

Acquisition Management Policy - (10/2016)

3.14 Security

3.14.1 Applicability

3.14.2 Policy

3.14.2.1 Contractor Personnel Security Program Revised 10/2016

3.14.2.1.1 Employment Suitability Revised 10/2007

3.14.3 Classified Information Revised 7/2007

3.14.4 Sensitive Unclassified Information

3.14.5 Facility Security Program

3.14.6 Information and System Security Revised 10/2016

3.14 Security

3.14.1 Applicability

This section is applicable to all screening information requests and contracts.

3.14.2 Policy

3.14.2.1 Contractor Personnel Security Program Revised 10/2016

The acquisition community shall ensure an adequate level of security for contractor employees as stated in FAA Order 1600.72A, allowing for compliance with OMB Circular A-130, "Management of Federal Information Resources", Executive Order 12829 "National Industrial Security Program", and DOD Directives 5200.2 and 5220.22M.

All FAA employees and contractor and subcontractor employees are subject to the FAA's Insider Threat Detection and Mitigation Program (ITDMP) provided they meet the definition of an "FAA employee" and fall within the scope of the program as defined in FAA Order 1600.82. For more information on this Program, please see https://employees.faa.gov/documentLibrary/media/Order/FAA_Order1600.82.pdf (FAA only).

3.14.2.1.1 Employment Suitability Revised 10/2007

Contractor employees (including contractors, subcontractors, or consultants) shall be subject to the same investigative and personal identification verification requirements as Federal employees if in similar positions requiring recurring access to FAA facilities or access to FAA information systems or sensitive information.

3.14.3 Classified Information Revised 7/2007

The CO will ensure that all proposed and awarded procurement actions contain appropriate provisions and clauses if access to classified information is required, in accordance with The National Industrial Security Program Operating Manual, DOD 5220.22-M and FAA Order 1600.72A, Contractor and Industrial Security Program.

3.14.4 Sensitive Unclassified Information

The CO, in coordination with the service organization, will ensure that all contractual actions contain provisions and clauses to protect the unauthorized dissemination of FAA sensitive information. Such information may entail Sensitive Unclassified Information (SUI), For Official Use Only (FOUO), Sensitive Security Information (SSI), or any other designator assigned by the US Government to identify unclassified information that may be withheld from public release. The Freedom of Information Act (FOIA) provides in exemptions 2 through 9, the guidelines for withholding sensitive unclassified information from the public and how such information must be

protected from unauthorized disclosure. Section 552a of Title 5, United States Code (the Privacy Act) identifies 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.

3.14.5 Facility Security Program

The Facility Security Risk Management process, as developed through the FAA's Facility Security Management Program, FAA Order 1600.69, shall be an integral part of program concept, planning, engineering design, and the implementation of required protective measures maintained throughout the lifecycle for physical security enhancements.

3.14.6 Information and System Security Revised 10/2016

The Federal Information Security Modernization Act, 2014 (FISMA), OMB Circular A-130, and other federal standards and regulations describe information security for all agency information that is collected, stored, processed, disseminated, or transmitted using agency or non-agency owned information systems. For additional FAA ISS Program policy, see FAA Order 1370.82A (FAA only). The contractor must comply with all applicable policies as indicated in the Statement of Work/Specification.

Regarding possible security breaches, in accordance with OMB Memorandum 07-16, when the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring any notification and corrective actions are taken.

FAA will notify and consult with the United States Computer Readiness Support Team (US-CERT) regarding information security incidents involving the information and information systems that support the operations and assets of the FAA, including contractor systems that support the FAA.

Offerors must indicate in responding to SIRs for Information Technology (IT) or services in support of IT whether they will be using an international processing hub or exchange for FAA data or information, or if any subcontractors or third parties more than 50% foreign owned will be processing, storing, or backing up the data and information.