

### T3.14.1 Security Revised 1/2009

#### A Security

1 Facility/Security Revised 1/2019

2 Information Security and Privacy Revised 10/2022

3 Personnel Security Revised 4/2022

4 Foreign Nationals Revised 4/2022

5 Related Security Guidance and Tools Revised 7/2023

6 Sensitive Unclassified Information Revised 4/2022

7 Defensive Counterintelligence Program (DCIP) Revised 10/2023

B Clauses Revised 1/2009

C Procurement Forms Added 9/2021

D Procurement Samples Added 9/2021

E Procurement Templates Added 9/2021

F Procurement Tools and Resources Added 9/2021

---

### **T3.14.1 Security** Revised 1/2009

#### **A Security**

##### **1 Facility/Security** Revised 1/2019

FAA Facility (per Order 1600.69C, FAA Facility Security Management Program, Appendix 1, #29) is defined as any building, structure, warehouse, appendage, storage area, utilities, and component, which, when related by function and location form an operating entity owned, operated or controlled by the FAA.

##### **2 Information Security and Privacy** Revised 10/2022

All systems and applications must undergo a Security Authorization as specified in FAA Order 1370.121B FAA Information Security and Privacy: Policy, as amended, and required by Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource (2016), and the Federal Information Modernization Security Act (FISMA) 2014. FAA Order 1370.121B as amended requires the use of the FAA Security Authorization Handbook, current version. The FAA Security Authorization Handbook provides the required guidance, process, and templates for conducting a Security Authorization and is based on the most current versions of the National Institute of Standards and Technology (NIST) Publications and Standards, Department of Transportation (DOT) Compendium and FAA Policies.

The Office of Information Security and Privacy (IS&P), Compliance Division, Assessment Branch (AIS-230) provides Security Authorization services to Office of Finance and Management (AFN) organizations and Lines of Businesses (LOBs) that have requested and funded these services.

FAA will further use the Information Security Continuous Monitoring (ISCM) objective to protect High Value Assets (HVAs) and information. FAA and Contractor responsibilities are further defined in AMS clause 3.14-9 “Information Security Continuous Monitoring (ISCM) and Forensics on Contractor Systems”.

*Privacy.* The Privacy Act provides safeguards for individual privacy when the FAA contracts for the design, development and/or operation of a system of records on individuals on behalf of the FAA to accomplish a program function. The Act requires that the contractor follow all of the rules on privacy that apply to the FAA.

An FAA employee may be criminally and/or civilly liable for violations of the Act. When the contract provides for operation of a system of records on individuals, contractors and their employees are considered employees of the FAA for purposes of the criminal penalties of the Act.

The Contracting Officer must review requirements to determine whether a contract will involve the design, development and/or operation of a system of records on individuals. If one or more of these tasks will be required, the Contracting Officer must insure that the contract specifically

identifies the system of records on individuals and the design, development and/or operation work to be performed. The statement of work must identify the FAA rules and regulations implementing the Privacy Act.

*Privacy and Information Technology.* Agencies must ensure that contracts for information technology address protection of privacy in accordance with the Privacy Act (5 U.S.C. 552a) and Part 24. In addition, each agency shall ensure that contracts for the design, development, and/or operation of a system of records using commercial information technology services or information technology support services include the following:

- (a) Agency rules of conduct that the contractor and the contractor's employees shall be required to follow.
- (b) A list of the anticipated threats and hazards that the contractor must guard against.
- (c) A description of the safeguards that the contractor must specifically provide.
- (d) Requirements for a program of FAA inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

The Department of Transportation's implementing rules and regulations for the Privacy Act are contained at 49 CFR Part 10.

### **3 Personnel Security** Revised 4/2022

#### *a. Definitions.*

- (1) *Access.* The ability to physically enter or pass through an FAA area or a facility; or having the physical ability or authority to obtain FAA sensitive information, materials, or resources; or the ability to obtain FAA sensitive 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 (LAN or WAN). When used in conjunction with classified information, access is the ability, authority, or opportunity to obtain knowledge of such information, materials, or resources, in accordance with the provisions of Executive Order (EO)12968, Access to Classified Information.
- (2) *Classified Acquisition.* An acquisition in which offerors must access classified information (Confidential, Secret, or Top Secret) to properly submit an offer or quotation, to understand the performance requirements, or to perform the contract.
- (3) *Classified Contract.* Any contract, purchase order, consulting agreement, lease agreement, interagency agreement, memorandum of agreement, or any other agreement between 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.

(4) *Classified National Security Information (CNSI)* or “classified information” is information that has been determined pursuant to Executive Order 13526 Classified National Security Information or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(5) *Contractor Employee*. A person employed as or by a contractor, subcontractor, or consultant supporting FAA or any non-FAA person who performs work or services for FAA within FAA facilities.

(6) *Electronic Questionnaires for Investigations Processing (eQIP)*. Government system used to electronically process initial and subsequent background investigation requests.

(7) *FAA facility*. Any staffed or unstaffed 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 FAA.

(8) *Foreign National*. Any citizen or national of a country other than the United States who has not immigrated to the United States and is not a Legal Permanent Resident (LPR) of the United States.

(9) *Immigrant Alien*. Any person not a citizen or national of the United States who has been lawfully admitted for permanent residence to the United States by the U.S. Citizen and Immigration Service (USCIS). (Refer to the Immigration and Nationality Act (INA)(8 United States Code 1101), Sections 101(a)(3) and (20).

(10) *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 USCIS, but who has not been lawfully admitted for permanent residence. (Refer to the INA, Sections 101(a)(3) and (20).

(11) *Operating Office*. An FAA line of business, an office or service in FAA headquarters or an FAA division-level organization in a region or center, or any FAA activity or organization that utilizes the services and/or work of a contractor.

(12) *Quality Assurance Program*. A system that provides 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 are dependable and reliable.

(13) *Resources*. FAA physical plant, sensitive equipment, information databases including hardware, software and manual records pertaining to agency mission or personnel.

(14) *Sensitive Information*. Any information which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an EO or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive data includes propriety data.

(15) *Sensitive Unclassified Information (SUI)*. SUI is unclassified information— *in any form including print, electronic, visual, or aural forms* - 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 (FOIA).

(16) *Servicing Security Element (SSE)*. The FAA headquarters, region, or center organizational element responsible for providing security services to a particular activity. Note: This term no longer applies to personnel security where the AXP organizational designation is now used instead. The term still applies to information and facility security.

(17) *Vendor Applicant Process (VAP)*. FAA system utilized to process and manage personnel security information for contractor personnel.

b. The National Industrial Security Program (NISP) was established by EO 12829, January 6, 1993, to ensure that cleared industry safeguards the classified information in their possession while performing work on contracts, programs, bids or research and development efforts. The NISP Operating Manual (NISPOM) prescribes the requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by the U.S. Government. Effective February 24, 2021, the NISPOM was codified in 32 CFR Part 117.32 CFR Part 117 is available online on govinfo at <https://www.govinfo.gov/content/pkg/FR-2020-12-21/pdf/2020-27698.pdf>.

c. AMS Policy Section 3.5, Patents, Data, and Copyrights, contains policy for safeguarding classified information in patent applications and patents.

d. *Classified Information-Responsibilities of the Contracting Officer (CO)*.

(1) Ensure that the Screening Information Request (SIR) and contract clearly identify the security, access, storage, and safeguarding requirements for contractor access to any Classified National Security Information (CNSI) as well as the highest level of access required. Additionally ensure that the contract documentation and processes comply with current NISP requirements.

(2) The CO must contact the Information Safeguards Division, AXF-200 and the responsible Office of Personnel Security (AXP) Division regarding FAA procedures and requirements for any contracting activity requiring contractor access to classified information, whether that information is owned by another agency or FAA. The responsible security organizations include the following:

(a) Headquarters – ASH Office of Infrastructure Protection, Information Safeguards Division, AXF-200

(b) ASH Office of Personnel Security (National Capital, AXP-300; East, AXP-400; Central, AXP-500 and West, AXP-600). The William J. Hughes Technical Center (WJHTC) is under the security cognizance of AXP-400 for classified

contracting processes.

(c) Mike Monroney Aeronautical Center (MMAC) – is under the security cognizance of AXP-500 for classified contracting processes.

(3) *Prescreening Information Request Phase.* COs should review all proposed Screening Information Requests (SIRs) to determine whether access to classified information may be required by offerors, or by a contractor during contract performance. If access to classified information is required, the CO must comply with subparagraph d.(1) and d.(2) above.

(4) *SIR Phase.* COs must:

(a) Ensure the classified acquisition is conducted in accordance with the requirements of d.(1) and d.(2) above;

(b) Include appropriate security requirements and clauses in SIRs (see AMS Clause 3.14-1, Security Requirements – Classified Contracts, and its alternates); and as appropriate in SIRs and contracts when the contractor requires access to classified information. Requirements for security safeguards in addition to those provided in AMS Clause 3.14-1, Security Requirements – Classified Contracts, might be necessary in some instances; and

(c) Ensure the use of Contract Security Classification Specification, DD Form 254 when classified contracts are employed. The DD 254 will be part of the contract. Instructions for DD 254 may be found at <https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254-Inst.pdf>.

Types of DD Form 254s are as follows:

- (i) Original –issued as part of a solicitation for a classified contract, upon the award of a classified contract, or upon the award of a classified subcontract;
- (ii) Revised – issued when there is a change to the security requirements or classification guidance The revised DD 254 will be incorporated into the contract by a contract modification; and
- (iii) Final – a final DD 254 is only used to authorize retention of classified material by the contractor beyond the two-year period automatically authorized by NISPOM at the end of the contract. The Contracting Officer must send an Authorization to Retain Classified Material Letter Template to the contractor authorizing this additional retention of classified material.

For consistency in the application of security requirements and classification guidance, the Information Safeguards Division (AXF-200) drafts all DD 254s.

e. *Employment Suitability and Security Clearances for Contractor Personnel.* FAA’s policy on personnel security for contractor employees, including those working on a FAA contract employed at contractor facilities, requires that procurement personnel take appropriate actions

to protect the Government's interest where it appears that contractor employees, subcontractors, or consultants may have access to FAA facilities, classified information, sensitive information, and/or resources. Additional details of the agency's contractor and industrial security program are provided in FAA Order 1600.1F.

*(1) Security Clearances for Contractor Employees.*

(a) FAA Orders 1600.2F and 1600.1F provide that contracts requiring contractor employees to have access to classified information must be prepared and processed according to the procedures contained in the National Industrial Security Program Operating Manual (NISPOM)

(b) In the case of a contract or agreement where the FAA requires persons not employed by the U.S. Government to have access to classified information, a statement to that effect should be included in the SIR and the requirements of FAA Order 1600.1F.

*(2) Employment Suitability of Contractor Employees.*

(a) FAA Order 1600.1F provides specific policy for determining suitability of FAA contractor employees for access to FAA facilities, classified information, Sensitive Unclassified Information (SUI), and/or network information systems. It outlines risk levels and associated investigations requirements, and identified additional specific requirements and exemptions from investigative requirements.

(b) As it pertains to suitability determinations, at a minimum, the following actions are required:

(i) The CO with input from the Operating Office (e.g., Contracting Officer's Representative (COR)), have the responsibility to make an initial determination as to whether the contract will require contractor employees to have access and be subject to, the order in any given SIR and/or contract. An assessment will be made up-front as to whether any positions contained in the staffing plan will require access to FAA facilities, classified information, sensitive unclassified information, and/or resources. If the CO determines that the order does not apply to a given SIR/contract, this will be documented in a memorandum to file, indicating the matter was given due consideration, addressed adequately, and said determination made. The CO may consult the responsible personnel security office for assistance in making the determination, if needed.

(ii) The Operating Office, in coordination with the COR, has the responsibility to make initial position risk/sensitivity level designations based on the initial list of positions and the Statement of Work (SOW). The Office of Personnel Management's (OPM) website contains information on the Position Designation System. The Position Designation Automated Tool at <https://pdt.nbis.mil> was created to ensure positions are designated uniformly and consistently. It is to be used by the Operating Office or COR to document position designations. All OPM Position

Designation Records must be submitted along with the SOW to AXP for review and approval during the solicitation phase.

(iii) For modifications to existing contracts that change the security posture of the contract, new Position Designation Records must be completed and sent to the appropriate AXP office for review and approval. Modifications that do not affect the security posture do not require completion of new Position Designation Records prior to the execution of the modification. For new contracts, the same process would be followed for determining risk/sensitivity level designations, using information required by way of a provision in the SIR.

(iv) *Contractor Staffing Access Questionnaire*. For all contracts subject to the requirements of FAA Order 1600.1F, the Contracting Officer must issue the Contractor Staffing Access Questionnaire or the Leased Space Unescorted Access Questionnaire as part of the solicitation. The Questionnaire from the successful offeror will be used by AXP for planning purposes in reference to contractor access needs under the contract. The solicitation must include the Questionnaire and direct the contractor to fill it out and submit it with their proposal. The contractor's responses to the questionnaire will not be considered as part of the proposal evaluation. The CO will forward the Questionnaire received from the successful offeror in response to a solicitation to 9-ASH-Security-Contract-Customer-Service@faa.gov immediately after contract award.

(v) AMS Clause 3.14-2 (or Real Property Clause 6.9.3 for Leased Space) will require the contractor to submit the completed documentation for each employee in a stated position, as necessary to permit the Office of Personnel Security to make an employment suitability determination. This documentation must be submitted through applicable systems or directly to the appropriate AXP office (for Privacy Act reasons) for approval, or denial of access, using the process described in FAA Order 1600.1F.

(vi) For new contracts, contractor employees must be required to submit the required documentation prior to performing or providing services or supplies under any FAA contract actions. Depending upon the nature and extent of access required, after an initial review of the documentation submitted by the contractor or contractor employee, AXP may grant interim suitability for the contractor employee to commence performing or providing services or supplies under the contract pending completion of the check and/or investigation and final suitability determination.

(vii) For modifications to existing contracts, contractor employees may continue working under the contract pending submission of the necessary documentation, if any, and completion of a background investigation by AXP, if required. Note there is a period of 30 days that cannot be exceeded in which contractors must submit the forms after the positions and designated risk levels have been identified via contract modification. AXP may establish conditions governing such access pending completion



of suitability investigation.

(viii) Notification of termination of employees performing within a stated position under a contract must be provided via the VAP to the FAA by the contractor within one (1) day.

(ix) COs will notify the appropriate AXP office whenever a contract is awarded. (For large contract awards, COs should invite AXP to the kick-off meeting or post-award conference). The CO will advise the AXP office of the awarded vendor, contract number, and the approved position designations for each labor category. In addition, the CO will notify the appropriate AXP office when the status of a contract changes (i.e., replaced, defaulted, terminated, etc.). Prior coordination of new contracts should have occurred between the Operating Office, the CO, and AXP.

*(c) Procedures for Processing Security Investigations.*

(i) Upon contract award, the CO or contractor will communicate to the personnel security specialist (PSS) a point of contact (POC) who will enter data into the Vendor Applicant Process (VAP) ([vap.faa.gov](http://vap.faa.gov)). This POC should be a representative designated by the contractor, and each contract may have a maximum of 5 POCs per contract. The VAP administrator will provide a Web ID, password to each POC and instructions how to operate the VAP system.

(ii) The VAP POC will enter into the VAP system basic identifying information for each contractor and subcontractor employee, requiring an investigation.

(iii) The PSS will examine the information in VAP and check for prior investigations and clearance information.

(AA) If a prior investigation exists that meets the investigative requirements of the position, there has not been a 2-year break in service, and there is no new derogatory information known, the PSS will notify the vendor and CO/COR that no investigation is required and that final suitability is approved.

(BB) If no previous investigation exists, the PSS will send the applicant an e-mail containing instructions for completing investigative requirements.

(iv) The applicant must complete the eQIP form and submit other applicable material within 15 days of receiving the e-mail from the PSS.

(v) If the eQIP form requires additional information, it will be rejected to the applicant with the reason for the rejection.

(vi) The PSS will notify the applicant and CO/COR of any interim

suitability determinations.

(d) *Removal of Contractor Employees.* The VAP POC must notify AXP when a contractor employee is terminated, resigns, or if otherwise removed from a contract by submitting a Removal record in VAP, within twenty-four (24) hours of the removal. CO/CORs have a responsibility to ensure that the vendor complies with this requirement. If a vendor fails to submit a removal record, the CO/COR must notify AXP of the removal as soon as practicable.

(e) *Reports.* The POCs, COs, and CORs have the ability to retrieve current roster reports from VAP for all contracts and contractor employees. The POC must run this report on a quarterly basis to ensure the roster is accurate, and immediately correct any discrepancies with the responsible AXP office.

f. *Costs of Investigations.* To pay for investigations, allotments of funds are made to regions, centers, and headquarters. Unless there has been a specific allotment to AXP to pay for all contractor employee investigations for operating officers that AXP services, each operating office must arrange to pay the costs for investigations on those employees working under contracts for which it is responsible. Security screenings, including fingerprint checks on contractor employees are funded through operational funds by each office or division. The operating office responsible for payment must provide AXP with the accounting code information necessary to have the cost charged appropriately.

g. *Contractor Off-Boarding Requirements.* Contractor employees departing from a FAA contract who have access to FAA facilities and/or Information Technology systems must each complete the FAA Contractor Employee Off-Boarding Form (see Procurement Forms). This does not apply to contractor employees who have been employed on the contract for less than six (6) months and have not been issued a yellow ID card.

The contractor employee's FAA sponsor is responsible for ensuring that the employee completes the Checklist. This responsibility may be delegated to the COR under a given contract. Contractor responsibilities are as indicated in AMS Clause 3.14-4 "Access to FAA Facilities, Systems, Government Property, and Sensitive Information" (or Real Property Clause 6.9.4 for Leased Space).

#### **4 Foreign Nationals** Revised 4/2022

Foreign nationals employed or hired by the contractor to perform services for the FAA must have resided within the United States for a minimum of the last three years unless a waiver of this requirement has been granted by AXP in accordance with FAA regulations (see AMS Clause 3.14-3 or Real Property Clause 6.9.2, Foreign Nationals as Contractor Employees).

#### **5 Related Security Guidance and Tools** Revised 7/2023

The following sections refer to areas within the AMS Guidance that contain security issues to be considered during contract formulation.

### T3.1.6 Nondisclosure of Information

### T3.2.1 Procurement Planning

#### T3.2.2.5 Commercial and Simplified Purchase Method

#### T3.2.2.6 Unsolicited Proposals

#### T3.2.2.7 Contractor Qualifications

### T3.3.1 Contract Funding, Financing & Payment

### T3.5 Patents, Rights in Data, and Copyrights

### T3.6.4 Foreign Acquisitions

### T3.8.9 Information and Communication Technology

## 6 Sensitive Unclassified Information Revised 4/2022

### a. *General.*

(1) FAA Order 1600.75, "Protecting Sensitive Unclassified Information (SUI)," outlines policy and guidance on protecting sensitive unclassified information (SUI).

(2) When a contract, order, lease, or agreement requires a contractor or offeror to have access to SUI, the Contracting Officer (CO) must incorporate appropriate security clauses into the solicitation or contract. These include clauses on safeguarding standards, personnel security suitability, and non-disclosure agreements.

(3) SUI may include information such as Personally Identifiable Information (PII), sensitive NAS data, construction drawings, or equipment specifications. Prospective FAA vendors may need access to this information to ensure they can accurately propose and perform the work that FAA requires.

(4) When a screening information request (SIR) includes information determined to be SUI, the CO (and anyone else granted access to the SUI) must take reasonable care disseminating the SUI documents and ensure the recipient has a *need-to-know* and is *authorized* to receive it.

b. *FOUO and SSI.* There are over 50 types of SUI; however the two types generally handled within FAA are:

(1) *For Official Use Only (FOUO).* FOUO is the primary designation given to SUI by FAA, and consists of information that could adversely affect the national interest, the conduct of Federal programs, or a person's privacy if released to unauthorized individuals. Uncontrolled issuance of FOUO may allow someone to:

(a) Circumvent agency laws, regulations, legal standards, or security measures;  
or

(b) Obtain unauthorized access to an information system.

(2) *Sensitive Security Information (SSI)*. SSI is a designation unique to the FAA, DOT, and the Department of Homeland Security (DHS) Transportation Security Administration (TSA), and applied to information meeting the criteria of 49 CFR Part 15, Part 1520 and Subpart A. SSI is information obtained or developed while conducting security activities, including research and development. Unauthorized disclosure of SSI can:

(a) Constitute an unwarranted invasion of privacy;

(b) Reveal trade secrets or privileged or confidential information; or

(c) Be detrimental to transportation safety or security.

c. *Distribution of SUI Information*. When distributing SUI information, the CO (and anyone else granted access to the SUI, including prime contractors, subcontractors, suppliers, etc.) must ensure the persons receiving the information are *authorized* to receive the SUI and have a *need-to-know*. Methods of pre-award SUI dissemination utilized in FAA include SAM.gov and other electronic transfer and dissemination.

d. *The System for Award Management (SAM.gov)*. SAM.gov is an E-Gov initiative that provides a secure environment for distributing sensitive acquisition information (to include SUI) to vendors during the solicitation phase of procurement. This system electronically disseminates information or data to the vendor community while still protecting SUI from unauthorized distribution. Data that can be uploaded into SAM.gov includes construction plans, equipment specifications, security plans, and SIRs. As FAA utilizes the FAA Contract Opportunities page located on SAM.gov to announce procurement opportunities, COs will utilize the Controlled Attachment functionality in SAM.gov when electronically distributing SUI.

(1) SAM.gov provides several security measures to include:

(a) During processing of a vendor's access request to SAM.gov, the vendor's profile is retrieved from the System for Award Management (SAM) using the Unique Entity Identifier (UEI);

(b) *Marketing Partner Identification Number (MPIN)*. A number required by SAM.gov to access SUI. This number is unique to each vendor, and chosen by the vendor when each vendor registers with SAM;

(c) Vendors receive an e-mail after registration to confirm the validity of their identity and contact information;

(d) The access level of the data in SAM.gov can be adjusted; the CO can

specifically allow access to only certain vendors, or if a vendor requests access to the data and they are not specifically authorized, the system will verify with the CO if access should be granted (termed "Explicit Access Request"); and

(e) The system tracks which Government users and vendors access the data through SAM.gov.

(2) Use of SAM.gov requires the CO to adhere to the following process:

(a) Upload SUI files into the SAM.gov website (<https://sam.gov/SAM/>) by the procurement request (PR) and solicitation numbers. Note that the problems may arise when uploading attachments greater than 250 mb.

(b) "Release" the solicitation: Prior to it being made available to anyone through SAM.gov, the CO must determine the scope of vendors allowed to access the data and release the data for authorized viewing.

(c) Once established in SAM.gov, the system provides the CO a web address to provide to vendors that will link authorized persons directly into the applicable data. The CO can email this link to individual vendors when access has been restricted, or can place it on a public announcement via the internet so, if properly registered, all interested parties may view the data.

(3) Web-based training and user guides are available to both FAA users and contractors at <https://sam.gov/SAM/>.

e. *Registration with SAM.gov.* For registration instructions, please refer to the SAM.gov website.

f. *Other Electronic Transfer and Dissemination.* Transfer and dissemination of SUI information beyond the intranet (internet or extranet, modem, DSL, wireless, etc.) must use at least 128 bit symmetric key encryption following NIST Special Publication 800-21 *Guideline For Implementing Cryptography in the Federal Government*. All transfers must use standard commercial products (such as PGP and Secret Agent) with encryption algorithms that are at least 128 bit symmetric (3DES, AES, RC4, IDEA, etc.), and follow the instructions outlined in this order. Authorized users that use project extranets for electronic project management during or after contract award to transfer SUI information are responsible for verifying and certifying to the CO that project extranets meet applicable physical and technical security requirements as determined by the Chief Information Officer. Access to the sites must be password protected and access must be granted only on a need-to-know basis. A record of those individuals who have had electronic access must be maintained by the CO or other disseminator in accordance with the system of keeping long-term records.

g. *Record Keeping.* Records of the signed forms must be maintained by the disseminator and destroyed 2 years after final disposition of the related SUI material (FAA Order 1350.14B and GRS 18 Item 1). At the completion of work, secondary and other disseminators must turn over their dissemination records to FAA, to be kept with the permanent files. The only records that the CO must keep for those vendors that utilize SAM.gov to request SUI are the request forms for hardcopy documentation and any documentation detailing subsequent

dissemination by the vendor and their subcontractors or suppliers. Records of those who accessed SUI information via SAM.gov and their associated SUI policy certifications are stored in SAM.gov itself.

h. *Retaining and Destroying Documents.* The requirements above must continue throughout the entire term of contract and for whatever specific time thereafter as may be necessary. Necessary record copies for legal purposes (such as those retained by the architect, engineer, or contractor) must be safeguarded against unauthorized use for the term of retention. Documents no longer needed must be destroyed (such as after contract award, after completion of any appeals process, or completion of the work). Destruction must be by burning or shredding hardcopy, and physically destroying CDs, deleting and removing files from electronic recycling bins, and removing material from computer hard drives using a permanent erase utility or similar software.

i. *Notice of Disposal.* For all contracts using SUI, the contractor must notify the CO that it and its subcontractors have properly disposed of the SUI documents, except the contractor's record copy, at the time of Release of Claims to obtain final payment.

j. *State and Local Governments.* To comply with local regulations, FAA must provide localities with documents to issue building permits and to approve code requirements. Public safety entities such as fire departments and utility departments require unlimited access on a need-to-know basis. These authorities must be informed at the time they receive the documents that the information requires restricted access from the general public. When these documents are retired to local archives, they should be stored in restricted access areas. This will not preclude the dissemination of information to those public safety entities.

## **7 Defensive Counterintelligence Program (DCIP) Revised 10/2023**

a. The Defensive Counterintelligence Program (DCIP) detects, deters, and denies illicit human and technical intelligence collection activities by a foreign power or agents of a foreign power as defined in 50 U.S.C. § 1801. This Program is implemented by FAA Order 1600.84 “FAA Defensive Counterintelligence Program.”

b. This Order applies to all contractors where contractor employees-

- (1) Are authorized unescorted access to non-public areas of FAA facilities;
- (2) Have access to non-public portions of FAA equipment, networks, or information systems; or
- (3) Have access to classified national security information (CNSI), sensitive unclassified information (SUI), or otherwise protected information in the possession of the FAA.

Contractor responsibilities under applicable contracts are specified in Clause 3.14-14 “Cooperation with Defensive Counterintelligence Program (DCIP) Requirements” (or Real Property Clause 6.9.6 for Leased Space or Land).

c. Responsibilities of COs and CORs under contracts where FAA Order 1600.84 applies are the following:

- (1) Familiarize themselves with their responsibilities and contractors' responsibilities as described in this Order, including without limitation cooperating with authorized DCIP inquiries and CI investigations.
- (2) COs should include the appropriate contract clauses and provisions in relevant contract(s) as necessary to ensure contractors are required to meet all of their responsibilities as described in this Order.
- (3) Ensure that contractors are aware of their responsibilities, as described in this Order and the relevant contract(s).
- (4) If there will be foreign travel by contractors under the contract, ensure contractors are aware of the international travel security briefing and foreign contact reporting requirements contained in FAA Order 1600.61C, *International Travel Security Program* at <https://my.faa.gov/org/linebusiness/ash/programs/ITSP.html#official> (FAA only), as well as the international travel security briefing and foreign contact reporting requirements of Security Executive Agent Directive-3 (SEAD-3) implemented by the FAA at <https://my.faa.gov/org/linebusiness/ash/programs/ITSP.html> (FAA only).
- (5) When requested by the DCIP and when necessary to protect CNSI, SUI, or otherwise protected information, an employee, as defined in FAA Order 1600.84, must sign a Defensive Counterintelligence Program Non-Disclosure Agreement (Appendix C to FAA Order 1600.84) prior to being briefed on any information pertaining to a DCIP inquiry, a CI investigation, or any other matter related to the DCIP.
- (6) COs or CORs may contact AXI-1, AXI-300, or AXI-310 directly with questions about their responsibilities, and employees' responsibilities, for cooperating with a DCIP inquiry or CI investigation.

## **B Clauses** Revised 1/2009

[view contract clauses](#)

## **C Procurement Forms** Added 9/2021

Document Name
Contract Security Classification Specification (DD 254)
Contractor Access Staffing Questionnaire
Contractor Employee Off-Boarding Form

**D Procurement Samples** Added 9/2021

Document Name

**E Procurement Templates** Added 9/2021

Document Name

**F Procurement Tools and Resources** Added 9/2021

Document Name