discuss the concerns. Every effort will be made to resolve a disagreement at the lowest, local level possible.


(2) The PSS will *not* sign the form until full agreement is met on the risk/sensitivity level designations.

10. Common Contractor Position and the Step-By-Step Procedures for Completing FAA Form 1600-77. The following is an example of how to complete Form 1600-77.


EXAMPLE: The Air Traffic Organization has just put together a contract to place contractor employees in Air Route Traffic Control Centers (ARTCCs) throughout the United States who will be working side-by-side with FAA employees on a specific computer system that supports the National Airspace Systems (NAS). The office, in consultation with the SSE, has already established that no security clearance and no access to classified information will be necessary for these contractor positions. The contract is ready to be awarded and a contract number has been assigned. For the purpose of this example, the program placement has been predetermined to be "Moderate."

a. Basic Information.

(1) Item 1. Contract Company/Subcontractor.

| | | |
|--|--|--|
|  U.S. Department of Transportation Federal Aviation Administration | CONTRACTOR POSITION RISK/SENSITIVITY LEVEL DESIGNATION RECORD | |
| Contract Company/Subcontractor XYZ Systems Corporation | | |

(2) Item 2. Organization Code or Cost Center and Contract/Solicitation Number

| | | |
|--|--|--|
|  U.S. Department of Transportation Federal Aviation Administration | CONTRACTOR POSITION RISK/SENSITIVITY LEVEL DESIGNATION RECORD | |
| Contractor Company/Subcontractor XYZ Systems Corporation | Organization Code or Cost Center Contract/Solicitation Number ATO DTFAWA-03-C-12345 | |

(3) Item 3. Purpose of Contract.

| |
|--|
| Purpose of Contract <i>Upgrade computer systems that support the NAS at various ARTCCs</i> |
|--|

(4) Item 4. Brief Position Description

| | |
|---|---|
| Purpose of Contract <i>Upgrade of comp sys that support the NAS</i> | Brief Position Description <i>Works on computer systems in support of the NAS</i> |
|---|---|

(5) Item 5. Position Title. (The sample title provided is only one example; other titles might be *Computer Programmer* or *Computer Analyst*.)

| | |
|--|--|
| Position Title <i>Systems Engineer</i> | |
|--|--|

b. Program Placement.

(1) Item 1. Impact on Efficiency of Service. This is to determine the potential risk to the national security that the Air Traffic Organization might cause. In this example, the impact on the efficiency of the service is *Moderate*.

| | | | | |
|---|-----------------------------------|---|---------------|-------------------------------------|
| If the position is a national security position (<i>security clearance required</i>) Sections I, II and III are optional. | | | | |
| RISK DESIGNATION SYSTEM | | | | |
| I. Program Placement | | | | |
| Impact on efficiency of service | Major <input type="checkbox"/> | Substantial <input type="checkbox"/> | Moderate X | Limited <input type="checkbox"/> |

(2) Item 2. Scope of Operations for efficiency of service. This is to determine the efficiency of the service. In this example, it is *Multi-Agency*.

| | | | | |
|---|--|--|-------------------|------------------------------------|
| Scope of Operations for efficiency of service | World Wide <input type="checkbox"/> | Gov't Wide <input type="checkbox"/> | Multi-Agency X | Agency <input type="checkbox"/> |
|---|--|--|-------------------|------------------------------------|

(3) Item 3. Placement. This establishes the program placement for your risk level. Chart A, section IV, is used to determine this item. In this example, it is *Moderate*.

| | | | | |
|-----------|-----------------------------------|---|---------------|-------------------------------------|
| Placement | Major <input type="checkbox"/> | Substantial <input type="checkbox"/> | Moderate X | Limited <input type="checkbox"/> |
|-----------|-----------------------------------|---|---------------|-------------------------------------|

c. Position Risk Points. This determines the degree of impact the *position* has on the program, including the potential risk or damage possible to the program. To establish the impact of a position, each risk factor description is rated on a point scale from 1-7, with 7 representing the highest potential for risk.

(1) Item a. Degree of Public Trust. Consensus of confident expectation for honesty, integrity, reliability, responsibility, or justice placed in a position. In this example, the point value for this risk factor is 7, *Major*.

| II. Position Risk Points | | |
|-------------------------------|-------------|---|
| a. Degree of public trust | (7-1) | 7 |
| b. Fiduciary responsibilities | (7-1) ----- | |
| c. Importance to program | (7-1) ----- | |
| d. Program authority level | (7-1) ----- | |
| e. Supervision received | (7-1) ----- | |
| TOTAL POINTS: | | |

(2) Item b. Fiduciary Responsibilities. This refers to whether the position has the authority or ability to obligate, control, or expend public money or items of monetary value (such as bonds). In this example, the point value for this risk factor is 1, *Limited*.

| II. Position Risk Points | | |
|--------------------------------------|--------------|----------|
| a. Degree of public trust | (7-1) | 7 |
| b. Fiduciary responsibilities | (7-1) | 1 |
| c. Importance to program | (7-1) | |
| d. Program authority level | (7-1) | |
| e. Supervision received | (7-1) | |
| TOTAL POINTS: | | |

(3) Item c. Importance to the program. This refers to the impact the *individual position* has, due to status or influence, on the program as a whole, either individually or collectively. In this example, the point value for this risk factor is 7, *Major*.

| II. Position Risk Points | | |
|---------------------------------|--------------|----------|
| a. Degree of public trust | (7-1) | 7 |
| b. Fiduciary responsibilities | (7-1) | 1 |
| c. Importance to program | (7-1) | 7 |
| d. Program authority level | (7-1) | |
| e. Supervision received | (7-1) | |
| TOTAL POINTS: | | |

(4) Item d. Program authority level. This refers to the ability to manipulate authority or control the outcome or results of all or key portions of a program or policy. In this example, the point value for this risk factor is 5, *Substantial*.

| II. Position Risk Points | | |
|-----------------------------------|--------------|----------|
| a. Degree of public trust | (7-1) | 7 |
| b. Fiduciary responsibilities | (7-1) | 1 |
| c. Importance to program | (7-1) | 7 |
| d. Program authority level | (7-1) | 5 |
| e. Supervision received | (7-1) | |
| TOTAL POINTS: | | |

(5) Item e. Supervision received. This item refers to the frequency with which the work is reviewed by a supervisor and the nature or degree of the review. In this example, the point value for this risk factor is 7 *Limited*.

| II. Position Risk Points | | |
|--------------------------------|--------------|----------|
| a. Degree of public trust | (7-1) | 7 |
| b. Fiduciary responsibilities | (7-1) | 1 |
| c. Importance to program | (7-1) | 7 |
| d. Program authority level | (7-1) | 5 |
| e. Supervision received | (7-1) | 7 |
| TOTAL POINTS: | | |

(6) Item f. Total points. Add up the points assigned to items a through e and enter the total. In this example, the total points is 27.

| II. Position Risk Points | | |
|-------------------------------|-------|---|
| a. Degree of public trust | (7-1) | 7 |
| b. Fiduciary responsibilities | (7-1) | 1 |
| c. Importance to program | (7-1) | 7 |
| d. Program authority level | (7-1) | 5 |
| e. Supervision received | (7-1) | 7 |
| TOTAL POINTS: 27 | | |

d. Risk/Sensitivity Level. To determine the risk level of a position, refer to Chart C, Position Risk Points, and to determine the sensitivity level of a position, refer to paragraph 6. For this example, we have already determined that our *Program Placement* is *Moderate* and our total *Position Risk Points* is 27. Refer to Chart C, find *Moderate* under the *Program Placement* column, then find where 27 points falls. In this example, 27 falls under the 24-29 column. By scrolling down the point column and across to the *Program Placement*, the Position Risk Level is *Moderate Risk*; therefore, enter 5 as the *Risk Level*.

| | |
|---|---|
| III. Risk/Sensitivity Level | |
| High Risk – 6 Moderate Risk – 5 Special-Sensitive – 4 | Critical-Sensitive – 3 Noncritical-Sensitive – 2 Low Risk – 1 |
| RISK LEVEL: 5 | |

e. Final Adjustment Factor(s), *including AIS Risk Criteria*. This section is for entering any unique factors that apply to the position. In this example, the position requires Level II AIS access.

| |
|--|
| IV. Final Adjustment Factor(s), Including AIS Risk Criteria |
| <i>AIS Level II access required.</i> |

f. Level of Security Clearance Required. This section is for entering the level of access to classified information required by the position. In this example, the position does not require access to classified, therefore, no security clearance is required.

| |
|--|
| Level of Security Clearance Required (To be filled in by the SSE) |
| <input type="checkbox"/> TOP SECRET <input type="checkbox"/> SECRET <input type="checkbox"/> CONFIDENTIAL <input checked="" type="checkbox"/> NONE |

g. Final Risk/Sensitivity Level. This section is for entering the final risk or sensitivity level for the position. For this example, the final risk level is 5, *Moderate Risk*. Once this information is entered, the form is ready to be signed by the operating office or CO and submitted to the SSE for review and approval.

| |
|---|
| V. Final Risk/Sensitivity Level |
| Final Risk/Sensitivity Level - 5, <i>Moderate Risk</i> Comments: |

h. Automated Procurement System Entry Code. This section is for entering the security requirement of the position by the requisitioner. This information is used to enter the Background Investigation Code (BIR). For this example, the BIR is YES – Background Check Required (1).

| |
|--|
| VI. Automated Procurement System Entry Code |
| <input type="checkbox"/> NO ACCESS – Investigation Not Required (3) <input checked="" type="checkbox"/> YES – Background Check Required (1) <input type="checkbox"/> ESCORT – Required (2) <input type="checkbox"/> CLASSIFIED (4) |

i. SSE actions.

(1) Once the PSS receives the completed form from the operating office or CO, he or she must review the data, ensure it is accurate and appropriate for the position described, and determine the level of investigation if any required for the position. The PSS must enter the information, sign the form, send the original to the logistics component and a copy to the operating office or the preparer of the form. (Refer to the sample completed form at the end of this chapter.)


(2) If the PSS determines that the information provided on the completed form is not accurate or appropriate for the position described, the form will *not* be approved.

(a) The PSS must advise the operating office or preparer of this determination and the reason for the determination.

(b) In consultation with the PSS, the operating office can either resubmit the form to show an appropriate risk/sensitivity level; provide additional justification for the risk/sensitivity level that was designated and forward the new form to the PSS for review and approval; or request that the PSS make the appropriate changes and send the signed form back to them.

| | | |
|--|---|------|
| Level of Investigation Required (To be filled in by the SSE) | | |
| <input type="checkbox"/> FP Check <input checked="" type="checkbox"/> NACI <input type="checkbox"/> ANACI <input type="checkbox"/> NACLC <input type="checkbox"/> MBI <input type="checkbox"/> LBI <input type="checkbox"/> BI <input type="checkbox"/> SSBI | | |
| Operating Office/CO (<i>providing input</i>) and Rtg Symbol | Signature of Operating Office/CO (<i>providing input</i>) | Date |
| Approving Security Official (<i>Type or Print name</i>) | Signature of Approving Security Official | Date |

Figure 6: COMPLETED SAMPLE

| | | | | | |
|--|--|---|-------------------------|-------------------------------------|--|
|  U.S. Department of Transportation Federal Aviation Administration | | CONTRACTOR POSITION RISK/SENSITIVITY LEVEL DESIGNATION RECORD | | | |
| Contract Company/Subcontractor XYZ Systems Corporation | | Organization Code or Cost Center Contract/Solicitation Number ATO/DTFAWA-03-C-12345 | | | |
| Purpose of Contract Upgrade of computer systems at various ARTCCs | | Brief Position Description Works on computer systems in support of the NAS | | | |
| Position Title Systems Engineer | | | | | |
| If the position is a national security position (security clearance required) Sections I, II and III are optional. | | | | | |
| RISK DESIGNATION SYSTEM | | | | | |
| I. Program Placement | | | | | |
| Impact on efficiency of service | Major <input type="checkbox"/> | Substantial <input type="checkbox"/> | Moderate X | Limited <input type="checkbox"/> | |
| Scope of Operations for efficiency of service | World Wide <input type="checkbox"/> | Gov't Wide <input type="checkbox"/> | Multi-Agency X | Agency <input type="checkbox"/> | |
| Placement | Major <input type="checkbox"/> | Substantial <input type="checkbox"/> | Moderate X | Limited <input type="checkbox"/> | |
| II. Position Risk Points | | | | | |
| a. Degree of public trust | (7-1) ----- | 7 | | | |
| b. Fiduciary responsibilities | (7-1) ----- | 1 | | | |
| c. Importance to program | (7-1) ----- | 7 | | | |
| d. Program authority level | (7-1) ----- | 5 | | | |
| e. Supervision received | (7-1) ----- | 7 | TOTAL POINTS: <u>27</u> | | |
| III. Risk/Sensitivity Level | | | | | |
| High Risk – 6 Moderate Risk – 5 Special-Sensitive – 4 | | Critical-Sensitive – 3 Noncritical-Sensitive – 2 Low Risk – 1 | | RISK LEVEL: <u>5</u> | |
| IV. Final Adjustment Factor(s), Including AIS Risk Criteria | | | | | |
| AIS Level II access required. | | | | | |
| Level of Security Clearance Required (To be filled in by the SSE) <input type="checkbox"/> TOP SECRET <input type="checkbox"/> SECRET <input type="checkbox"/> CONFIDENTIAL X NONE | | | | | |
| V. Final Risk/Sensitivity Level | | | | | |
| Final Risk/Sensitivity Level - <u>5, Moderate Risk</u> Comments: | | | | | |
| VI. Automated Procurement System Entry Code | | | | | |
| <input type="checkbox"/> NO ACCESS – Investigation Not Required (3) X YES – Background Check Required (1) <input type="checkbox"/> ESCORT – Required (2) <input type="checkbox"/> CLASSIFIED – (4) | | | | | |
| Level of Investigation Required (To be filled in by the SSE) <input type="checkbox"/> FP Check X NACI <input type="checkbox"/> ANACI <input type="checkbox"/> NACLC <input type="checkbox"/> MBI <input type="checkbox"/> LBI <input type="checkbox"/> BI <input type="checkbox"/> SSBI | | | | | |
| Operating Office/CO (providing input) and Rtg Symbol | Signature of Operating Office/CO (providing input) | | | Date | |
| Approving Security Official (Type or Print name) | Signature of Approving Security Official | | | Date | |

CHAPTER 5. INVESTIGATIVE REQUIREMENTS AND INITIATION PROCEDURES

1. Introduction. This chapter prescribes specific investigative requirements that apply to contractor employee positions and the procedures for initiating required investigations.

2. Types of Background Investigations. The Office of Personnel Management (OPM) conducts background investigations for all FAA contractor employees who do not require access to classified information. They also conduct background investigations for the Defense Security Service (DSS) who is responsible for ensuring that background investigations for all contractor employees requiring access to classified information are conducted. The following identifies the various types of investigations conducted by OPM that will be referred to throughout this chapter. For a detailed explanation of each type of investigation listed below, refer to Appendix A, Glossary and Acronyms.

a. Standard initial investigations:

- (1) Fingerprint Check.
- (2) National Agency Check (NAC).
- (3) National Agency Check with Inquiries (NACI).
- (4) Access National Agency Check with Inquiries (ANACI).
- (5) Minimum Background Investigation (MBI).
- (6) Limited Background Investigation (LBI).
- (7) Background Investigation (BI).
- (8) Single Scope Background Investigation (SSBI).
- (9) Reimbursable Suitability/Security Investigation (RSI).

b. Reinvestigations:

- (1) Periodic Reinvestigation (PRI).
- (2) Periodic Reinvestigation for Single Scope Background Investigation (SSBI-PR).
- (3) National Agency Check, Law Enforcement, and Credit (NACLC).

c. Special Agency Agreement (SAC). A limited investigation (or a series of checks) conducted on a person, done only through special agreement between OPM and an agency.

d. Advance NAC. An OPM product that consists of searches of the Security and Suitability Investigations Index, Defense Clearance and Investigations Index, FBI's Identification Division, and FBI's Records Management Division. This product is provided in advance of the completion of an investigation. (Refer to paragraph 15a(3) of this chapter for additional information.)

3. Investigative Requirements. The personnel security specialist (PSS) located in the servicing security element (SSE) will determine the type of investigation required by the risk or sensitivity level of the position, and in some cases, the security clearance required for a person holding the position. In most circumstances, they will apply the same investigative requirements to contractor employees as FAA employees, if they have comparable exposure to FAA facilities, sensitive unclassified information, and resources. A contractor employee who requires an investigation can begin work only when the PSS has received all necessary investigative forms, addressed any issues, granted interim suitability, and provided written notice to the logistics component, operating office, and/or contract company authorizing the contractor employee to begin work. (Refer to Appendix B for a sample written authorization.) FAA does not have a requirement to conduct investigations on contractor employees who have no access to FAA facilities, sensitive unclassified information, or resources. (NOTE: The process for allowing contractor employees to work on FAA contracts will be changing with the implementation of Homeland Security Presidential Directive 12 (HSPD-12), Policy for Common Identification Standard for Federal Employees and Contractors.)

a. High-risk positions. PSSs must ensure that all contractor employees in these positions receive an initial BI and a PRI every 5 years. They must favorably adjudicate all investigations and satisfactorily address all issues before the employee is allowed to perform the duties of the position.

b. Moderate-risk positions. PSSs must ensure that all contractor employees in these positions receive at least a NACI investigation. There is no reinvestigation requirement for moderate-risk positions.

c. Low-risk positions. PSSs must ensure that all contractor employees in these positions receive, at a minimum, a fingerprint check. There is no reinvestigation requirement for low-risk positions.

d. Critical-area positions. PSSs must ensure that all contractor employees in positions having comparable exposure to FAA facilities, sensitive unclassified information, or resources as do FAA employees receive the minimum investigative requirement of a NACI, unless otherwise specified. As a reminder, these positions can include, but are not limited to, air traffic control, weapons carrying, information resources, communications,

information resources penetration testing, and those located in or having access to sensitive areas. If there is *any* doubt as to whether a position fits into this category, conduct a NACI.

e. Fiduciary positions. PSSs must ensure that all contractor employees who perform fiduciary duties or support FAA positions having fiduciary responsibilities receive a NACI and a credit check as the minimum investigative requirement. The positions affected by this requirement include, but are not limited to, contract specialists, cashiers, and other positions:

- (1) whose major responsibility involves the authority or ability to obligate, control, or expend FAA money or items of monetary value and who can directly impact the contract; or
- (2) that directly support FAA employees in positions whose major responsibility involves the authority or ability to obligate, control, or expend public money or items of monetary value.

f. Information resources positions in non-critical areas. The minimum investigative requirement for contractor employees who are performing duties in non-critical areas, such as, supply contractors, contractors who provide computer hardware, software, or services is a fingerprint check. However, the investigative requirements for these positions may vary. The PSS and the operating office must consider:

- (1) The risk level of the position.
- (2) Length of the contract.
- (3) Nature and extent of access to FAA sensitive unclassified information and resources and the level of access to the information resource.

g. Escort positions. In order to perform escort duties, a contractor employee is required to have a completed, favorably adjudicated NACI. However, in an effort to meet this requirement and expedite the process, the PSS may conduct an OPM Advance NAC (paragraph 2d of this chapter). The PSS will notify the logistics component when the Advance NAC is completed and favorably adjudicated, and the contractor employee will be allowed to perform escort duties while the NACI is still in process. If the PSS determines that the information contained in the Advance NAC is not favorable, the contractor employee will not be used as an escort until the completion and favorable adjudication of the NACI. Please note that an Advance NAC is not a stand-alone investigation to be used for other than the purpose described in this paragraph. Advance NAC information must be entered into the "Remarks" section of the Investigations Tracking System (ITS) to certify that the individual meets the escort requirements. (Refer to chapter 7, paragraph 1a.) It is the responsibility of the office who is requesting the escort, to contact their regional PSS to ensure that the contractor employee assigned to perform these duties has the appropriate investigation.

4. Exemption and Escort Requirements. As the PSS, you must apply the following criteria to all binding agreements between the FAA and another party and to contractor employees in positions that require temporary, intermittent, or seasonal access to FAA-owned or leased facilities. (Temporary, intermittent, or seasonal access is defined as either routine but non-recurring access, or non-routine access.) These positions may include janitorial service work, construction, maintenance and repair persons, and delivery persons such as Federal Express (FEDEX) and United Parcel Service (UPS). The operating office or logistics component will generally make the determination of exemption applicability.

a. Applicability of exemption criteria for investigative requirements. Contractor employees who require temporary, intermittent, or seasonal access to FAA-owned or leased facilities can be exempt from any investigative requirement but must be escorted. While it is understood that it may not be feasible for FAA to conduct security screenings for all temporary situations, operating offices must not use this exemption and subsequent escorting as a means to satisfy local compliance issues. If a facility is not able to comply with escort practices because of lack of resources, management can opt to request that the SSE conduct a security screening.

(1) Routine access refers to a contractor employee who needs access to an FAA-controlled area at routine intervals, e.g., two days per week, every Monday, etc., for longer than a 6-month period but not in excess of a total of 180 days.

(2) Routine, but non-recurring (short-term) access refers to a contractor employee who needs access to an FAA-controlled area at routine intervals, e.g., every day, two days per week, every Monday, etc., but over a limited period of time. Non-recurring means that the contract's period of performance is for a narrowly defined scope, generally not to exceed 6 months with the capability of extending on a month-to-month basis not to exceed 1 year, and the contract is not anticipated to be renewed. For example, a contractor employee who needs access to an FAA-owned or leased facility every day for the next 3 weeks (period of performance) to complete a specific work assignment would fall under this definition.

(3) Non-routine access refers to a contractor employee who needs access that is infrequent and undefined, regardless of the contract's period of performance. For example, a 2-year service contract that requires a contractor employee to access an FAA-owned or leased facility to work on equipment when it malfunctions; or a 5-year service contract for window cleaning that requires the contractor to have access for a short period of time would fall under this definition.

b. Examples of situations that do not have an investigative *or* escort requirement.

(1) In the case of a utility or maintenance person who requires access to unstaffed FAA-owned or leased facilities that contain NAS or communications equipment,

if the meter is outside of the building and the utility company employee does not have any access to the building or equipment, no security screening is required. If the person *does* have access to the building, a security screening or escort is required. This, however, may not be feasible since a different individual may respond each time to equipment failures or maintenance. It may, therefore, be more feasible for the PSS to conduct a security screening on the individual who maintains the facility keys (possibly the maintenance person's supervisor or shift manager) and hold them responsible for their employees. The key-keeper could potentially be an FAA employee.

(2) In the case of deliveries made by FEDEX, UPS, or other such companies whose employees are licensed and bonded and who carry company identification, no security screening or escort is necessary under this order. However, the facility manager may have existing procedures in place for accepting deliveries that the individual must comply with.

(3) In the case of construction workers who are doing work on new construction, no security screening or escort is necessary unless the construction is co-located with an FAA facility, or within an already existing FAA structure.

c. Escort requirements. When it is determined that a contractor employee is exempt from the investigative requirements, that contractor employee must be escorted when entering and within FAA-owned or leased facilities as defined in FAA Order 1600.69, FAA Facility Security Management Program. Escort is defined as being in the same vicinity and maintaining visual contact of the contractor employee while within the FAA-owned or leased facility. It does not mean that an individual must follow and maintain physical control of the contractor employee while within the facility.

(1) All FAA and contractor employees who perform escort duties must have a completed, favorably adjudicated NACI unless the requirements of paragraph 3g of this chapter are met.

(2) There is no set number of people that can be escorted at one time, however, the number should be manageable for the individual providing the escort.

(3) Under no circumstances will a contractor employee have unescorted access unless he or she has met the requirements for a security screening and the PSS has granted approval for him or her to begin working.

d. Examples of situations requiring escort.

(1) In the case of delivery personnel and repair technicians, such as, water, vending machine, copier repair technicians, etc., if the access to facilities, sensitive unclassified information, or resources is minimal, they are exempt from the

investigative requirement under this order, however, they must comply with existing facility escort procedures, and FAA Order 1600.69.

(2) In the case of individuals who install furniture for a 2-month period of time, they are exempt from the investigative requirement under this order, but must comply with existing facility escort procedures, and FAA Order 1600.69.

(3) In the case of workers who need access to a facility during non-working hours, such as carpet cleaners or carpet installers, they may be exempt from the investigative requirement under this order, but must comply with facility escort procedures.

5. Contract Janitorial, Construction, Maintenance, Property Management, and Repair Workers in Leased Facilities.

a. When FAA occupies a GSA-leased facility and GSA has contracted for janitorial, construction, maintenance, property management, or repair work, GSA is responsible for conducting background investigations on these workers, unless they are exempt pursuant to paragraph 4a of this chapter. This information should be contained in the contract clauses. GSA is responsible for making the suitability determinations and providing us with a listing of the names of the cleared workers. The PSS must enter this information into ITS or file the list in the contract file.

b. When FAA occupies a GSA-leased facility and is delegated authority to contract for janitorial, construction, maintenance, property management, or repair work, FAA is responsible for conducting the background investigations on these workers, unless they are exempt in accordance with paragraph 4 of this chapter. FAA is also responsible for making the suitability determinations (refer to chapter 6 or this order). The PSS must enter all suitability information into ITS in the contractor module.

c. When GSA leases a facility from a lessor for FAA to occupy that includes janitorial, construction, maintenance, property management, or repair services, GSA is responsible for conducting the background investigations on these workers, unless they are exempt pursuant to paragraph 4 of this chapter. GSA will make the suitability determinations and provide us written notification listing the names of the cleared workers. This should be specified in the clauses for all lease contracts. This information should be contained in the contract clause.

d. When FAA occupies leased facilities but directly contracts for janitorial, construction, maintenance, property management, or repair work, FAA is responsible for conducting the background investigations and making the suitability determinations on such workers, unless they are exempt pursuant to paragraph 4 of this chapter. The PSS must enter all suitability information into ITS in the contractor module.

e. If feasible, when FAA leases a facility from a lessor that includes janitorial, construction, maintenance, property management, or repair services, contracted for or by the lessor, FAA is responsible for conducting the background investigations on these workers and making the suitability determination, unless they are exempt pursuant to paragraph 4 of this chapter, or it is a non-negotiable item in the lease agreement.

6. Special Circumstance Investigative Requirements. We, the FAA, often occupy facilities that are occupied by one or more other tenants. Some of these tenants may have separate, ground-floor entrances and some may access their space by passing through our space or public space.

a. We currently have no requirement or provision for the processing of other Government agency personnel, private industry concerns, or tenants such as credit unions or cafeterias located in facilities also occupied by us but that are not on our payroll and do not occupy our space.

b. When we occupy facilities that are occupied by one or more other tenants such as a credit union or cafeteria where these tenants have internal access to or must pass through FAA-occupied space to access their occupied space, we will not conduct a security screening on these persons unless the responsible real estate contracting officer (RECO) has negotiated specific provisions for conducting such screenings with the lessor and the provisions are included in the contract or other agreement between the lessor and the tenant(s). The RECO and operating office must then ensure that no persons enter FAA space until authorized to do so by the PSS.

c. When determining whether to negotiate with the lessor to include provisions for conducting security screenings on these types of employees in the contract or other agreement, the operating office, RECO, and PSS must consider:

(1) Would conducting security screenings on the other tenant(s) be in the best interest of the FAA?

(2) Is FAA the controlling tenant? If not, it is not feasible to expect to conduct security screenings on every tenant in a multi-tenant facility nor is it feasible to conduct security screenings on credit union or cafeteria workers and not on other tenants. Do not seek to conduct security screenings on private businesses including, but not limited to, accounting firms, law firms, medical practices, and retail establishments.

(3) Is the sole other tenant a credit union or cafeteria? If so, is FAA its primary customer?

(4) Is there any other way to prevent or minimize access to FAA-occupied space by the other tenant(s)? For example, can the lessor establish a separate entrance for the other tenant(s)?

d. If there is any doubt or question as to whether or not to conduct a security screening on an individual, the PSS should consult with their General Counsel.

7. Investigative Requirements for Immigrant and Nonimmigrant Aliens as Contractors. Before FAA allows access to its facilities, sensitive unclassified information, and resources to an immigrant or nonimmigrant alien under a contract or other agreement, the operating office must consult with the PSS located in their SSE, the Office of the Chief Counsel, or their regional or center Counsel. The nature of the work and extent of access to FAA facilities, information, and resources will dictate whether such individuals can be utilized under the contract or other agreement and the investigative requirements.

a. Use of nonimmigrant aliens under unclassified FAA contracts or other agreements.

(1) A nonimmigrant alien is defined as any person not a citizen or national of the United States who has been authorized to work in the United States by the Department of Homeland Security (DHS), but *who has not been lawfully admitted for permanent residence*.

(2) Nonimmigrant aliens in the United States can work as contractor employees under *unclassified* FAA contracts in low or moderate risk positions with access to FAA facilities, information, and resources under other agreements to which the FAA is a party as long as the following conditions are met.

(a) A valid risk level designation can be made for the position.

(b) The individual has resided within the United States for a minimum of 3 of the last 5 years.

(c) An appropriate security screening can be adequately conducted.

(d) If the nonimmigrant alien has not resided in the United States for a minimum of 3 of the last 5 years, a waiver of this requirement can be requested, and submitted for approval to the Director, Office of Internal Security and Investigations, AIN-1, or his or her designee before the individual can begin work. (Refer to paragraph 9 of this chapter.)

(e) Appropriate immigration checks through DHS or other agency checks are conducted.

(f) Approval of the waiver and interim suitability are granted, and all other checks are completed and favorable.

(3) The minimum investigative requirement for nonimmigrant aliens who have met the 3-year residency requirement and who work or provide services or supplies

under an FAA contract will be dictated by the position risk level. For example, a nonimmigrant alien who applies for a janitorial position that is low risk would require, at a minimum, a fingerprint check. For other low risk or moderate risk positions, a NACI would be the minimum requirement.

(4) In any situation where the operating office or the SSE determines that it is in FAA's best interest to restrict access or work under a contract to United States citizens only, the appropriate contract or other agreement must contain a clause specifying that restriction. In determining whether or not to apply this restriction in a given situation, the logistics component and operating office, in consultation with the SSE, must consider the nature and extent of access, particularly in regard to sensitive, proprietary, and classified information. If a decision cannot be reached, they must contact their region or center Office of Chief Counsel.

b. Use of immigrant aliens under unclassified contracts or other agreements.

(1) An immigrant alien is defined as any person not a citizen or national of the United States *who has been lawfully admitted for permanent residence to the United States* by DHS.

(2) Immigrant aliens in the United States can work as contractor employees under *unclassified* FAA contracts in low, moderate, or high risk positions with access to FAA facilities, information, and resources under other agreements to which the FAA is a party as long as the following conditions are met.

- (a) A valid risk level designation can be made for the position.
- (b) The individual has resided within the United States for a minimum of 3 of the last 5 years.
- (c) An appropriate security screening can be adequately conducted.
- (d) If the immigrant alien has not resided in the United States for a minimum of 3 of the last 5 years, a waiver of this requirement must be requested and submitted for approval to AIN-1 or his or her designee before the individual can begin work. (Refer to paragraph 9 of this chapter.)
- (e) An appropriate immigration check through DHS or other agency checks are conducted.
- (f) Approval of the waiver and interim suitability are granted, and all other checks are completed and favorable.

(3) The minimum investigative requirement for immigrant aliens who work on, or provide services or supplies under, an FAA contract will be dictated by the position risk level.

(4) In any situation where the operating office or the SSE determines that it is in FAA's best interest to restrict access or work under a contract to United States citizens only, the appropriate contract or other agreement must contain a clause specifying that restriction. In determining whether or not to apply this restriction in a given situation, the logistics component and operating office, in consultation with the SSE, must consider the nature and extent of access, particularly in regard to sensitive, proprietary, and classified information. If a decision cannot be reached, they must contact their region or center Office of Chief Counsel.

c. Use of immigrant and nonimmigrant aliens under classified FAA contracts or other agreements. Immigrant and nonimmigrant aliens cannot have access to classified information or work as contractor employees or consultants under classified FAA contracts or other agreements unless there are compelling reasons in furtherance of our mission.

(1) Immigrant aliens at FAA's discretion can be granted limited access to classified information only for a specific program, project, contract, license, certificate, or grant for which there is a need for such access. However, such individuals will not be eligible for access to any greater level of classified information than the U.S. Government has determined can be releasable to the country of which the individual is currently a citizen.

(2) Nonimmigrant aliens in the United States cannot be used under any FAA classified contract or agreement.

8. Exceptions to the Residency Requirement.

a. U.S. citizens who worked in a foreign country for the U.S. Government in a Federal position or as a member of one of the branches of the U.S. military are exempt from the requirement to have resided in the United States for 3 of the last 5 years.

b. Foreign nationals and immigrant aliens applying for contractor employee positions at FAA locations overseas are exempt from the requirement to have resided in the United States for 3 of the last 5 years.

c. Foreign nationals and immigrant aliens applying for positions under contracts within the United States who are not exempt from the investigative requirements under paragraph 3 of this chapter can be granted a waiver of the requirement to have resided in the United States for 3 of the last 5 years, provided the operating office submits a request in writing to AIN-1. The request must be approved by AIN-1, or his or her designee, prior to the contractor employee beginning work. (Refer to paragraph 9 of this chapter.)

d. Foreign nationals not residing in the United States but working for a foreign entity and supporting FAA contracts outside the United States are exempt from the investigative requirement.

e. Foreign nationals who fall under paragraph 8d of this chapter, are exempt from the investigative requirement unless they have access to FAA facilities, resources, and sensitive unclassified information. If they do have access, the PSS cannot conduct an appropriate background check on these types of foreign nationals, so they must obtain as much information as possible and forward the information to AIN-400. Foreign nationals often are granted a form of clearance under the North Atlantic Treaty Organization (NATO). The PSS should make every attempt at obtaining a copy of the NATO certificate that was issued by the country who granted the clearance. They can use this to certify background check information. All information obtained from the certificate should be recorded in ITS. Depending upon access and circumstances, operating offices must ensure that these foreign nationals are escorted at all times.

9. Procedures for Requesting a Residency Waiver. The operating office or logistics component, in consultation with the PSS, can submit a request for waiver of the 3-year residency requirement to the Office of Internal Security and Investigations, AIN-1, through their SSE.

a. They must ensure that requests for waivers are in writing, i.e., memorandum or email, and include:

- (1) a detailed justification of the reason for the waiver request;
- (2) a copy of a completed FAA Form 1600-77 for the position;
- (3) the name, date of birth, place of birth, and country of citizenship of the individual under consideration;
- (4) identity of the line of business, organization, or office by routing symbol and title or the physical location(s) where the individual will be working and the extent of time he or she will be at that location; and
- (5) name of contract company and contract number.

b. ASN-1 or his or her designee will advise the SSE or PSS within 5 days, if possible, whether or not the waiver has been approved. If approved, the PSS will notify the operating office or logistics component within 1 working day upon approval of the waiver and interim suitability determination.

c. The PSS will advise the operating office or logistics component immediately upon determining that a waiver request is disapproved or a foreign national is not suitable for employment under an FAA contract or other agreement.

10. Investigative Requirements for Access to Information Resources. A person has access to information resources when he or she can exercise privileges to read and write information or other data electronically stored or processed in a digital format. Personnel security plays an integral part in information resources security because it ensures sufficient protection for FAA systems and their data. Because of the nature of information resources and the ease with which large amounts of data can be retrieved, manipulated, and deleted, FAA is more stringent with access requirements than for the same level of data contained in records systems outside information resources.

a. Positions requiring Level I access to information resources. Level I data is the authorization to read or write classified information or data electronically stored in a digital format. The minimum investigative requirement is dictated by the position sensitivity level and the level of security clearance required. The contract company must coordinate with DSS for contractor employee investigations and security clearances. (Refer to paragraph 3 of this chapter.)

b. Positions requiring Level II access to information resources. Level II data is the authorization to read or write sensitive unclassified or Privacy Act information or data electronically in a digital format. The minimum investigative requirement will be a fingerprint check or a NACI as dictated by the position risk level designation. If the position is deemed a critical-area position, the minimum investigative requirement will be an NACI. (Refer to paragraph 3 of this chapter.)

c. Positions requiring Level III access to information resources. Level III data is the authorization to read or write unclassified and nonsensitive information or data electronically stored in a digital format. The minimum investigative requirement for these positions will be a fingerprint check. If the position is deemed a critical-area position, the minimum investigative requirement will be an NACI. (Refer to paragraph 3 of this chapter.)

11. Standards for Using and Obtaining Previous Investigations. Some contractor employees may have already been investigated by another Federal agency. As the PSS, you should use these investigations whenever practicable to reduce the number of investigation requests, associated costs, and unnecessary delays. You should conduct updated investigations for all contractor employees who are new to a contract and whose current investigation is older than 10 years. You must follow the standards below.

a. Any investigation not older than 10 years that was conducted by or for another Federal agency on a contractor employee that is of the *same type and scope* as the one

required for the position is sufficient to meet the investigative requirements provided that the contractor employee has had no break in employment in excess of 2 years with the other Federal agency. You can accept all such investigations except when there is substantial information indicating that an individual may not meet the suitability standards and criteria stated in chapter 6.

b. Any investigation not older than 10 years that was conducted by or for another Federal agency on a contractor employee that is a level *higher* than that required for the position is sufficient to meet the investigative requirements provided the contractor employee has had no break in employment in excess of 2 years with the other Federal agency. You can accept all such investigations except when there is substantial information indicating that an individual may not meet the suitability standards and criteria stated in chapter 6.

c. Any investigation conducted by or for another Federal agency on a contractor employee whose scope is *less* than that required for the position can be upgraded as provided for by OPM to meet the investigative requirements of the position if it was conducted within the past year, and the contractor employee has had no break in employment in excess of 2 years with the other Federal agency. You can accept all such investigations in conjunction with an upgraded investigation, except when there is information indicating that an individual may not meet the suitability standards and criteria stated in chapter 6.

d. You cannot use an investigation conducted by a state or local government agency, regardless of how extensive it is, because it does *not* meet the investigative requirements stipulated in paragraph 3 of this chapter. However, if there are unique circumstances that warrant immediate hiring; such as, the terrorist attack of September 11, 2001, FAA will make an exception to this requirement.

e. You cannot use an investigation conducted by a private company or non-government entity regardless of how extensive it is, because it does *not* meet the investigative requirements stipulated in paragraph 3 of this chapter.

12. Process for Using and Obtaining Previous Investigations.

a. When reviewing investigative forms, the PSS should pay particular attention to questions 11, 16, and 18 on the SF-85P, Questionnaire for Public Trust Positions because the contractor employee may have reported a previous investigation. Such information may include:

- (1) recent Federal employment;
- (2) military service, including service with the National Guard or reserves;

(3) continuous employment with a contractor in support of a Government contract with no break in service of more than 2 years; or

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

b. If feasible, the PSS must obtain any previous investigation that is readily available for review prior to authorizing a contractor employee to begin work.

c. If the previous investigation is not readily available, the PSS must obtain as much information as possible about the investigation before authorizing the contractor employee to begin work. To obtain this information, contact:

(1) the security office of the agency for which the investigation was conducted; or

(2) the agency that conducted the investigation; OPM, Defense Security Service (DSS), Federal Bureau of Investigation (FBI), etc.

d. If no previous investigation is available for review, but current information on the SF-85P revealed potential issues, the PSS should initiate a new investigation.

13. Funding for Contractor Security Screenings. Each line of business will fund security screenings, such as background investigations and fingerprint checks on contractor employees, unless other funding provisions have been made with their SSE. The operating or program office for which the work, services, or supplies are being contracted must establish a funding mechanism for these security screenings. They should not incorporate this funding into the affected contracts and they should establish procedures to provide the SSE with funding information. On behalf of the SSE, the PSS will notify operating offices of all cost increases for an investigation.

14. Initiating and Closing Investigations. The PSS is responsible for ensuring that all requests for investigation that do not involve access to classified information are submitted to OPM as required by this paragraph within 5 -10 working days of receipt. Since DSS conducts the background investigations for contractor employees who require access to classified information and grants the security clearances, this section will not address those investigations.

a. Submission of forms. The logistics component has the primary responsibility for ensuring that required investigative forms for investigation of contractor employees are submitted to the PSS. The PSS is responsible for providing written authorization allowing the contractor employees access to FAA facilities, sensitive unclassified information, and resources. The operating office will assist the logistics component as necessary.

- (1) Prior to any contractor employee beginning work on an FAA contract, contract companies must submit completed investigation forms on each individual directly to the SSE. Because of Privacy Act requirements, and the sensitive nature of the forms, all forms must be submitted in a sealed envelope. The contract company should not review investigation forms unless provisions have been made between the employee and the company to do so. When circumstances prevent direct submission to the SSE, the forms may be submitted in a sealed envelope directly to the logistics component who will send them without inspection to the SSE who will forward to the PSS for processing.
 - (2) The contract company must send a letter, along with the investigation forms, identifying each proposed contractor employee, and the contract number.
- b. Forms Requirement.** Specific forms required to initiate security screenings are:
- (1) For low risk positions requiring a fingerprint check – one FD-258, FBI Fingerprint Card, OF-306, Declaration for Federal Employment (Appendix D). The OF-306 serves as a release of information.
 - (2) For low and moderate risk positions requiring a NACI – one FD-258, and one Standard Form (SF) 85P, Questionnaire for Public Trust Positions.
 - (3) For moderate risk positions with fiduciary responsibilities requiring a NACI – one FD-258, one SF-85P, and one DOT Form 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (Appendix E).
 - (4) For high risk position requiring a BI - one FD-258, one SF-85P and DOT Form 1631.
- c. Initiation guidelines.** As the PSS, you must:
- (1) Review the investigative forms for accuracy and completeness and determine whether any background investigation has been previously conducted prior to submission to OPM. Return incomplete forms to the logistics component or contract company in a sealed envelope for correction by the affected contractor employee, *or* contact the affected contractor employee to obtain any missing or omitted information. Contact the logistics component or COTR for assistance if you cannot reach the contractor employee. You must not discuss the specific information required with the logistics component or COTR without approval of the contractor employee; therefore, the logistics component or COTR should have the contractor employee contact you directly.
 - (2) Initiate all contractor employee background investigations to OPM within 5 - 10 working days of receipt of the completed investigative forms if no additional information is required.

(3) Not submit any forms to initiate an investigation until you have completed the preliminary review and are satisfied that the forms are complete and accurate.

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

(1) Discontinue an investigation whenever it becomes clear that the investigation is no longer needed, such as when a contractor employee declines a position or is no longer being considered, and there is no indication that he or she will return as a Government contractor. The logistics component, operating offices or contract company must immediately notify you when they become aware that discontinuing an investigation is warranted.

(2) Telephonically advise OPM immediately upon determining that an investigation should be discontinued. You may follow up with a written notification either by letter, electronically, or fax that includes the reason for discontinuance. Also, notify the servicing accounting office to advise them of the expected charge for the incomplete investigation, if any. You can contact OPM, if necessary, to resolve any subsequent question as to the charge for an incomplete, discontinued investigation. Generally, OPM will charge the full price for an investigation unless it is cancelled within the first five days. In that case, it may be better if you allow the investigation to continue rather than discontinue it since the contractor employee may transfer to another contract.

15. Filling Out Investigative Forms. If you are the PSS, you should follow the guidance below when completing the top portion of the investigative forms.

a. Complete the *Agency Use Block* items A through P on the *top portion* of each SF-85P submitted for initiation of an investigation.

(1) OPM Use Only: When requesting an Advance Fingerprint, enter *R* into the codes section.

(2) Item A, *Type of Investigation*: Enter the appropriate three-character code for the type of investigation required (refer to the current Federal Investigations Notice for the current OPM expedite and discontinue codes and case billing rates.)

(3) Item B, *Extra Coverage*: Enter the appropriate number or letter when requesting extra coverage or when attaching additional items. Some of the most common extra coverage items are an Advance NAC, enter 3; an INS check, enter *H*; and a credit check, enter 2. Contact OPM for other extra coverage items. Notify the operating office if there is an additional cost for conducting the extra coverage.

- (4) Item C, *Sensitivity/Risk Level*: Transfer the sensitivity or risk level designation from the corresponding FAA Form 1600-77.
- (5) Item D, *Compu/ADP*: Enter the letter *C* if the position is a computer position; if not *leave blank*.
- (6) Item E, *Nature of Action Code*: Enter *CON* to indicate this is a contractor position.
- (7) Item F, *Date of Action*: Leave blank if the contractor has *not* begun work under the contract, including, but not limited to, purchase order, consulting agreement, lease agreement, or MOA. If the contractor employee has begun work, enter the date authorized.
- (8) Item G, *Geographic Location*: Leave blank.
- (9) Item H, *Position Code*: Leave blank.
- (10) Item I, *Position Title*: Enter the *position title*.
- (11) Item J, *SON*: Enter the 4-digit submitting office number.
- (12) Item K, *Location of Official Personnel Folder (OPF)*: Check the *None* block.
- (13) Item L, *SOI*: Enter the 4-digit security office identifier.
- (14) Item M, *Location of Security Folder*: Normally, check the *NPI* block. However, if there is a security file that we created for the contractor employee, check the *SOI* block. If there is no security file or there is no pertinent information in the security file, check the *NPI* block.
- (15) Item N, *OPAC-ALC Number*: Enter the required number or code.
- (16) Item O, *Accounting Data and/or Agency Case Number*: Enter the appropriation or accounting code provided by the operating officer, or logistics component and the cost of the investigation (refer to the current Federal Investigations Notice for the current OPM expedite and discontinue case billing rates).
- (17) Item P, *Requesting Official*: Enter the name, title, and telephone number of the authorizing official. Your supervisor or you should then sign the form. *Do not* date the form until ready to send it to OPM.

b. When requesting a NACI for fiduciary positions, the PSS may:

- (1) Request the extra coverage credit check from OPM.
- (2) Conduct the credit check, in house, where available.

c. The PSS must submit all forms to OPM, Federal Investigations Processing Center (FIPC), P.O. Box 618, Boyers, Pennsylvania, 16018-0618.

16. Closing and Adjudicating Investigations.

a. OPM will send all reports of investigation to the SSE identified by the SOI code on the SF-85P. The PSS must review all reports of investigation for investigative sufficiency and resolve any deficiencies prior to final adjudication.

b. The PSS must adjudicate all reports of investigation on contractor employees to determine their suitability to work under FAA contracts with access to FAA facilities, sensitive unclassified information, or resources. In cases where the PSS believes that information developed during the course of an investigation might result in an unfavorable suitability determination after due process was provided, he or she must consult with the region/center logistics component and any office with a valid need to know. (Refer to chapter 6.) The PSS can also request that an agency report of investigation be opened to resolve issues that may warrant further investigation.

17. Disposition of Incomplete/Closed Pending Investigations. As the PSS, you may determine that an investigation received from OPM that is not entirely complete but contains substantial information, can be adjudicated for suitability if the outstanding portion is *unlikely* to help resolve any issues or impact final adjudication. If the outstanding portion *is likely* to resolve any issues or *may* impact a final suitability determination, you must wait until all outstanding items are received before making a final suitability determination.

CHAPTER 6. SUITABILITY AND ADJUDICATION DETERMINATIONS

1. Application. We, the FAA, use the same suitability standards and criteria, and adjudication process for contractor employees that we use for Federal employees and applicants to ensure fair, impartial, and equal consideration. We must make a suitability determination on every contractor employee in a public trust position working under an FAA contract for which a security screening is deemed necessary. We make this determination based on the application of sound adjudicative guidelines to security screenings, including background investigations, fingerprint checks, and related security information concerning contractor employees or applicants.

2. Responsibility. Within FAA, personnel security specialists (PSS) located in the servicing security element (SSE) are assigned all suitability adjudication authority for contractor employees applying for work under *unclassified* contracts. As stated in paragraph 3 of this chapter, the focus of the adjudication is on whether use of a person in a contract capacity will promote the efficiency of the service. This chapter prescribes to the PSS suitability determination requirements and the basic suitability adjudication process for the FAA.

3. Suitability. Suitability means fitness or eligibility for employment and refers to identifiable character traits and past conduct sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a Federal contractor job with appropriate efficiency and effectiveness. PSSs must focus on whether use of the individual in a contract capacity will promote the efficiency of the Federal service when applying these standards and criteria to the contractor environment. They must realize that suitability is different from a person's ability to fulfill the qualification requirements of a job, which is measured by experience, education, knowledge, skills, and abilities.

4. Suitability Requirements.

a. OPM will send all reports of investigation to the SSE. The PSS will review them for investigative sufficiency and resolve any deficiencies in the report prior to formal adjudication.

b. If, after receipt of a completed report of investigation, the PSS determines that additional investigative work is required to make a suitability determination, he or she must follow the criteria and procedures outlined in this chapter.

c. The PSS must adjudicate all reports of investigation on contractor employees to determine their suitability to work under FAA contracts that provide access to FAA facilities, sensitive unclassified information, and resources.

d. The PSS must provide contractor employees due process prior to making an unfavorable suitability determination based on information obtained in a report of investigation, however, if circumstances warrant, FAA can deny the contractor employee access to its facilities, sensitive unclassified information, and resources, until all issues are resolved.

(1) The PSS must provide due process either orally or in writing. They can either give or read the contractor employee a Privacy Act Notice (Appendix F) prior to beginning the process then clearly explain the unfavorable information. The affected contractor employee has an opportunity to respond to unfavorable information within a reasonable amount of time, but not more than 15 days from the date of the due process notification.

(2) The PSS must communicate directly with the affected contractor employee when providing due process to protect his or her rights under the Privacy Act.

(3) The PSS must consider any information the contractor employee has provided within the prescribed timeframe before making a final suitability determination, however, FAA does not have to give him or her any additional opportunity to respond to the decision.

(4) The PSS must make a suitability determination based on the information available if the contractor employee does not respond within the prescribed timeframe.

(5) The PSS must notify the logistics component in writing of unfavorable suitability determinations. The logistics component must then notify the contract company to remove the employee from performance under the contract or to take other action as directed. The logistics component must then report back to the PSS when the removal or other action is completed. An example of other action is: denying a person access to FAA financial records due to bad credit history, but still allowing him or her to work at either another location or in another position where such access is not required.

(6) PSSs must coordinate with AIN-400 either verbally or in writing *before* taking adverse action on any contractor employee supporting a *national* contract. This includes denying interim as well as, final suitability, or requesting reassignment or removal of a contractor employee.

(7) Due to strict requirements under the Privacy and Freedom of Information Acts, PSSs can release information only to the contractor employee on whom the information pertains.

5. Suitability Adjudication. Suitability adjudication is an assessment of past and present conduct that if adverse can cause an impact on the efficiency of the service. As

the PSS, you must assess or decide whether there is a reasonable expectation that the use of a person under contract or other agreement with FAA either would or would not promote the efficiency of the service. You will make suitability determinations through a three-level process of adjudication consisting of:

a. Basic suitability adjudication. This is the first level of suitability adjudication and is an assessment of conduct as it affects a person's suitability to work or provide services under any FAA contract, including, but not limited to, purchase order, consulting agreement, lease agreement, or MOA.

b. Position risk adjudication. The next step in the adjudication process applies to persons rated suitable at the basic suitability level who are being considered for work or to provide services in specific positions. It is an assessment of a person's conduct as it affects his or her suitability in terms of the risk or sensitivity level of a specific position. In this step, you must view issues more seriously when the position is at a higher risk or sensitivity level in order to reflect the greater potential for adverse impact on the efficiency of the service.

c. Position performance adjudication. This is the final step in the adjudication process and it applies to persons who have been rated suitable at the first two levels. You must assess the issues or conduct in terms of its *nexus* or potential impact of the person's performance in a specific position, including any indicated risk for abuse of the public trust in carrying out specific duties.

6. Suitability Guidelines. You, the PSS, must apply the suitability standards outlined in this chapter when making all suitability determinations including interim suitability. The following subparagraphs provide you with a definition and an explanation of these standards and additional criteria where necessary, examples of each criterion, how to apply each criterion when adjudicating, and potentially mitigating factors.

a. Misconduct or Negligence in Prior Employment.

(1) Definition. Behavior that would have a bearing on efficient service in the position in question or would prevent or interfere with an effective accomplishment of an agency's mission.

(2) Examples of issues.

(a) Violation of agency rules and regulations.

(b) Employee fraud, negligence, embezzlement.

(c) Employee theft.

(3) General application.

(a) The misconduct or negligence in prior employment may or may not have resulted in disciplinary action or dismissal from that employment.

(b) If dismissal resulted, you should place the primary emphasis on the act or conduct that prompted the dismissal rather than on the mere fact that the person was dismissed. The emphasis of the adjudication must be on the act or conduct, *not* the disciplinary action. Some employers will lay off or offer resignation options to an employee who was negligent or committed misconduct rather than remove the employee by direct dismissal. The adjudicator must focus on a pattern of employment conduct that is incompatible with successful job performance.

(4) Mitigating conditions.

(a) Amount of time that has transpired since the incident(s) in question.

(b) Age of the applicant at the time of the incident(s) in question.

(c) Evidence that the individual has been rehabilitated.

(d) Favorable performance reviews.

(e) Favorable testimony from supervisors.

(f) The misconduct was the result of pressure, coercion, or personality conflict, and those pressures and/or conditions are no longer present in the person's life, and are not likely to recur.

b. Criminal or Dishonest Conduct.

(1) Examples of criminal conduct.

(a) Theft.

(b) Prostitution.

(c) Burglary.

(d) Murder.

(e) Sexual assault.

(f) Rape.

(g) Assault and battery.

- (h) Indecent exposure.
 - (i) Child molestation.
 - (j) Falsification of documents.
- (2) Examples of dishonest conduct (some of these examples may also be criminal conduct).
- (a) Willful disregard of financial obligations.
 - (b) Embezzlement.
 - (c) Check fraud.
 - (d) Income tax evasion.
 - (e) Filing deceptive loan applications.
 - (f) Benefit fraud.
 - (g) Offer or acceptance of a bribe.
- (3) General application. There must be a *nexus* between this conduct and the duties of the position to which applied.
- (a) This conduct may or may not have resulted in arrest.
 - (b) The primary concern with criminal conduct is the nature of the conduct, whether or not the person has served time or made amends, evidence of rehabilitation, and the effect such conduct can have on the efficiency of the service. You must consider the facts and circumstances of the behavior in all decisions, even where the record has been expunged or a pardon has been granted. Persons under indictment or formal criminal charges may not be considered for work or to provide services under any FAA contract, including, but not limited to, purchase order, consulting agreement, lease agreement, or MOA until disposition is made of the pending charges if the pending charges required referral.
 - (c) The primary concern with dishonest conduct is whether the act was a deliberate disregard for the rights of others, for the benefit of the individual committing the act or for the benefit of other persons.
- (4) Mitigating conditions.

- (a) The crime or dishonest conduct was an isolated incident.
- (b) The criminal or dishonest behavior was not recent.
- (c) The person did not voluntarily commit the criminal or dishonest act and/or the factor(s) leading to the conduct is not likely to recur.
- (d) The person was pressured or coerced into committing the criminal or dishonest act, those pressures and/or conditions are no longer present in the person's life, and are not likely to recur.
- (e) Acquittal of the crime.
- (f) There is clear evidence of successful rehabilitation.

c. Financial Irresponsibility.

- (1) Examples of financial irresponsibility include.
 - (a) Judgments.
 - (b) Collection accounts.
 - (c) Delinquent accounts.
 - (d) Liens.
 - (e) Non-payment of child support.
- (2) General application. You must not make a determination based solely on the dollar amount of indebtedness.
- (3) Mitigating conditions.
 - (a) The individual has demonstrated intent to re-pay, satisfy, or resolve the indebtedness.
 - (b) The individual has consulted with a financial counseling service to consolidate and resolve the indebtedness.
 - (c) The indebtedness was the result of a catastrophic event, such as a death or serious illness in the family for which the individual was financially responsible.

(d) The indebtedness was the result of a clerical error on the part of the reporting credit bureau or creditor and the individual is able to provide proof of the error.

(e) The indebtedness was the result of alcohol or drug abuse, family pressures, and/or other factors that are no longer present in the person's life and are not likely to recur.

(f) There is no nexus between the conduct and the duties of the position.

d. Intentional False Statement, Deception, or Fraud in Examination or Appointment.

(1) Explanation. Evidence that an applicant has been deceptive either by omission of information or by untruthful responses to questions asked on the application or investigative forms.

(2) Examples of issues include.

(a) Bogus claims of formal education or degrees or altering college transcripts.

(b) Failure to admit criminal charges, arrests, and/or convictions.

(c) Failure to admit or misrepresenting financial delinquencies.

(d) Failure to admit or misrepresenting medical issues.

(e) Omission of employment problems or terminations.

(f) Failure to admit or misrepresenting alcohol or drug problems.

(g) Impersonation in examination.

(h) Collusion in examination.

(i) Assuming the identity of a person who has eligibility for a given Federal position.

(j) Altering the score on an OPM Notice of Rating.

(k) Altering the condition of discharge on military discharge documents.

(l) Falsifying an application or appointment document.

(3) General application. The false statement, deception, or fraud must be a material fact, one which, had it been known prior to appointment, would have substantially influenced the decision to select the person over other competitors or would have affected that person's relative position on a certificate of eligibles.

(4) Mitigating conditions.

(a) The falsification was an isolated incident, was not recent, and the individual subsequently provided the correct information *voluntarily*.

(b) The individual made prompt, good faith efforts to correct the falsification *before* being confronted with the facts.

(c) The omission of the material fact was caused or significantly contributed to by the inadequate advice of authorized personnel and the previously omitted information was promptly and fully provided.

(d) The person was pressured or coerced into committing the act, those pressures and/or conditions are no longer present in the person's life, and are not likely to recur.

e. Alcohol Abuse.

(1) Explanation. The abuse must be of a nature and duration that suggests that the person would be prevented from performing the duties of the position in question, or would constitute a direct threat to property or the safety of others.

(2) Examples of alcohol-related issues.

(a) Alcohol-related arrests and incidents away from work, such as Driving Under the Influence (DUI), Driving While Intoxicated (DWI), fighting, child or spousal 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, drinking on the job, or disciplinary problems and/or terminations from employment resulting from the use and/or abuse of alcohol.

(c) Alcohol-related counseling or treatment. Diagnosis by a credentialed medical professional of alcohol abuse or alcohol dependence.

(d) Habitual or binge consumption of alcohol to the point of impaired judgment.

(e) Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

(3) General application.

(a) You must obtain evidence that suggests the contractor employee can be prevented from performing the duties of the position in question or would constitute a direct threat to property or the safety of others.

(b) Current, continuing abuse would *ordinarily* be disqualifying. Abuse can manifest itself in poor employment records, debts, domestic difficulties, or convictions. 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 non-disqualifying.

(4) Mitigating conditions.

(a) The alcohol-related incidents do *not* indicate a *pattern*.

(b) The problem occurred a number of years ago or outside the scope of the investigation and there is *no* indication of a *recent* problem.

(c) Positive changes in behavior supportive of sobriety.

(d) The alcohol abuse was the result of indebtedness, family pressures, and/or other factors that are no longer present in the person's life and are not likely to recur.

(e) There is no nexus between the conduct and the duties of the position.

f. Illegal Use of Narcotics, Drugs, or Other Controlled Substances.

(1) Explanation. Improper or illegal involvement with drugs or controlled substances raises questions regarding an individual's willingness or ability to protect sensitive unclassified information. In addition, drug abuse or dependence may impair social or occupational functioning, interfering with the individual's ability to perform the duties of the position in question and rendering the individual a direct threat to property or the safety of others.

(2) Examples of issues include.

(a) Drug-related arrests and incidents.

(b) Admission of use.

- (c) Disciplinary problems or terminations related to drug activity.
 - (d) Drug-related counseling or treatment.
 - (e) Failing a drug-screening test.
 - (f) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale or distribution.
 - (g) Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional.
 - (h) Recent drug use or an expressed intent not to discontinue the use/abuse.
- (3) General application.
- (a) You must obtain evidence that a contractor employee has had illegal involvement with narcotics, prescription drugs, or other controlled substances without documented substantial rehabilitation.
 - (b) Current or recent use or possession would *ordinarily* be disqualifying. Any pattern is also disqualifying, unless there is a clear, lengthy break since the last occurrence.
- (4) Mitigating conditions.
- (a) The drug involvement was not recent.
 - (b) The drug involvement was an isolated incident or aberration or was the result of indebtedness, family pressures, or other factors and these factors and circumstances are no longer present in the person's life and are not likely to recur.
 - (c) The individual satisfactorily completed a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.
 - (d) The individual demonstrated intent not to abuse any drugs or controlled substances in the future.

g. Questionable Loyalty.

- (1) Explanation. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force. An individual must be unquestionably

loyal to the U.S. The willingness to act in the best interest of the FAA and, in turn, the U.S. is in doubt if there is any reason to suspect an individual is disloyal.

(2) Examples or indicators of disloyalty (possible disqualifying conditions).

(a) Involvement in any act of sabotage, espionage, treason, terrorism, sedition or other act whose aim is to overthrow the U.S. Government and/or alter the form of government by force or violence or by other *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 U.S. Government or any state or subdivision by force or violence or by other unconstitutional means.

(d) Involvement in activities that unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the constitution or laws of the United States or of any state.

(e) Establishing contact with any representative of a foreign government whose interests may be contrary to those of the U.S.

(f) Membership in an organization that advocates or commits criminal acts against the U.S. Government.

(g) Establishing contact with a seditionist, anarchist, or terrorist.

(3) Mitigating conditions.

(a) The person was unaware of the unlawful aims of the individual or organization with which he or she has established an association and severed ties upon learning of this.

(b) The person's involvement was only with lawful or humanitarian aspects of such an organization.

(c) Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest.

(d) The person's involvement or association with such activities was not recent.

(4) General application: Traitorous acts are disqualifying. Any question concerning an applicant's loyalty to the United States is a serious suitability issue that will likely be disqualifying.

(a) Knowing membership in, with specific intent to further the aims of, an organization that 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 U.S. Government by unlawful or unconstitutional means is disqualifying.

(b) You must establish one or more of the following:

1 The person is a member of the organization.

2 The aims of the organization were/are illegal.

3 The person is aware of the illegal aims of the organization.

4 The person has done something to further the illegal aims of the organization.

h. Statutory/Regulatory Debarment.

(1) Explanation. Any statutory or regulatory bar that prevents the lawful employment of the person involved in the position in question. This criterion applies only to Federal employees, but is a concern when making a suitability determination on a contractor employee.

(2) Examples of statutory and regulatory debarment.

(a) Participation in a strike against the U.S. Government. (Legal Authority – 5 U.S.C. 7311; 18 U.S.C. 1918.)

(b) Willful and unlawful concealment, removal, mutilation, or destruction of public records and materials. (Legal Authority - 18 U.S.C. 2071 (b).)

(c) Knowing and willful failure to register under Section 3 of the Military Selective Service Act (50 U.S.C. App. 453). (Legal Authority - 5 U.S.C. 3328.)

(d) Individuals who have been convicted of a misdemeanor crime of domestic violence are prohibited by statute from possessing any firearm or ammunition. This provision applies to persons convicted at any time prior to or after the passage of the September 30th, 1996, amendment. There is no exception for law enforcement officers/agents. (Legal Authority - 18 U.S.C. 922 (g)(9).)

(3) Mitigating conditions. There are no mitigating factors or conditions to statutory or regulatory debarment.

(4) General application. Statutory disqualifications are used in specific situations when an individual has committed certain acts defined by the statute as disqualifying for Federal employment. Contractor employees cannot be debarred, however, this criterion should be considered in conjunction with the other criteria.

7. General Adjudication Process. You, the PSS, serve as an adjudicator.

a. You must consider *all* available, reliable information about the person in question. This is referred to as the *whole person* concept. You must consider past and present, favorable and unfavorable information in reaching a determination. There must be a *nexus* between the behavior, conduct, or incident in question, and the duties of the position.

b. You must consider the following factors when making suitability determinations, where pertinent to the individual case:

- (1) Kind of position applied for, including degree of public trust or risk in the position.
- (2) Nature and seriousness of the conduct.
- (3) Circumstances surrounding the conduct.
- (4) Recency of the conduct.
- (5) Age of the person at the time of the conduct.
- (6) Contributing societal conditions.
- (7) Absence or presence of efforts toward rehabilitation.
- (8) A combination or pattern of issues.

c. Other factors affecting suitability determinations.

(1) You must also examine actions taken by a contractor employee *subsequent* to the issues in question. Consider whether the person:

- (a) Voluntarily reported the information.
- (b) Was truthful and complete in responding to questions or inquiries.

(c) Sought assistance and followed professional guidance, where appropriate.

(d) Has demonstrated positive changes in behavior and employment.

(2) Background investigations will sometimes include information provided by source(s) who request confidentiality under the Privacy Act. This is known as protected source information. You can use protected source information in the resolution of derogatory information without identifying the source as long as the information is corroborated by at least one other source.

(3) Classified information may appear in background investigations and may contain derogatory information requiring resolution. If necessary, you should consult with his or her supervisor as to the appropriate handling and use of this information in the adjudicative process.

(4) All males born after December 31, 1959, including legal permanent residents, must have registered with the Selective Service. If the contractor employee has not registered before his 26th birthday, he must provide you with an explanation explaining the reasons why he did not register. Do not disqualify a contractor employee merely on the fact that he did not register with the Selective Service.

(5) You must not deny interim suitability to a contractor employee who is currently serving probation for a crime based solely on fact that he or she is on probation. In these cases, consider the nature of the crime and the guidelines outlined in this paragraph and paragraph 6 of this chapter, as well as other factors contained in this chapter.

d. As the PSS, you should determine whether the issue(s) is/are actionable or non-actionable when derogatory information is identified and weighed against the above factors.

(1) Actionable. An issue for which resolution requires you to contact the person in question, either orally or in writing, in order to make a suitability determination. Any issue deemed actionable must be adjudicated. It is not sufficient to resolve derogatory information by merely indicating that the person exhibits acceptable job performance.

(2) Non-actionable. An issue that has been previously favorably adjudicated, is minor in seriousness, has no nexus with the position applied for, or is well outside of the scope of the investigation; one that has been negated to the point that it would have no bearing on the applicant's suitability for employment.

8. Issue Resolution. While the examination and evaluation of the seriousness of issues for contractor personnel mirrors that of Federal employees, the means by which you, the PSS, must resolve these issues and the extent to which contractors are afforded due

process is more limited. For example, contractor employees have no appeal rights. FAA has full control over granting, denying, withholding, and terminating unescorted access to its facilities or sensitive unclassified information to contractor employees based on the results of a background investigation. Prior to taking steps toward issue resolution, you must present a Privacy Act Notice or similar advisement to the contractor employee. You must resolve issues in one of the ways below, or a combination thereof:

a. Telephonic. Conduct telephonic interviews, as necessary. Use this method of issue resolution to resolve relatively minor but actionable issues.

b. Written inquiry. Obtain written documentation, as necessary. Use this method of issue resolution to resolve issues of a serious nature that would likely result in denial of suitability when other attempts to contact the affected contractor employee have failed. The objective of the letter of inquiry is to obtain information and written documentation from the affected contractor employee to be used in the adjudicative process and to resolve the issue(s).

c. Personal Subject interview. Conduct a face-to-face interview, when practicable. Use this method of issue resolution to resolve issues of a serious nature that would likely result in denial of suitability or when immediate resolution of the issue(s) is desired.

d. Additional SSE investigation. Conduct additional investigative work, if needed, to resolve issues *before* making a suitability determination.

(1) Additional investigation criteria.

(a) The PSS may request that a Report of Investigation (ROI) be opened whenever:

1 the additional work required consists of interviews with several sources or extensive records checks.

2 there is at least one material, unresolved issue, the resolution of which would impact a suitability determination; and

3 a determination was made that the Subject of the investigation is still under active consideration as a contractor employee and has neither declined employment with the contractor nor been terminated by the contractor.

(b) The PSS should *not* request an agency ROI:

1 solely to conduct an interview of a contractor employee, or to conduct brief, follow-up records checks with courts or law enforcement agencies.

2 to conduct checks that can be conducted electronically or by mail.

3 when existing reports resolve all material issues; i.e., issues whose resolution would be likely to impact a suitability determination.

4 when admissions by the Subject provide sufficient information on which to make a suitability determination.

5 when issues, even if unresolved, are minor or in the distant past, and resolution would *not* impact a suitability determination.

(2) Initiation of agency ROIs. FAA investigators conduct all ROIs following procedures established by the Office of Internal Security and Investigations (AIN). If an investigation is not necessary, the PSS should interview the Subject in person or telephonically, or send a letter or memorandum to him or her in order to fulfill the due process requirements. The PSS can also request that the Subject provide information or documentation regarding the issues.

(3) Documenting investigative work.

(a) If there is a need for substantial investigative work in addition to an interview with a contractor employee, then all of the investigative results, including the interview, will be reported in an ROI in accordance with procedures established by AIN.

(b) If there is no need for an investigation, then the PSS must prepare a memorandum or summary to the contractor employee's PSF to document the results of an interview and any additional checks conducted. Include written statements from the Subject.

e. Additional OPM investigation. The PSS can request that OPM re-open an investigation or that OPM expand the investigation (for an additional fee) in order to resolve issues identified in the OPM investigation that were not resolved or followed up by OPM.

f. The final step in the adjudication process involves an assessment of conduct in terms of its present or potential impact on the person's ability to occupy a specific position, including any indicated risk for abuse of trust in the position or any potential for damage to our mission.

9. Due Process. As stated in paragraph 8 of this chapter, contractor employees have no formal appeal rights. Before making an unfavorable suitability determination, you, the PSS, must afford the affected contractor employee an opportunity to refute, explain, or mitigate any unfavorable information. You must:

a. Afford the contractor employee due process and address all material issues, and, if necessary, deny interim suitability.

b. Afford the contractor employee due process and address all material issues, and, if necessary, deny final suitability.

c. Afford the contractor employee due process and address all material issues that arise after the employee has been working on the contract.

d. Request temporary removal of a contractor employee during the due process phase if the issues are significant enough to cause a threat to safety, i.e., a contractor air traffic controller who is arrested for drug usage; or someone who is exhibiting violent behavior that can cause harm to FAA personnel.

10. Due Process Procedures. Below are procedures for providing due process that the PSS must follow:

a. Provide a Privacy Act Notice (Appendix F) or verbal Privacy Act advisement to the contractor employee. When provided verbally, notate as such.

b. Conduct an interview, either telephonic or in person, of the affected contractor employee to resolve minor actionable issues, or ask for documentation that could mitigate the issue. Upon completion of the interview, prepare a memorandum summarizing the information discussed and requested, or have the Subject provide a written statement addressing the issues.

c. If an interview cannot be conducted, send the affected contractor employee a letter of inquiry to resolve all serious actionable issues.

(1) Prepare a letter to the affected contractor employee on regional, center, or divisional letterhead and include a description of the issue(s) requiring resolution.

(a) All written inquiries must be sent via certified mail with return receipt directly to the affected contractor employee and addressed, "TO BE OPENED BY ADDRESSEE ONLY."

(b) The questions contained within the letter of inquiry should pertain only to the issues disclosed during the investigative process.

(c) Allow the affected contractor employee a minimum of 15 days, *after receipt*, to respond to a written inquiry. Grant extensions of up to 15 days total to the affected contractor employee to respond to a written inquiry, if requested by the contractor employee.

- (2) Advise the operating office or logistics component of any extensions afforded a contractor employee.
- (3) File a copy of the written inquiry in the affected contractor employee's PSF.
- (4) If a contractor employee does *not* respond to a written inquiry within the given time frame, the person should no longer be considered for the position. An unfavorable determination does *not* mean that the contractor must terminate the affected contractor employee, only that the affected contractor employee will not be allowed to work on, or provide services under, the FAA contract.
 - (a) Prepare a memorandum advising the logistics component that the person is no longer being considered.
 - (b) The contract company or logistics component can always request that the person be reconsidered if he or she later provides the requested information.
- d. It is the responsibility of the affected contractor employee, *not* the PSS, to obtain and provide all requested information and documentation necessary to resolve identified issues.
- e. Complete the INV Form 79A, Report of Agency Adjudicative Action, to indicate type of action taken and submit to OPM.

11. Interim Suitability Determinations. An interim suitability determination is a preliminary assessment that the PSS makes which allows a contractor employee to begin working under an FAA contract prior to completion and adjudication of the background check, and would involve little or no risk to the agency. The PSS should consider interim suitability determinations as the final suitability notification, unless information or situations arise that question the contractor employee's suitability.

12. Interim Suitability Requirements. Interim suitability determinations are not automatic and will not be approved until the PSS has received and reviewed all required investigative forms for each affected contractor employee, addressed any issues, and authorized the affected contractor employee in writing to begin work.

a. Depending on the access the individual has to FAA facilities, sensitive unclassified information, or resources, and the nexus to the position, the PSS can use the following as *possible* disqualifying factors *if not mitigated favorably*:

- (1) Any felony conviction within the last 5 years.
- (2) More than one felony conviction, regardless of when it occurred.

- (3) More than one arrest, regardless of when it occurred.
- (4) Any discharge from employment or resignation after being told he or she would be fired within the last 5 years.
- (5) Pattern of misconduct or abuse.

b. When the PSS is unable to satisfactorily address issues during the interim suitability stage and consequently interim suitability is denied, he or she must notify the logistics component who, in consultation with the operating office, should advise the PSS whether or not to continue with a background check.

13. Documentation and Notification. As the PSS, you must:

- a.** Keep all interim suitability determinations in the contractor security file, or electronically.
- b.** Notify the logistics component, operating office, or contract company in writing of all interim suitability determinations whether favorable or unfavorable.
- c.** Keep copies of all documentation pertinent to the adjudication, including letters or memorandum of proposed action; written challenges, replies, or documentation supplied by the affected contractor employee; and a written summary of any oral response for any case where you propose denial of suitability. If you denied suitability to a contractor employee, keep this documentation for at least 2 years from the date of your final decision.
- d.** Notify your Medical division of all contractor employees in safety-related positions who were denied suitability because of multiple alcohol or drug related issues.
- e.** Be sure to enter all contractor employee records in ITS even if you denied interim suitability. Remember, all PSSs access ITS information and rely on its accuracy.

14. Issuance of FAA Identification (ID) Media. The procedures outlined below will be changing with the implementation of Homeland Security Presidential Directive (HSPD) -12. Refer to the latest edition of FAA Order 1600.25, FAA Identification Media, Official Credentials, Passports, and Vehicle Identification Media, for additional information on FAA ID media issuance.

a. SSEs can issue FAA ID media to contractor employees provided that:

- (1) the contractor employee has been granted interim suitability or a final adjudication determination has been made;
- (2) access to an FAA facility(ies) is at least two times or more a week; and

(3) DOT Form 1681, Identification Card/Credential Application (Appendix G), is completed and signed by the logistics component, COTR, SSE, or other designated FAA employee.

b. SSEs may issue ID media to contractor employees after interim suitability is granted, however, they must ensure that a contractor employee who will be used to provide escort duties does not do so until the requirements of chapter 5, paragraph g, are met.

c. SSEs may issue a form of FAA ID media to consultants who are U.S. citizens working with high-level FAA officials. There is no investigation requirement for these consultants, as long as, the operating office submits a request to the SSE with justification that an agency ID is required, the SSE approves the request, and DOT Form 1681 is appropriately completed and signed.

d. SSEs will not issue FAA ID media to any contractor employee who does not require access to an FAA facility(ies).

e. SSEs will review and make a decision on any request for FAA ID media that does not fit into paragraphs a-d listed above, such as, substitute contractor employees for janitorial services, maintenance, construction, etc.

15. Security Determinations. For sensitive positions, a security determination will usually be made subsequent to a favorable suitability adjudication. While the PSS will make the suitability determinations on contractor employees who are in public trust positions, it will normally not be involved in making security determinations. The Defense Security Service is responsible for conducting the background investigations on all contractor employees requiring access to classified information (including Periodic Reinvestigations), making the security determinations, and granting the facility and security clearances. (Refer to chapter 8.)

CHAPTER 7. CONTRACTOR SECURITY RECORDS

1. Contractor Security Records. In order to maintain records on contractor employees, the FAA must have an automated investigations tracking system. In addition, personnel security specialists (PSS) located in the servicing security element (SSE) must create a Contractor Security File (CSF) for each contract award that has a security requirement and for other awards that warrant it. They must also create a contractor personnel security file (PSF) for contractor employees when there are reports of investigation or other contractor security materials warranting retention. (NOTE: The PSS does not need to create a PSF for every contractor employee.)

a. Investigations Tracking System (ITS). ITS is the primary database that is currently being used in FAA to maintain and monitor the status of personnel security actions on contractor employees. As the PSS, you must:

- (1) Enter required information promptly upon receipt of investigative forms. You have the responsibility to ensure that the data is maintained, current, and accurate in ITS because all of the SSEs have access to this information and rely on its accuracy.
- (2) Enter information concerning contractor employees, including name; social security number; contract company name; contract identification number; position risk/sensitivity level designations; investigations initiated and completed; security clearance actions; interim and final suitability; waivers of investigative requirements; and any other pertinent information.
- (3) Summarize and enter any action or pertinent information concerning a contractor employee, along with the date of entry and your initials in the *Remarks* section. You must ensure that this information is concise and in chronological order. If the information regarding the contractor employee is too lengthy to be put in Remarks, use that section to make a notation of the location of the PSF.
- (4) Enter an X in the *Issues* box and explain in *Remarks*, if there are significant issues either during interim suitability, final suitability, or at any time during the contractors employment. NOTE: If issues are resolved, indicate as such in *Remarks*, however, uncheck the *Issues* box.

b. Contractor security files (CSF). The CSF is used to house all investigative forms and documents relating to a contract that has a security requirement. CSFs will contain, as applicable:

- (1) Copies of FAA Forms 1600-77. If forms are maintained electronically, the PSS does not need to make them part of the CSF, but should notate the file as such.

- (2) Statement of Work (SOW) and security clauses or documentation that the PSS reviewed them.
- (3) Letter from the contract company that certifies individuals on a contract.
- (4) Notifications of interim suitability determinations.
- (5) Documentation and notification of adverse actions.
- (6) OF-306, Declaration of Federal Employment, when it is signed by the contractor employee for use as a release for submission of a fingerprint check.
- (7) Notifications from the contract company of contractor employees who have terminated from the contract or moved to another contract.
- (8) Modifications to contracts that impact security, i.e., contract renewed under a new contract number, etc.
- (9) Documentation of exemption from investigative requirements, if applicable.
- (10) Copies of forms or memoranda documenting final, temporary or interim security clearances, such as, Letters of Consent from the Department of Defense.
- (11) Periodic reports (quarterly, biannually, or as required by the contract) from the contract company that reflect the status of contractor employees.
- (12) Other significant documents or memoranda relating to the contract not listed above.

c. Contractor Personnel Security File (PSF). The PSF is used to house all investigative information relating to a contractor employee when there are reports of investigation and other materials warranting retention. As the PSS, you do not need to keep background checks that contain only minor unfavorable information or outdated information that it is no longer significant. Do not create a PSF solely to maintain security investigative forms or for minor unfavorable information that was adjudicated favorably. However, you should enter the information in the *Remarks* section of ITS in the case of minor issues. Only create a PSF on a contractor employee if you determine that the information warrants retention.

- (1) Not every contractor employee requires a PSF. You should create a PSF under the following circumstances:
 - (a) Contractor employees in high-risk positions requiring a Background Investigation (BI).
 - (b) Foreign national contractors on whom a waiver was requested.

- (c) Contractor employees on whom adverse action was taken.
- (d) Contractor employees whose background check contained unfavorable information that needed resolution.
- (2) The PSF must contain as applicable:
 - (a) Reports of investigation completed by FAA and other agencies, if there is pertinent information.
 - (b) Credit reports only if it is pertinent to the adjudication.
 - (c) Subject interviews conducted to resolve issues that did not warrant an FAA ROI.
 - (d) Case Summary Sheet for background check adjudications, if applicable.
 - (e) Documentation and records received from the Subject mitigating issues.
 - (f) A copy of INV Form 79A or other OPM form documenting final adjudicative action (required only when a PSF is created).

d. File Retention. As the PSS, you do not need to keep a PSF after the contract has been terminated unless the contract has been renewed under a different number, or the contractor employee moved to another company. Keep the PSF:

- (1) For as long as the contractor employee is working under an FAA contract.
- (2) For 30 days following termination of employment if it contains insignificant suitability information or does not contain an FAA ROI.
- (3) For 5 years following termination if it contains an FAA ROI.
- (4) For a period of 2 years from the date of non-selection for non-selected contractor employees who were denied interim suitability due to unfavorable information. If it contains an FAA ROI, keep for 5 years.
- (5) For a period of 2 years from the date of termination for contractor employees whose suitability might be in question due to unfavorable information, but who terminated employment before the information could be adjudicated. If it contains an FAA ROI, keep for 5 years.

2. Review of PSFs. Under the Privacy Act, the SSE must provide contractor employees an opportunity to review their PSF upon request, if one exists. Contractor employees should make all requests for review of their PSF in writing to the SSE where they are

located. They may also, in writing, authorize a representative to review their PSF. If a contractor employee makes the request verbally, the PSS should explain that the request must be submitted in writing to the SSE. The PSS must follow the procedures below when complying with a request for review:

- a. Review the file before letting the contractor employee or authorized individual have access to it or before sending it to a field facility for the contractor employee's review.
- b. Remove any report of investigation completed by another agency, such as OPM, DSS, or FBI, and inform the contractor employee or authorized individual in writing that:
 - (1) the PSF contains a report completed by a specified agency;
 - (2) FAA is not authorized to release it directly to the contractor employee or authorized individual; and
 - (3) the contractor employee or authorized individual should contact the investigating agency directly in order to request a copy.
- c. Remove any other information, such as identification of a confidential source or information concerning an ongoing investigation that is exempt from release under the Privacy Act.
- d. It is preferable for contractor employees to review their PSF at the SSE where they work, however, if they are not located near the SSE, then the PSS can mail the PSF per paragraph e below.
- e. If the contractor employee works at any other location, send only a certified true copy of the PSF to the duty location, retaining the original in the SSE. Enclose the copy in an envelope addressed to the contractor employee marked, "TO BE OPENED BY ADDRESSEE ONLY."
- f. When the review takes place in person at the SSE, the contractor employee or authorized individual must review it only under the direct observation of an SSE employee. That person must provide the contractor employee or authorized individual a reasonable amount of time to review the file and ensure that he or she does not withdraw any documents or pages from it.

3. Safeguarding Records and Privacy Act Requirements. Records, whether electronic or hard copy, that contain sensitive unclassified and Privacy Act information must be protected at all time during handling, transmittal, storage, and release. As the PSS, you must:

a. Provide access to PSFs, reports of investigation, any record of derogatory information, including a contractor employee's response to it, only to individuals who, in their official capacity, have a need to know such information, and to individuals authorized in writing by the contractor employee.

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

c. Carefully control medical reports included as part of an investigation to ensure that the information they contain is disseminated only to persons who need it for suitability adjudication.

d. Protect reports of investigation, PSFs, and other records that contain classified information, and sensitive unclassified information, in accordance with the latest edition of FAA Orders 1600.2, Safeguarding Controls and Procedures For Classified National Security Information and Sensitive Unclassified Information, and 1600.75, Protecting Sensitive Unclassified Information (SUI).

e. Protect, transmit, store, and destroy all PSFs, reports of investigation, personal history statements, and other contractor security records and documents which contain information of a personal or privileged nature, per the latest editions of FAA Orders 1600.2, and 1280.1, Protecting Privacy of Information About Individuals. You must restrict a contractor employee from access to any such records either on himself or herself or on any other employees.

(1) At a minimum, these records will be considered "For Official Use Only." You do not need 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, you should individually mark them "For Official Use Only."

(2) You must ensure that all reports of investigation will be stored in a safe, locked cabinet, or other equally secure area.

(3) You must ensure a need to know before releasing an FAA ROI, or extracts or summaries of these reports to anyone outside your SSE.

4. Privacy Act Requirements. In responding to requests under the Privacy Act for disclosure of information in PSFs and FAA ROIs, the PSS must follow all requirements of the latest edition of FAA Order 1280.1, and the paragraph below.

a. Do not release any report of investigation completed by another Federal agency in response to a Privacy Act request without the consent of that agency (refer to paragraph 2 of this chapter).

b. When receiving third party requests for records, follow the procedures for responding to them as outlined in the latest editions of FAA Orders 1270.1, Freedom of Information Act Program, and 1280.1. Such requests must be in writing.

- (1) The PSS must ensure that a third party request for records under the Privacy Act has a signed statement, by the first party to whom the record pertains, granting the FAA permission to release the records to the specific third party.
- (2) If a third party request for records 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, or other specific identification, the PSS should process the request 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, or other specific identification, then the PSS should respond to the request under the provisions of the FOIA.
- (4) If the request concerns a deceased individual, the PSS must respond to it under the provisions of the FOIA.

CHAPTER 8. NATIONAL INDUSTRIAL SECURITY PROGRAM

1. General. This chapter states policy and procedures for implementing the National Industrial Security Program (NISP) at FAA. It implements E.O.12829, NISP. FAA must apply these procedures whenever contract companies, contractor employees, subcontractors, consultants, or other persons performing work for or under the direction of a Department of Transportation (DOT) administration or organization 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, is responsible for implementing and monitoring the NISP and for issuing implementing directives that will be binding on agencies. By agreement between DOT and the Department of Defense (DOD), DOT authorized DOD to act for, and on behalf of, them in providing security services for the protection of classified information that DOT releases to contract companies, contractor employees, and consultants.

b. When acting as a contracting agency, DOT has the authority and responsibility to perform the functions specified for a user agency in the latest editions of the National Industrial Security Program Operating Manual (NISPOM) and the Industrial Security Regulation (ISR), both of which are issued by DOD. DOD grants facility clearances to contract companies 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 requires persons not employed by the U.S. Government to have access to classified information, the operating office must include that information in a statement with the procurement request. The operating office must also prepare and submit with the request a draft Form DD 254, Contract Security Classification Specification (refer to Appendix C). The Form DD 254 must be prepared as specified in the ISR or other DOD regulations or instructions. The operating office must coordinate the draft Form DD 254 with its servicing security element (SSE) to ensure appropriate classification. The personnel security specialist (PSS), located in the SSE, must review and initial it as assurance that they agree with the contents.

b. If you are the contracting officer (CO) you must review all proposed procurement actions during pre-contract negotiations to determine if there is need for FAA to share classified information with a contractor. If so, you must advise the PSS and provide a list

of prospective bidders. You are responsible for taking action required by DOD. You must also sign and issue a Form DD 254 for each Screening Information Request/Solicitation for Offer.

c. The CO must issue a completed Form DD 254 with the award of each classified contract, including follow-on contracts, and provide a copy of the form to the PSS for initialing.

d. The CO must submit to the PSS electronic or hard copies of FAA Forms 1600-77 identifying the position sensitivity levels, and a Statement of Work (SOW) for review. The PSS must approve or disapprove each form.

e. The CO must ensure that each classified contract or consulting agreement contains a security clause. This clause must specify everything that a contractor or contractor employee has to do to ensure that FAA and DSS can process all contractors for any needed facility or security clearances, and do so according to requirements and procedures stated in the NISPOM, ISR, or other DOD regulations. The CO must make sure that the contract also specifies that all requests for classified visits are followed per the NISPOM and are certified by the SSE prior to forwarding to the organization to be visited.

f. DSS will work directly with contract companies and contractor employees to grant facility clearances and to grant security clearances to individuals. Once a security clearance is granted, the contract company must ensure that the DSS information is forwarded to the SSE.

g. The CO must notify the PSS and DSS whenever the status of a contract changes (i.e., replaced, defaulted, or terminated).

4. Annual Review of Form DD 254. The operating office must review Forms DD 254 for accuracy and currency annually on the anniversary date of the contract, or more often if required by the ISR or other DOD regulation. If changes are necessary, the operating office and the contracting office, in coordination with the SSE, will issue a revised Form DD 254 preparing it as specified in the ISR or other DOD regulation. If no change is necessary, the operating office must notify all holders of the Form DD 254 that it is current in all respects.

5. Visit Requests. Whenever a contractor employee is required to visit an FAA facility and have access to classified information, the contract company must complete, certify, and process a visit request as specified in the NISPOM, ISR, or other DOD regulation and submit the request to the respective SSE for processing.

a. The contract company must ensure that all requests are submitted on company letterhead and include:

- (1) Full name of visitor.
- (2) Position, company, and contract number, if applicable. For subcontractors, identify the name of the company and contract number for which they are working.
- (3) Social security number.
- (4) Date and place of birth.
- (5) Citizenship.
- (6) Clearance information including type of clearance, date of issuance, and basis for the clearance, e.g., Single Scope Background Investigation completed by DSS 3/2/00.
- (7) Purpose and location of visit.
- (8) Date(s) and duration of visit.
- (9) Point of contact at the FAA location, including telephone and fax numbers.

b. The PSS should return requests or call the company regarding visits requests that do not contain the information identified in paragraph 5a of this chapter, to get the information not supplied.

c. The PSS must notify the FAA point of contact or contact office in writing of all approved visit requests either by email or fax signed by them with a notation certifying that the visit is approved.

d. Points of contact or contact offices receiving information directly from a company must return the request to the company notifying them of the proper procedures and directing the company to resend the request through the SSE.

e. The PSS must enter all visitors processed under this paragraph in the non-employee module of the Investigations Tracking System (ITS). If the request specifically identifies the individual as a contractor or subcontractor working on an FAA contract, then process under normal contractor procedures and record in the contractor module of ITS.

f. The PSS must maintain the original incoming request and destroy when no longer active, unless their office has procedures in place to keep the information for a certain period of time.

CHAPTER 9. QUALITY ASSURANCE REVIEW

1. Introduction. This chapter establishes policies and procedures in support of a quality assurance review for the FAA Contractor and Industrial Security Program. It also serves as a quality assurance planning tool for conducting reviews of offices with security and contractual authority to ensure compliance with current FAA orders and other federal regulations. These offices include servicing security elements (SSE), Office of Acquisitions, Policy and Contracting (ATO-A), Assistant Administrator for Region and Center Operations (ARC-1), and logistics components.

a. The objective of the quality assurance program is to ensure that established procedures and processes accomplish FAA's mission(s). It provides for a means of continuous review and oversight to assure that the products and services produced and managed by the program appropriately meet established standards, are consistent, and satisfy FAA's mission.

b. The primary objective of the quality assurance reviews conducted on the Contractor and Industrial Security Program is to ensure that unauthorized access or compromise to FAA's facilities, sensitive and classified information, and resources has not occurred.

2. Program Mission Statement. The quality assurance program applies to the FAA Contractor and Industrial Security Program. This program will ensure:

a. FAA contractor and industrial security policies and procedures parallel the Federal personnel security policies and procedures to the fullest extent practicable.

b. Consistent, efficient, and appropriate implementation of the laws, regulations, and procedures that govern contractor and industrial security by all responsible entities.

c. Employment of entities or persons under FAA contracts promotes the efficiency of the agency and is in the best interest of national security.

3. Quality Assurance Review Standards.

a. The Office of Internal Security and Investigations, Personnel Security Division, AIN-400, will conduct periodic quality assurance reviews as prescribed by this chapter, of all regional and center offices. For the remainder of this chapter, a quality assurance review will be referred to as, *review*.

b. AIN-400 will create a team consisting of two or more persons who will conduct the review. Team composition will consist of a team leader, generally filled by a senior AIN-400 personnel security specialist (PSS), a representative(s) from an SSE not located in the region or center that is being reviewed, and possibly a representative from the logistics component.

c. AIN-400 will closely coordinate all reviews with the SSE and the logistics component of the region or center being reviewed.

d. The AIN-400 team leader must notify the region or center offices at least 30 days prior to commencement that the review is taking place.

4. Conducting the Quality Assurance Review. A successful review requires careful planning, preparation, coordination, organization, and implementation. This chapter provides the team with tools to conduct the review and should be followed as closely as possible, in order to provide the best manner in which to assess the program. Each team member must become familiar with the steps to be performed during a review. This will facilitate an efficient and effective review.

a. Preliminary phase. The team leader must:

(1) Review this order and become familiar with the applicable laws, policies, criteria, and steps necessary to perform the review.

(2) Advise the Assistant Administrator for Region and Center Operations, ARC-1, of the impending review to ensure that the region or center logistics manager is notified.

(3) Notify the office to be reviewed and the responsible headquarters, regional, or center office, in writing, at least 30 days prior to commencement of the on-site review and request:

(a) A list of all awards at the review site whose primary function is information resources penetration testing.

(b) A list of all *classified* awards.

(c) A list of all weapons carrying awards.

(d) A list of all *unclassified* awards for the last fiscal year.

(4) Select 100% of all information resources penetration, classified, and weapons carrying awards for review, and notify the SSE and logistics component of the selections.

(5) Randomly select 20% of all other awards for the past fiscal year, unless the number is less than 25, in which case all must be reviewed. Notify the SSE and the logistics component of the selections.

(6) Ensure that the SSE and the logistics component have all selected awards ready for the team to review, and, if feasible, a private space to conduct the review.

(7) Advise the SSE and the logistics component of any individuals that are to be interviewed regarding the review, and coordinate with them to ensure availability of the individuals.

(8) Examine any materials that were requested in conjunction with the review.

(9) Arrange an in-brief with the review site management.

b. Preliminary phase. The team members must:

(1) Review this order and become familiar with the applicable laws, policies, criteria, and steps necessary to perform the review.

(2) At the request of the team leader, examine any materials that were requested in conjunction with the review.

(3) Assist the team leader regarding any of the items listed above.

c. On-Site Review. The team will:

(1) Conduct an in-brief with managers of the SSE and logistics component, and any other people that the region or center feels should participate. Provide daily briefings, if needed.

(2) Review all requested contract files in the logistics component and check each file to determine that it contains:

(a) FAA Forms 1600-77, Contractor Position Risk/Sensitivity Level Designation, that are accurately completed and contain the appropriate signatures and approvals. If these forms are electronic, it should be notated in the file and still be reviewed.

(b) Interim suitability letters.

(c) Proper security clauses.

(d) Confirmation that the security requirement was properly coded in the logistics database.

(e) Form DD-254 if the contract is classified.

(f) Letters of action pertaining to a contractor employee, if applicable.

(g) Other correspondence that might have an impact on security.

- (3) Review all requested contract security files in the SSE and check each file to determine if it contains:
- (a) A copy of the Statement of Work (SOW) or documentation that the SOW was reviewed.
 - (b) FAA Forms 1600-77 that are accurately completed and contain the appropriate signatures and approvals. If these forms are electronic, it should be notated in the file and still reviewed.
 - (c) Reports of contractor employee listings from the contract company.
 - (d) Transmittal letters from the contract company that certifies individuals on a contract.
 - (e) Notifications of interim suitability determinations.
 - (f) Documentation of adverse actions and confirmation of action taken.
 - (g) Notifications from the contract company of contractor employees who terminated from a contract or moved to another contract.
 - (h) Modifications to contracts that impact security.
 - (i) Documentation of exemption from investigative requirements, when practicable.
 - (j) Documentation of waiver approvals or denials for the 3-year residency requirement for foreign nationals.
 - (k) Copies of forms or memoranda documenting temporary, interim, or final security clearance, such as Letters of Consent from the Department of Defense.
 - (l) Other significant documents relating to the contract, not listed above.
- (4) Review selected PSFs or electronic data for contractor employee background information to see if it coincides with the investigation requirement of the contract positions.
- (5) Conduct interviews of logistics components and SSEs to evaluate their level of knowledge and compliance of the contractor program.
- (6) Collect all necessary supporting documentation or non-compliance documentation.

- (7) Conduct an exit briefing to advise management of significant findings and observations that were discovered during the review. All other findings will be included in the final report.

5. Preparing the Report. The team leader is responsible for writing the report based on the findings and observations discovered during the review. This report is the primary official written record of the quality assurance review. It is intended to provide senior management with concise, candid evaluations of policy and program effectiveness and to inform them of conditions or situations that require attention or intervention. It is not intended to be a detailed review of every feature of the assessed entity. This report should stress major issues and shortcomings, as well as noteworthy contributions to program operations and the agency. The team leader should complete each report with 60 days of the conclusion of the on-site review.

a. Upon completion of the report, AIN-400 must provide a copy of the final report to the Assistant Administrator for Security and Hazardous Materials, ASH-1; Director of Field Operations, AHS-1; Vice President for Acquisition and Business Services, ATO-A (for headquarters reports); and Assistant Administrator for Region and Center Operations, ARC-1 (for region and center reports).

b. ARC-1 is responsible for providing the review site a copy of the final report within 5 days of receipt of the final review report when applicable.

6. Findings and Recommendations. The team must include in the report all findings, corrective actions taken (if corrections were made at the time of the on-site review), recommendations, identification of best practices, if applicable, and observations.

a. Findings are supported by corresponding evidence and deal with noncompliance of FAA orders. The team cannot make a recommendation without a finding. Findings are based on the answers to the following:

- (1) When you conducted the review step(s), what did you find?
- (2) What is the reason for the finding, if known?
- (3) If the finding is not corrected, what will be the impact to the agency?

b. Observations are matters that the team considers important enough to be included in the report but are less significant and basically consultative in nature. Observations are generally issues that are not compliance related.

c. Recommendations are the team's contributions to improving the affected region's performance and to helping managers handle problems more effectively. Effective recommendations should be:

- (1) specific and clearly stated in simple language;
- (2) practical and should direct action based on the *current* situation; and
- (3) directed to the *office*, not individual, responsible for the problem.

7. Report Retention.

- a.** Review sites should keep a copy of review reports for their sites.
- b.** Region/center SSEs must keep a copy of the reports for all quality assurance reviews conducted within their areas of responsibility.
- c.** AIN-400 will keep a copy of all reports and documentation collected during the review and for all past reviews they conducted.

FIGURE 8. SAMPLE QUALITY ASSURANCE REPORT**DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION**

QUALITY ASSURANCE REVIEW OF [ENTER OFFICE NAME(S) AND LOCATION(S)]**DATE OF REVIEW:** [ENTER DATE(S) OF REVIEW]**DATE OF REPORT:** [ENTER DATE REPORT FINALIZED]**REPORT BY:** [ENTER DESIGNATION OF REVIEWING OFFICE]

SUMMARY: [A brief narrative summary of the review, including an overall assessment of the office's compliance, a brief statement of primary findings, and highlights of best practices found or *exceptional* support provided by the review office staff.]

INTRODUCTION: [This report documents the results of a quality assurance review conducted on _____. The review was conducted by _____ and included an evaluation of _____'s implementation of the FAA's contractor and industrial security program. Specific areas evaluated were procurement reviews, contractor employee position risk and sensitivity level designations, procedures for investigative forms review, investigative requirements determinations, escort of uncleared contractor employees, and ITS or IPPS data entry. During the on-site review, FAA representatives of the _____ played an integral role in the review process and provided invaluable support and assistance.]

PURPOSE: [To provide senior management with concise, candid evaluations of policy and program effectiveness and to inform them of conditions or situations which require their attention or intervention. Security from criminal acts and the human factors important to safety are goals in the FAA's 1996 Strategic Plan. Quality assurance reviews support these goals by ensuring compliance with the laws and regulations governing security to minimize the risk of damage to FAA systems, unauthorized disclosure of sensitive and classified information, and the vulnerability of FAA facilities, resources, and personnel to crime and terrorism.]

METHODOLOGY: [This quality assurance review followed procedures established by the quality assurance process contained in FAA Order 1600.72A, Contractor and Industrial Security Program.]

SECTION I. CONTRACTOR SECURITY PROGRAM REVIEW:

1.1. Evaluation Process: [Explain steps taken and information requested for the conduct of the quality assurance review.]

1.2. Findings and Recommendations:

[Identify each primary finding individually, state why it is a finding. Follow each finding with a recommendation for corrective action and identify the office(s) responsible for taking the corrective action.]

Finding #1:**Recommendation:****Finding #2:****Recommendation:****Finding #3:****Recommendation:****1.3. Observations:**

[Identify each observation individually, state why it is an observation. Follow each observation with a recommendation for corrective action and identify the office(s) responsible for taking the corrective action.]

1.4. Best Practices:

[Identify any best business practices found.]

SECTION II, AGENCY IMPACT:

[Identify the impact of findings and observations, i.e., if the situation(s) or condition(s) are not corrected, what would be the impact to the agency? This needs to be specific statements regarding each primary finding and an overall broad statement of the impact on FAA's security posture, if applicable.]

SECTION III, SUGGESTIONS FOR IMPROVEMENT:

[Provide a detailed description of all reviewer suggestions that can strive toward full agency program compliance.]

APPENDIX A. GLOSSARY AND ACRONYMS

Access. The ability to physically enter or pass through an FAA area or facility; or having the physical ability or authority to obtain FAA sensitive unclassified information, materials, and resources; or the ability to obtain FAA sensitive unclassified information by technical means including the ability to read or write information or data electronically stored or processed in a digital format such as on a computer, modem, the Internet, or a local- or wide-area network. When used in conjunction with classified information, access is the ability, authority, or opportunity to obtain knowledge of such information, materials, or resources.

Access Authorization. Certification that a person is currently authorized to have access to classified information.

Advance NAC. An Office of Personnel Management (OPM) product that consists of an itemized list of the National Agency Check (NAC) results of an investigation that is provided in advance of the completion of the investigation.

Automated Information System. An assembly of computer or telecommunications equipment, facilities, personnel, software, and procedures configured for the purpose of communicating, storing, calculating, computing, summarizing, or retrieving data and information with a minimum of human intervention.

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

Background Investigation (BI). An OPM investigation consisting of searches of the OPM's Security and Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation's (FBI) Identification Division, and FBI's Records Management Division; a credit search; personal interviews of the subject and sources; written inquiries; 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.

Background Investigation Requirement (BIR). An automated systems entry code used by the logistics component to determine a contract's security classification; e.g., background investigation required; escort required; classified contract; no security requirement.

Classified Contract. Any contract, purchase order, consulting agreement, lease agreement, interagency agreement, memorandum of agreement, or any other agreement between the FAA and another party or parties that requires the release or disclosure of classified information to the contractor and/or contractor employees in order for them to perform under the contract or provide the services or supplies contracted for.

Classified Information. Official information or material that requires protection in the interest of national security and is labeled or marked for such purpose in accordance with the provisions of Executive Order 12958, Classified National Security Information.

Commercial-Off-the-Shelf (COTS). Commercial-off-the-shelf is a product or service that has been developed for sale, lease or license to the general public and is currently available at a fair market value.

Contract. A legally enforceable binding agreement between two or more persons or parties. For the purposes of this and all related orders, includes, but is not limited to, purchase orders, consulting agreements, lease agreements, interagency agreements, memorandums of agreement, and any other agreement between the FAA and another party or parties.

Contracting Officer. An official who has authority to enter into and/or administer contracts and makes determinations or findings with respect to those contracts on behalf of the FAA.

Contracting Officer's Technical Representative (COTR). An individual designated in writing by a contracting officer to act as a technical representative to facilitate administration of a contract. (Interchangeable with contracting officer's representative (COR).)

Contractor Security. The standards and procedures utilized to determine and document that the use of an individual pursuant to a contract with the Federal Government will promote the efficiency of the service.

Contractor Employee. A person employed as or by a contractor, subcontractor, or consultant to the FAA, or any non-FAA person who performs paid or non-paid work or services for the FAA.

Critical Area Positions. Positions that have a direct impact on communications, automated information systems, safety, security, and/or the National Airspace System (NAS), and/or are located in or have access to sensitive areas and security offices.

Defense Clearance and Investigations Index (DCII). An automated index of digitally stored data of investigations conducted by the Department of Defense (DOD) on military personnel, DOD civilian employees and applicants, and contractors.

Dual Citizen. A citizen of the United States also having citizenship in another country.

Due Process. A process that is established to protect individual rights and liberties which provides the Subject an opportunity to deny, explain or refute any allegations or adverse information used in an investigation.

Escorting. A Federal or other appropriately cleared person or persons accompanying a contractor employee or other specified individual to prevent unauthorized access to FAA facilities, information, and/or resources. The escort must keep the individual(s) requiring escort in plain view at all times and must be constantly aware of the individual's actions.

Facility [as it applies to the Contractor and Industrial Security Program]. Any manned or unmanned building, structure, warehouse, appendage, storage area, utilities, and components, which when related by function and location form an operating entity owned, operated, or controlled by the FAA.

FAA Employee. Any person employed directly by the FAA.

Felony. A conviction of a crime that is punishable by a possible imprisonment of more than one year.

Fingerprint Check. This check consists of searches of the FBI's Identification Division.

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.

Industrial Security. The standards and procedures utilized to determine and document that use of an individual pursuant to a contract with the Federal Government is clearly consistent with the interests of the national security by ensuring protection of classified information in the custody of and/or accessed by U.S. industry.

Information Resources. An assembly of computer or telecommunications equipment, facilities, personnel, software, and procedures configured for the purpose of communicating, storing, calculating, computing, summarizing, or retrieving data and information with a minimum of human intervention.

Limited Background Investigation (LBI). An OPM investigation consisting of searches of the SII, DCII, FBI's Identification Division, and FBI's Records Management Division, a credit search, personal interviews of the 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 of coverage.

Minimum Background Investigation (MBI). An OPM investigation consisting of searches of the SII, DCII, FBI's Identification Division, and FBI's Records Management Division, written inquiries, telephone inquiries to follow up on written inquiries not returned, a credit search, Subject interview, and record searches for a total of 5 years of coverage.

National Agency Check (NAC). An OPM investigation consisting of searches of the SII, DCII, FBI's Identification Division, and FBI's Records Management Division.

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

National Agency Check, Law Enforcement Checks, and Credit (NACLC). An OPM investigation consisting of a NAC, written inquiries, record searches, and a credit check covering specific areas of a person's background during the most recent 5 years.

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.

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

Nexus. A direct or logical connection between a person's conduct and the duties and responsibilities of the position applied for.

Non Immigrant Alien. Any person not a citizen or national of the United States who has been authorized to work in the United States by the Department of Homeland Security.

Operating Office. For the purposes of this and all related orders, an FAA line of business, activity, or organization utilizing the services and/or work of a contractor.

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

Personnel Security (Program). The standards and procedures utilized to determine and document that the employment or retention in employment of an individual with the Federal Government 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 adjudicates personnel security investigations for suitability and/or security for employment in or under contract to the Federal Government.

Personnel Security Investigation. An investigation, also referred to as a background investigation, conducted to aid in determining an applicant or employee's suitability for employment, qualifications for a position, or loyalty to the United States.

Personnel Security Manager. A specifically appointed individual within an agency 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 Level. The designation of a position based on its relative importance to the national security.

Proprietary Information. Confidential commercial or financial information.

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.

Quality Assurance. A system that provides for a means of continuous review and oversight of a program/process to ensure (1) compliance with applicable laws and regulations; (2) the products and services of the program/process satisfy the mission of the program; and (3) the products and services are dependable and reliable.

Real Estate Contracting Officer (RECO). An official who has authority to enter into and/or administer real estate contracts and makes determinations or findings with respect to those contracts on behalf of the FAA.

Reimbursable Suitability Investigation (RSI). An OPM investigation conducted to resolve a suitability issue raised in a previous investigation.

Resources (as it applies to the Contractor and Industrial Security Program). FAA physical plants, sensitive equipment, information databases including hardware and software, and manual records pertaining to agency mission or personnel.

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

Security Adjudication. The determination as to whether the employment or continued employment of an individual, and the person's access to classified information, if

necessary, can reasonably be expected to be clearly consistent with the interests of national security.

Security Clearance. Authorization for access to classified national security information at a specific level.

Security and Suitability Investigations Index (SII). An electronically stored information in digital format created and maintained by OPM consisting of investigations conducted by OPM and certain other agencies as reported to OPM.

Sensitive Security Information (SSI). SSI is a designation unique to DOT and its operating administrations and to the Department of Homeland Security. It applies to information that is obtained or developed while conducting *security activities*, including research and development activities.

Sensitive Unclassified Information (SUI). Unclassified information – *in any form including print, electronic, visual, or aural* – that must be protected from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under the Freedom of Information Act.

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

Single Scope Background Investigation (SSBI). An OPM investigation consisting of a 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.

Single Scope Background Investigation Periodic Reinvestigation – (SSBI-PR). An OPM investigation conducted to update an SSBI that consists of personal interviews of the subject and sources, searches of the SII, DCII, FBI's Identification Division, and FBI's Records Management Division, a credit search, and written inquiries and record searches covering specific areas of a person's background during the most recent 5 years.

Special Agreement Check (SAC). An OPM limited investigation (or a series of checks) conducted on a Subject, done only through special agreement between OPM and an agency.

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 job with appropriate efficiency and effectiveness.

Suitability Adjudication. The process of determining a person's suitability for employment with, by, or for the Federal Government or to work or provide services as a contractor to the Federal Government.

ACRONYMS

| | |
|---------------|---|
| AHS | Office of Field Operations |
| AIN | Office of Internal Security and Investigations |
| AIS | Automated Information Systems |
| ANACI | Access National Agency Check with Inquiries |
| ASH | Assistant Administrator for Security & Hazardous Materials |
| BI | Background Investigation |
| CFR | Code of Federal Regulations |
| CO | Contracting Officer |
| COTR | Contracting Officer's Technical Representative |
| CSF | Contractor Security File |
| DCII | Defense Clearance and Investigations Index |
| DHS | Department of Homeland Security |
| DOD | Department of Defense |
| DOJ | Department of Justice |
| DOT | Department of Transportation |
| DSS | Defense Security Service |
| EO | Executive Order |
| FBI | Federal Bureau of Investigation |
| FEDEX | Federal Express |
| GSA | General Services Agency |
| HSPD | Homeland Security Presidential Directive |
| ISR | Industrial Security Regulation |
| ITS | Investigations Tracking System |
| LBI | Limited Background Investigation |
| LC | Logistics Component |
| LMS | Logistics Management Specialist |
| MBI | Minimum Background Investigation |
| MOA | Memorandum of Agreement |
| NAC | National Agency Check |
| NACI | National Agency Check with Inquiries |
| NACLC | National Agency Check with Inquiries, Credit, and Law Enforcement |
| NAS | National Airspace System |
| NATO | North Atlantic Treaty Organization |
| NISP | National Industrial Security Program |
| NISPOM | National Industrial Security Program Operating Manual |
| OMB | Office of Management and Budget |
| OO | Operating Office |

| | |
|----------------|---|
| OPF | Office Personnel Folder |
| OPM | Office of Personnel Management |
| OST | Office of the Secretary of Transportation |
| PO | Purchase Order |
| PRI | Periodic Reinvestigation |
| PSF | Personnel Security File |
| PSS | Personnel Security Specialist |
| RECO | Real Estate Contracting Officer |
| ROI | Report of Investigation |
| RSI | Reimbursable Suitability Investigation |
| SAC | Special Agreement Check |
| SFO | Solicitation for Offer |
| SII | Security Investigation Index |
| SIR | Screening Information Request |
| SOW | Statement of Work |
| SSBI | Single Scope Background Investigation |
| SSBI-PR | Periodic Reinvestigation for SSBI |
| SSE | Servicing Security Element |
| UPS | United Parcel Service |
| USC | United States Code |

APPENDIX B. INTERIM SUITABILITY LETTER

Subject: Contractor Interim Suitability
Determination – [Applicant's
Name]

Date:

From: Personnel Security Specialist

Reply to
Attn of:

To: CO/LMS/RECO NAME, Routing Symbol,
& Contract Number (if known)

_____ A preliminary review has been completed and this applicant can start work. This does *not* constitute a security clearance and the applicant is *not* eligible for access to classified national security information. If there are no issues with the applicant's investigation, this interim suitability will serve as final suitability. If there are issues, you will be notified.

_____ The applicant failed to complete all of the required information on the SF-85P. The application has been returned to the contractor for corrections which must be made before interim suitability can be granted.

_____ The applicant failed to submit the investigative forms within the prescribed time frame. This applicant is no longer being considered.

_____ Due to questionable information developed during the preliminary review, the applicant cannot be granted interim suitability. The applicant cannot begin working on the FAA contract. You must make the decision as to whether or not you wish us to continue with the background investigation.

_____ Due to questionable information developed during the background investigation, further investigative review is required. You will be notified when the case is completed.

_____ Due to questionable information during the background investigation, the request for suitability is being denied. The applicant must be removed from the FAA contract.

_____ Due to not meeting the 3-year residency requirement, the request for interim suitability is being denied. You must make the decision as to whether or not you wish us to continue with the background investigation and wait for its completion before a suitability determination can be made. Refer to FAA Order 1600.72A for possible exceptions.

Personnel Security Specialist's Name

APPENDIX C. PREPARATION OF DD FORM 254

1. **General.** This appendix contains instructions for preparation of DD Form 254, "Contract Security Classification Specification," for classified contracts as extracted from the National Industrial Security Program Operating Manual (NISPOM). Although this form is *not* completed by the servicing security element (SSE), he or she must review the information, ensure it is accurate and appropriate, and then initial it. The information provided here is designed to familiarize SSEs with the requirements and their responsibilities regarding DD Form 254.

The DD Form 254 was designed for a User Agency to provide a contractor with the security requirements and classification guidance needed for performance of a classified contract. When properly completed, it will contain information concerning the most common situations that occur in a classified contract. It will have to be adapted as necessary for contracting situations that may not be covered by the form. When a contractor will require access to certain types of classified information, for example Communications Security (COMSEC), North Atlantic Treaty Organization (NATO), Special Access Program, or Intelligence, the program manager, and contracting officer, logistics management specialist, or real estate contracting officer, must obtain assistance from the SSE. SSEs will assist in verifying a contractor's facility clearance and safeguarding capability.

2. **Preparing the DD Form 254.** The following information corresponds to the items on DD Form 254. An explanation and other pertinent information are provided for each item on DD Form 254.

Item 1. Clearance and Safeguarding.

In Item **1a**, insert the highest level of facility clearance required by the contractor for performance of the contract. Use only the words **TOP SECRET, SECRET, or CONFIDENTIAL**. Special caveats such as RESTRICTED DATA, FORMERLY RESTRICTED DATA, COMSEC INFORMATION, etc., are not appropriate in this Item. The contractor must have a valid facility clearance at least as high as the classification indicated in this Item.

In Item **1b**, insert the highest level of safeguarding capability required by the contractor for performance of the contract. The classification level shown in **1b** may not be higher than that shown in **1a**. If the contractor will not possess classified information at the cleared facility in performing the contract, enter "Not Applicable" (N/A) or "None."

| | |
|--------------------------------------|--------------------------------|
| 1. CLEARANCE AND SAFEGUARDING | |
| a. | FACILITY CLEARANCE REQUIRED |
| b. | LEVEL OF SAFEGUARDING REQUIRED |

Item 2. This Specification Is For:

Enter prime contract number in **2a** unless it is a solicitation, in which case, see Item **2c**. If this Form DD 254 is a solicitation, then enter "X" in this block.

Insert "X" for the subcontract number in **2b**. This block is only used by prime contractors for subcontractors.

Insert "X" in **2c** unless this is a solicitation or research and development effort, in which case you should enter an appropriate identification number. Enter the due date if this is a solicitation.

| | |
|--|----------------------|
| 2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i> | |
| a. PRIME CONTRACT NUMBER | |
| b. SUBCONTRACT NUMBER | |
| c. SOLICITATION OR OTHER NUMBER | Due Date (YYMMDD) |

Item 3. This Specification Is:

When the original DD Form 254 is issued, insert “**X**” in **3a** and enter date. The date of the original will appear unchanged on each revised or final DD Form 254 issued there after. Item **3a** applies when a solicitation is issued and when the subcontract is awarded.

When a revised DD Form 254 is issued, insert “**X**” in **3b**, show revision number and enter date of revision. Each time a revision is issued, it shall be given a sequential revision number.

At the end of a contract, a final DD Form 254 must be issued. Insert “**X**” in **3c** and enter the date. If a final DD Form 254 is issued, Item **5** is always marked “**Yes**.”

| | | |
|--|--------------|----------------------|
| 3. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i> | | |
| a. ORIGINAL <i>(Complete date in all cases)</i> | | Due Date (YYMMDD) |
| b. REVISED <i>(Supersedes all previous specs.)</i> | Revision No. | Due Date (YYMMDD) |
| c. FINAL <i>(Complete Item 5 in all cases)</i> | | Due Date (YYMMDD) |

Item 4. Is this a Follow-on Contract?

This Item pertains to follow-on contracts. The contract must be to the same contractor for the same item or service as the preceding contract. When these conditions exist, enter an “**X**” in the “**YES**” box, and enter the preceding contract number in the space provided. This Item authorizes the contractor to transfer classified material received or generated under the preceding contract to the current contract. It is assumed that the contractor will require access to the same information for performance of the follow-on contract as was required for the previous contract.

If this is not a follow-on contract, enter an “**X**” in the “**NO**” box.

| | | | | |
|--|--------------------------|-----|--------------------------|-------------------------------------|
| 4. IS THIS A FOLLOW-ON CONTRACT? | <input type="checkbox"/> | Yes | <input type="checkbox"/> | No. If Yes, complete the following: |
| Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to the follow-on contract. | | | | |

Item 5. Is This A Final DD Form 254?

If a final DD Form 254 is being issued, enter an “X” in the “YES” box, the date of the contractor’s request for retention of classified material and the authorized period of retention in the spaces provided. You are the decision-maker regarding the authority to allow the contractor to retain classified material. Therefore, if you do not want the contractor to retain the classified material enter “No Authorized” in the space provided at the end of the box.

If this is not a final, enter an “X” in the “NO” box.

| | | | | |
|---|--------------------------|-----|--------------------------|-------------------------------------|
| 5. IS THIS A FINAL DD Form 254? | <input type="checkbox"/> | Yes | <input type="checkbox"/> | No. If Yes, complete the following: |
| In response to the contractor’s request dated _____, retention of the identified classified material is authorized for the period of _____. | | | | |

Item 6. Contractor.

Item 6 is used by the FAA when issuing the prime contract.

You must provide the name and address, to include zip code, of the contractor in box 6a.

The SSE will assist in providing the Cage Code (box 6b) and Cognizant Security Office (CSO) data (box 6c). It should be noted that CSO will always be the Director of Industrial Security for DSS who has industrial security jurisdiction over the geographical area in which the contract is located. If the FAA will retain inspection rights (SAP/SCI contracts), then the FAA will be identified in box 15 as discussed below. Conduct of inspections by the FAA does not affect the CSO designation and does not relieve the FAA of the responsibility of providing a copy of the DD Form 254 to the CSO.

| 6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i> | | |
|--|--------------|---|
| a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip Code) |
| | | |

Item 7. Subcontractor.

This is the responsibility of the prime contractor and must be completed by the prime contractor when a subcontract is issued.

However, project managers and/or COs/LMSs/RECOs will be notified of the use of a subcontractor when the prime contractor identifies them in Item 17d. It is recommended that specific security guidance be provided as discussed in Item 13. Specifically, prime contractors are not authorized to use subcontractors without the express approval of the FAA.

| 7. CONTRACTOR | | |
|--------------------------------|--------------|---|
| a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip Code) |
| | | |

Item 8. Actual Performance.

This Item will be completed when the contractor's work is performed at a location other than the contractor's prime location. For example, the contract may be let to a company based in Chicago but the work will be performed in El Paso.

The information for Items **8a, b,** and **c,** however, is completed as discussed for Item **6** on the DD Form 254.

| 8. ACTUAL PERFORMANCE | | |
|--------------------------------|--------------|---|
| a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip Code) |
| | | |

Item 9. General Identification Of This Procurement.

Enter a short, concise, and *unclassified* description of the procurement action in this block. This may be Services, Study, Research, Development, Production, etc. For example, "information systems security assessment services."

If there is doubt regarding the classification of the description, contact the SSE for assistance and treat the information as classified until a determination is made.

| |
|--|
| 9. GENERAL IDENTIFICATION OF THIS PROCUREMENT |
| |

Item 10. This Contract Will Require Access To:

These items are marked "YES" or "NO" according to the requirements of each contract. An explanation of each item follows this illustration.

| 10. THIS CONTRACT WILL REQUIRE ACCESS TO: | YES | NO |
|--|-----|----|
| a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION | | |
| b. RESTRICTED AREA | | |
| c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION | | |
| d. FORMERLY RESTRICTED DATA | | |
| e. INTELLIGENCE INFORMATION | | |
| (1) Sensitive Compartmented Information (SCI) | | |
| (2) Non-SCI | | |
| f. SPECIAL ACCESS INFORMATION | | |
| g. NATO INFORMATION | | |
| h. FOREIGN GOVERNMENT INFORMATION | | |
| i. LIMITED DISSEMINATION INFORMATION | | |
| j. FOR OFFICIAL USE ONLY INFORMATION | | |
| k. OTHER (Specify) | | |

Box 10.a. Communications Security (COMSEC) Information. If the contractor will require access to any COMSEC information, enter an "X" in the "YES" box. COMSEC information includes accountable or non-accountable COMSEC information and controlled cryptographic items (CCI). If

accountable COMSEC information is involved, the contractor must have a COMSEC account and Item **11h** (below) would be marked “YES.” An “X” in the “YES” box imposes the requirements of the COMSEC Supplement to the NISPOM on the contractor for safeguarding the COMSEC information. Access to any COMSEC information requires special briefings at the contractor facility. Access to classified COMSEC information requires a final US Government clearance at the appropriate level.

Boxes 10.b., c, and d. It is highly unlikely these boxes will ever be marked “YES,” since this is information which is classified and controlled under the Atomic Energy Act of 1954, or CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI), is required.

Box 10.e.(1 and 2) Intelligence Information.

Intelligence Information is under the jurisdiction and control of the Director of Central Intelligence (DCI) and is circulated within the Intelligence Community. If Intelligence Information is involved in an FAA contract, the SSE is responsible for ensuring that the additional security requirements outlined in various DCI Directives are incorporated in the guidance provided to the contractor and are tailored to the performance requirements of the contract. It should be noted that the contractor is responsible for incorporating the additional security requirements in any subcontract document itself or in Item **13**. The CSO does not conduct security inspections for SENSITIVE COMPARTMENTED INFORMATION (SCI) but is responsible for inspections of non-SCI in the possession of a subcontractor. If access to SCI is required, Item **10e(1)** and Items **14** and **15** would always be marked “YES.”

If access to non-SCI is required, Item 10e(2) would be marked “YES,” Item **14** would be marked “YES,” and Item **15** would be marked “NO.”

In some cases, **10e(1)** and **(2)** will both be marked “YES,” Item **14** marked “YES,” and Item **15** completed as appropriate. Access to intelligence information requires a final U.S. Government clearance at the appropriate level.

Box 10.f. Special Access Program (SAP) Information. Should the FAA implement a SAP, it would have to be approved by the Administrator with security oversight provided directly by Associate Administrator for Security and Hazardous Materials, ASH-1. When SAP information is involved, the FAA is responsible for providing the contractor with the additional requirements needed to ensure adequate protection of the information. The contractor is responsible for incorporating the additional security requirements in the subcontract document itself or in Item **13**. When this Item is marked “YES,” Item **14** would be marked “YES,” and Item **15** should be completed as appropriate. (Some SAPs qualify as carve-outs, but not all.) Access to SAP information requires a final US Government clearance at the appropriate level and special briefings.

Box 10.g. NATO Information. This means information/documents belonging, to and circulated by, NATO. Access to NATO information requires a final U.S. Government clearance at the appropriate level and special briefings.

Box 10.h. Foreign Government Information. This Item includes any foreign government information except NATO. Access to classified foreign government information requires a final US Government clearance at the appropriate level.

Box 10.i. Limited Dissemination Information (LIMDIS). This means restrictive controls established by an original classification authority to emphasize need-to-know protective measures available within the regular security system. Contracts which involve LIMDIS controls do not qualify for carve-out status. When this Item is marked “YES,” Item **14** would be marked “YES,” and Item **15** marked “NO.”

10.j. For Official Use Only Information (FOUO). This Item is applicable only in a classified contract that interfaces with DOD activities, missions or support. When this Item is marked “YES,” the FAA is responsible for providing the contractor with the safeguards necessary for protection of the

information. The contractor is responsible for incorporating those safeguards in the subcontract. Should there be a requirement for FOUO, SSEs will provide special guidance as required.

Box 10.k. Other. Use this Item for any other information not included in **10a** through **j**. Specify the type of information and include any additional remarks needed in Item **13**.

Item 11. In Performing This Contract, The Contractor Will:

These items are marked “**YES**” or “**NO**” according to the requirements of each contract. An explanation of each item follows this illustration.

| 11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL | YES | NO |
|--|------------|-----------|
| a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT FACILITY | | |
| b. RECEIVE CLASSIFIED DOCUMENTS ONLY | | |
| c. RECEIVE AND GENERATE CLASSIFIED MATERIAL | | |
| d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE | | |
| e. PERFORM SERVICES ONLY | | |
| f. HAVE ACCESS TO US CLASSIFIED INFORMATION OUTSIDE THE US, PUERTO RICO, US POSSESSIONS, AND TRUST TERRITORIES | | |
| g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER | | |
| h. REQUIRE A COMSEC ACCOUNT | | |
| i. HAVE TEMPEST REQUIREMENTS | | |
| j. HAVE OPERATION SECURITY (OPSEC) REQUIREMENTS | | |
| k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE | | |
| l. OTHER (Specify) | | |

Box 11.a. Have access to classified information only at another contractor's facility or a Government Activity. Note the word *only*. This means that there will be no access to classified information at the contractor's facility. The contractor will not be required to have any safeguarding capability at its facility and Item **11b** would be marked “**N/A**” or “**None**.” If the “**YES**” box is marked for this Item, add the following annotation in Item **13**: “**Contract performance is restricted to [enter name and address of contractor facility(ies) or government activity].**”

Box 11.b. Receive classified documents only. Note the word *only*. This means the contractor will receive classified documents but is not expected to generate classified information that will require detailed guidance. The classification markings shown on the documents received will provide the classification guidance necessary. Add the following annotation in Item **13**: “**Any classified information generated in performance of this subcontract shall be classified according to the markings shown on the source material.**”

Box 11.c. Receive and generate classified material. This means the contractor is expected to receive and generate classified material (documents and/or hardware) and will require detailed security classification guidance for performance of the subcontract. If the “**YES**” box is marked for this item, detailed security classification guidance must be provided to the contractor. The guidance may be included

in Item **13**, attached to the DD Form 254, forwarded under separate cover, or included in the subcontract document itself. Statements, as appropriate, shall be included in Item **13** to direct the contractor to the guidance for the contract.

Box 11.d. Fabricate, modify, or store classified hardware. If “YES,” include as much information as possible (additional information can be added in Item **13**) to indicate if Restricted or Closed Areas will be required. How much hardware is involved? How large? If more than two cubic feet of storage is required, request the SSE contact the CSO to verify storage capability exists at the contract facility.

Box 11.e. Perform services only.

“YES” in this Item will require a statement in Item **13** to explain the services and to provide appropriate guidance. Sample statements are given below. For service-type contracts not covered, add any appropriate statement in Item **13** that explains why the contract is a classified contract and provide guidance as necessary to ensure protection of the classified information.

If Graphic Arts Services, add the following statement in Item **13**: **“Reproduction services only. Classification markings on the material to be reproduced will provide the classification guidance necessary for performance of this subcontract.”**

If Engineering Services, add the following statement in Item **13**: **“Contract is for engineering services. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this subcontract.”**

If Equipment Maintenance Services, add the following statement in Item **13**: **“Contract is for equipment maintenance services on equipment which process classified information. Actual knowledge, generation, or production of classified information is not required for performance of this contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded by escorting personnel. Any classification guidance needed will be provided by the Service.”**

If Guard Services, add the following statement in Item **13**: **“Contract is for Guard services. Cleared personnel are required by the NISPOM to provide supplemental controls.”**

Box 11.f. Have access to US classified information outside the US, Puerto Rico, US Possessions and Trust Territories. If “YES,” indicate city and country of overseas performance in Item **13**. Item **14** may be “YES” and should be completed if appropriate. A copy of the DD Form 254 must be provided to the US activity responsible for overseas security administration.

Box 11.g. Be authorized to use the services of Defense Technical Information Center (DTIC) or other secondary distribution center. “YES” in this Item means the contractor is authorized to use the services of DTIC and will require any subcontractor to prepare and process a DD Form 1540 and DD Form 1541 through the prime contractor.

Box 11.h. Require a COMSEC account. If accountable COMSEC information will be provided to the contractor, enter an “X” in the “YES” box. If non-accountable COMSEC information is involved, enter an “X” in the “NO” box.

Box 11.i. Have TEMPEST requirements. Prior approval of the SSE is required before imposing TEMPEST requirements on a contractor. TEMPEST requirements are in addition to the requirements of the NISPOM. If “YES” in this Item, Item **14** must also be “YES” and the pertinent contract clauses identified or appropriate information added in Item **13**.

Box 11.j. Have Operations Security (OPSEC) requirements. Prior approval of the SSE is required before imposing any OPSEC requirements on a contractor. OPSEC requirements are in addition to the requirements of the NISPOM. If “YES” in this Item, Item 14 must also be “YES” and the pertinent subcontract clauses identified or appropriate information added in Item 13.

Box 11.k. Be authorized to use the Defense Courier Service (DCS). This Item authorizes the contractor to use the services of DCS. Only certain classified information qualifies for shipment by DCS. It is the responsibility of the Service to comply with DCS policy for qualified shipments when approving use of the services of DCS.

Box 11.l. Other (Specify). Use this Item to add any additional performance requirements not covered above. The performance requirements listed above are included as part of the form because they are common situations that occur in classified contracts. If they are not applicable to the contract requirements, indicate “NO” for all of them, add in Item 11.l: “See Item 13,” and include appropriate statements in Item 13.

Item 12. Public Release.

The contractor is responsible for obtaining the approval of the prime contractor and the Service prior to release of any information under the contract, except for certain types of information authorized by the NISPOM. Complete this Item as necessary to direct the contractor to the SSE should they desire coordination and approval for public releases.

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by this Industrial Security Manual or unless it has been approved for public release by appropriate US Government authority. Proposed public releases shall be submitted for approval prior to release

☐

Direct

☐

Through (*Specify*)

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.

* In the case of non-DOD Agencies, requests for disclosure shall be submitted to that agency.

Item 13. Security Guidance. This is the most important part of the entire DD Form 254.

In completing this Item, ask yourself the following questions:

- A. What classified information will the contractor need in the performance of this contract?
- B. Guidance.
 - 1. What guidance will the contractor need to protect the classified information?
 - 2. Is the guidance in the prime contract DD Form 254 adequate?
 - 3. Are there other guides which may provide guidance that will assist the contractor?

C. Hardware.

1. Will classified hardware be furnished to or generated by the contractor?
2. What information makes the hardware classified?
3. Will hardware being generated require classification?
4. At what stage in its production does it become classified?
5. What unique characteristics are involved that need protection?
6. Are there design features which require protection?
7. What technical information requires protection?
8. What breakthroughs would be significant if achieved in an R&D effort?
9. Are there some performance limitations that require protection?

D. These are merely some of the questions that should be asked when preparing guidance for a contract. Put yourself in the contractor's place and try to determine what guidance will be needed to properly protect the classified information that will be furnished or generated under the contract.

E. Use this Item to identify applicable guides, to provide narrative guidance which identifies the specific types of information to be classified, to provide appropriate downgrading or declassification instructions, to provide any special instructions, explanations, comments or statements required for information or to clarify any other items identified in the DD Form 254. Each contract is unique in its performance requirements. Don't try to follow a format or provide all the guidance in this Item. Give reasons for the classification. Write the guidance in plain English. Use additional pages as necessary to expand or explain the guidance.

F. The DD Form 254, with its attachments and incorporated references, is the only authorized means for providing security classification guidance to a contractor. It should be written as specifically as possible and it should include only that information that pertains to the contract for which it is issued. It should not contain references to internal directives or instructions. If such documents provide guidance applicable to the contract, the pertinent portions should be extracted and provided as attachments. Any and all documents referenced and/or cited in Item 13 should be provided to the contractor, either as attachments or forwarded under separate cover if they are classified. The requirements of the NISPOM should not be extracted and included in a DD Form 254. The NISPOM provides safeguarding requirements and procedures for classified information, not security classification guidance. Security classification guidance provides detailed information that relates what information requires classification, what level of classification to assign, and the downgrading or declassification instructions that apply to the information or material generated by the subcontractor in the performance of the contract.

G. It is a difficult task to prepare security guidance that covers all of the performance requirements of a classified contract. It is an even more difficult task to prepare guidance that can be understood and implemented by the contractor. Encourage the contractor to assist in the preparation of the guidance, if at all possible, and to provide comments and/or recommendations for changes in the guidance that has been provided. Only through effective communication with the contractor can you achieve guidance that is understandable and ensure the proper classification and protection of the information generated in the performance of the contract.

13. Security Guidance. The security classification guidance needed for the classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Item 14. Additional Security Requirements.

This Item applies any time security requirements are imposed on a contractor that are in addition to the requirements of the NISPOM. “YES in this Item requires the project manager, COTR, or the SSE to incorporate the additional requirements in the contract document itself or to incorporate the additional requirements by statements or reference in Item 13. Attendant costs incurred due to additional security requirements are subject to negotiation by, and reimbursement to, the contractor and are the responsibility of the FAA activity that imposed the additional requirements in the contract. Approval of the SSE is required prior to imposing additional security requirements on a contractor. A copy of the additional security requirements shall be provided to the CSO.

| | | |
|--|-----|----|
| 14. Additional Security Requirements. Requirements, in addition to ISM requirements, are established for this contract. <i>(If YES, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)</i> | Yes | No |
| | | |

Item 15. Inspections.

This Item applies when the CSO is relieved of inspection responsibility in whole or in part. “YES” in this Item requires the SSE to provide information on the specific areas carved-out and to conduct the inspections. A copy of the DD Form 254 must be provided to the appropriate CSO.

When access to SCI is required (Item 10e(1) is marked “YES”), the following statement shall be added in this Item: “**The [FAA or appropriate Agency or Military Department Senior Intelligence Officer] has exclusive security responsibility for all SCI classified material released or developed under this contract and held within the contractor’s SCIF. DSS is relieved of security inspection responsibility for all such material but retains responsibility for all non-SCI classified material released to or developed under this subcontract and held within the contractor’s SCIF.**”

| | | |
|--|-----|----|
| 15. INSPECTIONS Elements of this contract are outside the inspection responsibility of the cognizant security office. <i>(If YES, explain and identify specific areas or elements carved out and the activity responsible for inspection. Use Item 13 if additional space is needed.)</i> | Yes | No |
| | | |

Item 16. Certification and Signature.

Item **16** shall contain the name, title, telephone number, address, and signature of a designated FAA employee certifying that the security requirements are complete and adequate for performance of the classified contract.

| | | |
|--|----------|----------------------------------|
| 16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below. | | |
| a. TYPED NAME OF CERTIFYING OFFICIAL | b. TITLE | c. TELEPHONE (Include Area Code) |
| d. ADDRESS (Include Zip Code) | | |
| e. SIGNATURE | | |

Item 17. Required Distribution.

The DD Form 254 is a contractual document and should be distributed with the contract document to all addressees. It is important that the DD Form 254 be distributed, as a minimum, to those shown in this Item. Other agencies or organizations may be added as necessary.

| | |
|-----------------------------------|--|
| 17. REQUIRED DISTRIBUTION: | |
| <input type="checkbox"/> | a. CONTRACTOR |
| <input type="checkbox"/> | b. SUBCONTRACTOR |
| <input type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input type="checkbox"/> | d. US ACTIVITY RESPONSIBLE FOR OVERSEASE SECURITY ADMINISTRATION |
| <input type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input type="checkbox"/> | f. OTHERS AS NECESSARY |

APPENDIX D. OF-306, DECLARATION FOR FEDERAL EMPLOYMENT**Declaration for Federal Employment**Form Approved
OMB No. 3206-0182**Instructions**

The information collected on this form is used to determine your acceptability for Federal and Federal contract employment and your enrollment status in the Government's Life Insurance program. You may be asked to complete this form at any time during the hiring process. Follow instructions that the agency provides. If you are selected, before you are appointed you will be asked to update your responses on this form and on other materials submitted during the application process and then to reconfirm that your answers are true.

All your answers must be truthful and complete. A false statement on any part of this declaration or attached forms or sheets may be grounds for not hiring you, or for firing you after you begin work. Also, you may be punished by a fine or imprisonment (U.S. Code, title 18, section 1001).

Either type your responses on this form or print clearly in dark ink. If you need additional space, attach letter-size sheets (8.5" X 11"). Include your name, Social Security Number, and form number on each sheet. We recommend that you keep a photocopy of your completed form for your records.

Privacy Act Statement

The Office of Personnel Management is authorized to request this information under sections 1302, 5801, 3304, 3328, and 5716 of title 5, U. S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations.

Your Social Security Number (SSN) is needed to keep our records accurate, because other people may have the same name and birth date. Public Law 104-134 (April 26, 1986) asks Federal agencies to use this number to help identify individuals in agency records. Giving us your SSN or any other information is voluntary. However, if you do not give us your SSN or any other information requested, we cannot process your application. Incomplete addresses and ZIP Codes may also slow processing.

ROUTINE USES: Any disclosure of this record or information in this record is in accordance with routine uses found in System Notice OPM/GOVT-1, General Personnel Records. This system allows disclosure of information for: training facilities; organizations deciding claims for retirement, insurance, unemployment, or health benefits; officials in litigation or administrative proceedings where the Government is a party; law enforcement agencies concerning a violation of law or regulation; Federal agencies for statistical reports and studies; officials of labor organizations recognized by law in connection with representation of employees; Federal agencies or other sources requesting information for Federal agencies in connection with hiring or retaining, security clearance, security or suitability investigations, classifying jobs, contracting, or issuing licenses, grants, or other benefits; public and private organizations, including news media, which grant or publicize employee recognitions and awards; the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, the Federal Labor Relations Authority, the National Archives and Records Administration, and Congressional offices in connection with their official functions; prospective non-Federal employers concerning tenure of employment, civil service status, length of service, and the date and nature of action for separation as shown on the SF 50 (or authorized exception) of a specifically identified individual; requesting organizations or individuals concerning the home address and other relevant information on those who might have contracted an illness or been exposed to a health hazard; authorized Federal and non-Federal agencies for use in computer matching; spouses or dependent children asking whether the employee has changed from a self-and-family to a self-only health benefits enrollment; individuals working on a contract, service, grant, cooperative agreement, or job for the Federal government; non-agency members of an agency's performance or other panel; and agency-appointed representatives of employees concerning information issued to the employees about fitness-for-duty or agency-filed disability retirement procedures.

Public Burden Statement

Public burden reporting for this collection of information is estimated to vary from 5 to 30 minutes with an average of 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden, to the U.S. Office of Personnel Management, Reports and Forms Manager (3206-0182), Washington, DC 20415-7500. The OMB number, 3206-0182, is valid. OPM may not collect this information, and you are not required to respond, unless this number is displayed.

U.S. Office of Personnel Management
5 U.S.C. 1302, 5901, 3304, 3328 & 5716

NSN 7540-01-016-7776

Optional Form 306
Revised January 2001
Previous edition obsolete for collection

Declaration for Federal Employment

Form Approved
GSA GEN. REG. NO. 27

GENERAL INFORMATION

| | |
|---|---|
| 1. FULL NAME (First, middle, last) # | 5. SOCIAL SECURITY NUMBER # |
| 3. PLACE OF BIRTH (include city and state or country) # | 4. DATE OF BIRTH (MM/DD/YYYY) # |
| 6. OTHER NAMES EVER USED (For example, maiden name, nicknames, etc.) # | 2. PHONE NUMBERS (include home, office) Day # Night # |

Selective Service Registration

If you are a male born after December 31, 1952, and are at least 18 years of age, civil service employment law (5 U.S.C. 552a) requires that you must register with the Selective Service System, unless you meet certain exemptions.

- 2a. Are you a male born after December 31, 1952? ☐ YES ☐ NO If "NO" skip 7b and 7c. If "YES" go to 7b.
- 7b. Have you registered with the Selective Service System? ☐ YES ☐ NO If "NO" go to 7c.
- 7c. If "NO," describe your reason(s) in item #19.

Military Service

8. Have you ever served in the United States military? ☐ YES Provide information below ☐ NO
If you answered "YES," list the branch, dates, and type of discharge for all active duty.
If your only active duty was training in the Reserves or National Guard, answer "NO."

| Branch | Dates | Type of Discharge |
|--------|-------|-------------------|
| | | |
| | | |
| | | |

Background Information

For all questions, provide all additional requested information under item 16 or in attached sheets. The circumstances of each event you list will be considered. However, in most cases you can still be considered for Federal jobs.

For questions 9, 10, and 11, your answers should include convictions resulting from a plea of guilty or nolo contendere (no contest), but omit (1) traffic fines of \$500 or less, (2) any violation of law committed before your 18th birthday, (3) any violation of law committed before your 18th birthday if finally decided in juvenile court or under a Youth Offender law, (4) any conviction set aside under the Federal Youth Corrections Act or similar state law, and (5) any conviction for which the record was expunged under Federal or state law.

- | | | |
|---|------------------------------|-----------------------------|
| 9. During the last 10 years, have you been convicted, been imprisoned, been on probation, or been on parole? (Include felonies, misdemeanors or explosive violations, misdemeanors, and all other offenses.) If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved. | YES <input type="checkbox"/> | NO <input type="checkbox"/> |
| 10. Have you been convicted by a military court-martial in the past 10 years? If no military service, answer "NO." If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved. | YES <input type="checkbox"/> | NO <input type="checkbox"/> |
| 11. Are you now under charges for any violation of law? If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved. | YES <input type="checkbox"/> | NO <input type="checkbox"/> |
| 12. During the last 5 years, have you been fired from any job for any reason, did you quit after being told that you would be fired, did you leave any job by mutual agreement because of specific problems, or were you discharged from Federal employment by the Office of Personnel Management or any other Federal agency? If "YES," use item 16 to provide the date, an explanation of the problem, reason for leaving, and the employer's name and address. | YES <input type="checkbox"/> | NO <input type="checkbox"/> |
| 13. Are you delinquent on any Federal debt? (Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) If "YES," use item 16 to provide the type, origin, and amount of the delinquency or default, and steps that you are taking to correct the debt or repay the debt. | YES <input type="checkbox"/> | NO <input type="checkbox"/> |

U.S. Office of Personnel Management

OMB 7540-004-0725

Standard Form 504
Revised January 2013
Prohibit all other reproduction and circulation

5010-104-004-004-004-004

Declaration for Federal Employment

Form Approved
OMB No. 3206-2102

Additional Questions

14. Do any of your relatives work for the agency or government organization to which you are submitting this form? (Include: father, mother, husband, wife, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepson, stepdaughter, stepbrother, step sister, half brother, and half sister.) If "YES," use Item 16 to provide the relative's name, relationship, and the department, agency, or branch of the Armed Forces for which your relative works.
- YES ☐ NO ☐
15. Do you receive, or have you ever applied for, retirement pay, pension, or other retired pay based on military, Federal civilian, or District of Columbia Government service?
- YES ☐ NO ☐

Continuation Space / Agency Optional Questions

16. Provide details requested in Items 7 through 15 and 18c in the space below or on attached sheets. Be sure to identify attached sheets with your name, Social Security Number, and Item number, and to include ZIP Codes in all addresses. If any questions are printed below, please answer as instructed (these questions are specific to your position and your agency is authorized to ask them).

Certifications / Additional Questions

APPLICANT: If you are applying for a position and have not yet been selected, carefully review your answers on this form and any attached sheets. When this form and all attached materials are accurate, read Item 17, and complete 17a.

APPOINTEE: If you are being appointed, carefully review your answers on this form and any attached sheets, including any other application materials that your agency has attached to this form. If any information requires correction to be accurate as of the date you are signing, make changes on this form or the attachments and/or provide updated information on additional sheets, initialing and dating all changes and additions. When this form and all attached materials are accurate, read Item 17, complete 17b, read 18, and answer 18a, 18b, and 18c as appropriate.

17. I certify that, to the best of my knowledge and belief, all of the information on and attached to this Declaration for Federal Employment, including any attached application materials, is true, correct, complete, and made in good faith. I understand that a false or fraudulent answer to any question or item on any part of this declaration or its attachments may be grounds for not hiring me, or for firing me after I begin work, and may be punishable by fine or imprisonment. I understand that any information I give may be investigated for purposes of determining eligibility for Federal employment as allowed by law or Presidential order. I consent to the release of information about my ability and fitness for Federal employment by employers, schools, law enforcement agencies, and other individuals and organizations to investigators, personnel specialists, and other authorized employees or representatives of the Federal Government. I understand that for financial or medical institutions, medical institutions, hospitals, health care professionals, and some other sources of information, a separate specific release may be needed, and I may be contacted for such a release at a later date.

- 17a. Applicant's Signature: _____ Date: _____
- (Sign in ink)
- 17b. Appointee's Signature: _____ Date: _____
- (Sign in ink)
- Appointing Officer:
Enter Date of Appointment in Connection
MM / DD / YYYY

18. Appointee (Only respond if you have been employed by the Federal Government before): Your elections of life insurance during previous Federal employment may affect your eligibility for life insurance during your new appointment. These questions are asked to help your personnel office make a correct determination.

- 18a. When did you leave your last Federal job? DATE: MM / DD / YYYY
- 18b. When you worked for the Federal Government the last time, did you waive Basic Life Insurance or any type of optional life insurance?
- YES ☐ NO ☐ Do Not Know ☐
- 18c. If you answered "YES" to Item 18b, did you later cancel the waiver(s)? If your answer to Item 18b is "NO," use Item 16 to identify the type(s) of insurance for which waivers were not canceled.
- YES ☐ NO ☐ Do Not Know ☐

**APPENDIX E. DOT FORM 1631, DISCLOSURE AND AUTHORIZATION
PERTAINING TO CONSUMER REPORTS PURSUANT
TO THE FAIR CREDIT REPORTING ACT**

UNITED STATES DEPARTMENT OF TRANSPORTATION

Disclosure and Authorization Pertaining to Consumer Reports
Pursuant to the Fair Credit Reporting Act

This is a release for the U.S. Department of Transportation to obtain one or more consumer/credit reports about you in connection with your application for employment or in the course of your employment with **the Federal Aviation Administration.**

One or more reports may be obtained for employment purposes, and used for evaluating your fitness for employment, promotion, reassignment, retention, or access to classified information.

I, _____, hereby authorize the U.S. Department of Transportation to obtain such report(s) from any consumer/credit reporting agency for employment purposes.

Signature

Date

Social Security Number

Current Organization Assigned

PRIVACY ACT STATEMENT

PURPOSE: The U.S. Government conducts background investigation and reinvestigations to establish that applicants or incumbents employed by the Government or working for Government under contract, are suitable for The Job. Information from this form is used primarily as the basis for this investigation. Complete this form only after a condition of employment has been made.

AUTHORITY: Depending upon the purpose of your investigation, the U.S. Government is authorized to ask for this information under Executive Order 10450, 10865, 1233, 12968: Sections 3301 and 9101 of Title 5, U.S. Code of Federal Regulations; sections 2165 and 2201 of Title 42, U.S. Code of Federal Regulations; sections 781 to 887 of Title 50, U.S. Code of Federal Regulations and parts 732 and 736 of Title 5, Code of Federal Regulations. Your Social Security Number is needed to keep records accurate because other people may have the same name and birth date. Executive Order 9397 also asks Federal Agencies to use this number to help identify individuals in agency records.

VOLUNTARY NATURE OF DISCLOSURE: Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or security clearance prospects.

DISCLOSURE OF INFORMATION: The information you give us for the purpose of investigating you for employment or a security clearance, we will protect it from unauthorized disclosure. The collection, maintenance, and disclosure of background investigation information is governed by the Privacy Act. The U.S. Department of Transportation has published notices in the Federal Register describing the systems of records in which your records will be maintained. You may obtain copies of the relevant notices from the person who gave you this form. The information on this form and information we collect during an investigation may be disclosed without your consent by the Privacy Act (5 USC 552a(b)) and as follows:

1. To the Department of Justice when: a) the Agency or any component thereof; or b) any employee of the Agency in his or her official capacity, or c) any employee of the Agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or d) the U.S. Government, is a party to litigation or has interest in such litigation, and by careful review, the Agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records.
2. To a court or adjudicative body in a proceeding when: a) the Agency or any component thereof; or b) any employee of the Agency in his or her official capacity; or c) any employee of the Agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or d) the U.S. Government, is a party to litigation or has interest in such litigation, and by careful review, the Agency determines that the records are both relevant and necessary to the litigation and the use of such records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records.
3. When a record on its face, or in conjunction with other records, indicates a violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general stance, particular program stance, regulation, rule, or issued pursuant thereto, the relevant records may be disclosed to the appropriate Federal, foreign, State, local, tribal, or other public authority responsible for enforcement, investigating or prosecuting such violation or charged with enforcing or implementing the stance, rule, regulation, or order.
4. To any source or potential source from which information is requested in the course of an investigation concerning the hiring or retention of an employee or other personnel action, or the issuing or retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.
5. To a Federal, foreign, state, local, tribal, or other public authority the fact that this system of records contains information relevant to the retention of an employee, or the retention of a security clearance, contract, grant, license, or other benefits. The other Agency or licensing organization may then make a request supported by written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the Agency or to another Federal Agency for criminal, civil, administrative, personnel, or regulatory action.
6. To contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to this record for which they have been engaged. Such recipients shall be required to comply with the Privacy Act of 1974, as amended.
7. To the new media or general public, factual information the disclosures of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy.
8. To Federal, State or local Agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign Governments, in order to enable an intelligence Agency to carry out its responsibilities under the Nation Security Act of 1947, as amended, the CIA Act of 1949, as amended. Executive Order 12333 or any successor order, applicable to National Security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.
9. To a Member of Congress or a Congressional staff member in response to an inquiry of a Congressional office made at the written request of the constituent about whom the record is maintained.
10. To the National Archives and Records Administration for records management inspections conducted under 44 USC 2904 and 2906.
11. To the office of Management and Budget when necessary to the review of private relief legislation.

**APPENDIX F. FAA FORM 1600-74, PRIVACY-ACT
NOTICE – EMPLOYEES/CONTRACTORS**



U.S. Department
of Transportation
**Federal Aviation
Administration**

**PRIVACY ACT NOTICE
AND
EMPLOYEE/CONTRACTOR INFORMATION ACKNOWLEDGEMENT**

Read carefully and initial each section. Initialing and signing this form is only an acknowledgement that you understand your rights under the Privacy Act of 1974 and as an employee or contractor of the Federal Aviation Administration and does not waive any of your rights under the Act or as an employee/contractor. The information requested will be used by officials of the FAA, and others with a need-to-know, in making determinations regarding employment designations, certifications, security clearances, access to classified information and restricted areas, qualifications, suitability, and loyalty. The information may be disclosed to other agencies in accordance with the routine uses printed on the reverse side of this form.

____ I have been informed and I understand this is an **official investigation** involving matters relating to my official duties as a Federal employee/contractor.

____ I have been informed and I understand that authority to collect information requested in this interview is derived from one or more of the following: Title 5, United States Code (U.S.C.), Section 301, Chapter 73 and Subchapters 1 and 11 of Chapter 75; Title 28, U.S.C., Section 1346; Executive Order 10450; and Executive Order 10865.

____ I have been informed and I understand that this is not a criminal investigation and neither the information I provide in response to questions by the investigator or any evidence gained by reason of my answers will be used against me in a criminal proceeding.

____ I have been informed and I understand that, as an **FAA employee**, if I refuse to cooperate and answer questions in this official investigation, my refusal to cooperate can be a basis for disciplinary action against me up to and including removal from Federal service.

____ I have been informed and I understand that, as an **FAA employee**, if I provide information during this official investigation that **I know to be false** at the time I provide the information, my providing false information can be a basis for disciplinary action against me which may result in my removal from Federal service and/or criminal prosecution under Title 18 U.S.C., Section 1001.

____ I have been informed and I understand that, as a **contractor employee**, if I provide information during this official investigation that **I know to be false** at the time I provide the information, my providing false information can be a basis for removal from a contract and/or criminal prosecution under Title 18 U.S.C., Section 1001.

____ I have been informed and I understand that, as a **contractor employee**, I am not required to cooperate with this investigative effort, that if I refuse to cooperate the FAA will evaluate my case on the basis of all available information, and that any investigative findings may cause my access to current and/or future FAA contract work to be denied.

Interviewee's Signature

Date

FAA Special Agent

Date

ROUTINE USE OF RECORDS

The information collected may be disclosed to other agencies and departments of the Federal Government and District of Columbia Government for employment purposes including fitness determinations, security clearances, access determinations, or evaluations of qualifications, suitability and/or loyalty to the United States Government. The information also may be disclosed to representatives of Federal agencies and departments who require access to the file pursuant to an investigation or inquiry conducted under appropriate authority, including investigations completed by the FAA and referred to other agencies for further investigation, prosecution, or administrative action. Moreover, the information may be disclosed to authorized representatives of U.S. air carriers where air safety might be affected. Finally, in the event of an indication of any violation or potential violation of the law, relevant information may be referred to the agency charged with responsibility for investigating or prosecuting the violation or enforcing the regulation.

APPENDIX G. DOT FORM 1681, IDENTIFICATION CARD/CREDENTIAL APPLICATION

| Applicant Data | | | | | |
|---|---|---|--|--|---------------------|
| Application for <input type="checkbox"/> Identification Card or <input type="checkbox"/> Credentials | | | | ID Card Number: <small>(To be completed by Issuer)</small> | |
| Last Name | First Name | Middle Name | Social Security Number | | |
| DOT Administration/Agency | Org. Seg. (OST only) Line of Business (FAA only) | Date/Place of Birth | | <input type="checkbox"/> M <input type="checkbox"/> F Sex (M/F) | |
| ft. in. Height | lbs. Weight | Hair Color | Eye Color | Citizenship | |
| Office Routing Symbol | Office Phone Number(s) | Issuing office use | | | |
| Office e-mail address | | Office (Street) Address | | | |
| ----- Contractors Only ----- | | | | | |
| Contractor Company | | Contract Number & Expiration Date | | Contracting Officer Name and Phone Number (printed) | |
| ----- Reason for Issuance ----- | | | | | |
| <input type="checkbox"/> New ID Card or Credential <input type="checkbox"/> Lost <input type="checkbox"/> Damaged <input type="checkbox"/> Stolen <input type="checkbox"/> Expired <input type="checkbox"/> Other (Specify): | | | | | |
| ----- Application for Credentials Only ----- | | | | | |
| New Credential Request Type: <input type="checkbox"/> Executive <input type="checkbox"/> Official <input type="checkbox"/> Other | | | Position title to appear on the credential | | |
| Credential Justification/Remarks | | | | | |
| ----- Applicant Signature ----- | | | | | |
| <input type="checkbox"/> Permanent <input type="checkbox"/> Contractor <input type="checkbox"/> Temporary <input type="checkbox"/> Other: Employee Type | | | Signature of Applicant | | Date of Application |
| ----- Information below to be filled out by the Sponsor ----- | | | | | |
| Expiration Date of ID Card | | Type of Card: <input type="checkbox"/> Permanent <input type="checkbox"/> Other <input type="checkbox"/> Temporary (Specify): | | | |
| Sponsor's Name & Phone Number (Typed or Printed) | | Routing Symbol | Date | Sponsor's Signature | |
| ----- Identity Verification Information below to be filled out by the Registrar or Trusted Agent (TA) ----- | | | | | |
| <input type="checkbox"/> Applicant's I-9 data has been verified | | <input type="checkbox"/> Applicant has submitted required investigation paperwork (if required) | | <input type="checkbox"/> Applicant has been fingerprinted <input type="checkbox"/> Applicant's picture for ID has been taken | |
| Registrar's/ TA's Name (Typed or Printed) | Routing Symbol | Date | Registrar's/TA's Signature | | |
| ----- Information below to be filled out by the Registrar ----- | | | | | |
| Individual is authorized to be issued the following ID type <input type="checkbox"/> Permanent <input type="checkbox"/> Temporary <input type="checkbox"/> Other: | | | | | |
| Individual has a completed and favorably adjudicated <input type="checkbox"/> NAC <input type="checkbox"/> NACI or higher <input type="checkbox"/> FBI Fingerprint Check <input type="checkbox"/> Other: | | | | | |
| Registrar's Name (Typed or Printed) | Routing Symbol | Date | Registrar's Signature | | |
| ----- Information below to be filled out by the Issuer ----- | | | | | |
| <input type="checkbox"/> DOT F 1681 is correctly completed. <input type="checkbox"/> Applicant's information in the ID system is correct. | | | | | |
| Issuer's Name (Typed or Printed) | Routing Symbol | Date | Issuer's Signature | | |
| ----- Applicant's Acknowledgement Receipt ----- | | | | | |
| Your card contains data that may be used to verify your identity. You must exercise care in handling your card. Do not bend or twist it, expose it to extreme heat or cold. You may keep the card only for as long as you are authorized to enter Federal buildings or have access to Federal information systems. You must return the card when you no longer need it, or upon demand by the government or your employer. You must inform your supervisor, your security representative, and/or the organization that issued your card if it is lost or stolen. You may be asked to wait for a period of time before a replacement card is issued. Please acknowledge receipt of your card and that you accept your responsibilities regarding its use and safeguarding by printing and signing your name below. | | | | | |
| Applicant's Name (Typed or Printed) | | | | Date | |

DOT F 1681 (test – 10/27)

Privacy Act Notice:

The information on this form is requested under authority of Titles 5 and 49, USC; Title 32, CFR; and Title 40 USC 486c. Submission of all data is mandatory in order to receive DOT identification media. The purpose is to provide a ready concentration of employee personal data to facilitate issuance, accountability, and recovery of required identification/credential card(s) which are issued to employees/contractors. The information provided will be used to issue such identification/credential card(s) as may be required to enable the employee or contractor to properly conduct assigned duties. Failure to provide all or any part of the requested data will result in your inability to be properly identified and, therefore, be unable to properly perform all aspects of your assigned official duties.