AMS/FAST CHANGE REQUEST (CR) COVERSHEET

Change Request Number: 18-16

Date Received: 1/18/18

Title: Information Systems Security Policy Changes

Initiator Name: Tim Eckert

Initiator Organization Name / Routing Code: Procurement Policy Branch, AAP-110

Initiator Phone: 202.267.7527

ASAG Member Name*:* Genesta Belton

ASAG Member Phone*:* 202.267.0332

Policy and Guidance: (check all that apply)

- ☒ Policy
- ☐ Procurement Guidance
- ☐ Real Estate Guidance
- ☐ Other Guidance
- ☐ Non-AMS Changes

Summary of Change:
Per FAA Order 1370.121 "Information Security and Privacy Program & Policy" Privacy part of 3.7 moved in with 3.14.6 Information Security. Also administrative updates to FAA order references.

Reason for Change:
Consistency with new FAA Order

Development, Review, and Concurrence: AIS-110, Acquisition Policy, Contracts, and Procurement Legal.

Target Audience: Contracting and program office personnel

Briefing Planned: No.

ASAG Responsibilities: ASAG approved 9/28/18.

Section / Text Location: 3.7, 3.14.6 and 4.11

The redline version must be a comparison with the current published FAST version.

- (●) I confirm I used the latest published version to create this change / redline

or

- ( ) This is new content

Links:
http://fast.faa.gov/docs/acquisitionManagementPolicy/acquisitionManagementPolicy_3.pdf
http://fast.faa.gov/docs/acquisitionManagementPolicy/AcquisitionManagementPolicy_4.pdf

Attachments: Redline and final documents.

Other Files: N/A

Redline(s):
Section Revised:
3.7.1 Applicability
3.7.2 Policy

Acquisition Management Policy - (~~7/2018~~ 10/2018)

3.7 ~~Protection of Privacy and~~ Freedom of Information Revised 10/2018
3.7.1 Applicability Revised 10/2018
3.7.2 Policy Revised ~~10/2016~~ 10/2018

3.7 ~~Protection of Privacy and~~ Freedom of Information Revised 10/2018

3.7.1 Applicability Revised 10/2018

~~Protection of privacy and f~~Freedom of information ~~are~~is applicable to all FAA procurements~~,~~ including agreements, real property, utilities, credit cards, commercial and simplified purchase method.

3.7.2 Policy Revised ~~10/2016~~ 10/2018

~~When the FAA contracts for the design, development, and/or operation of a system of records on individuals, the FAA will apply the requirements of the Privacy Act to the contractor and its employees working on the contract.~~

The FAA will comply with the Freedom of Information Act which requires that the FAA provide information to the public by (i) publication in the Federal Register; (ii) providing an opportunity to read and copy records; or (iii) upon a reasonable request. Certain information may be exempted from disclosure; such as, classified information, trade secrets, and confidential commercial or financial information, interagency or intra-agency memoranda, or to personal and medical information pertaining to an individual.

Redline(s):
Section Revised:
3.14.2.1 Contractor Personnel Security Program
3.14.6 Information and System Security and Privacy

Acquisition Management Policy - (~~7/2018~~ 10/2018)

3.14 Security
- 3.14.1 Applicability
- 3.14.2 Policy
  - 3.14.2.1 Contractor Personnel Security Program Revised ~~10/2016~~ 10/2018
    - 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 and Privacy Revised ~~10/2016~~ 10/2018

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~~ 10/2108

The acquisition community must 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_Order_1600.82.pdf~~
https://www.faa.gov/regulations_policies/orders_notices/(FAA only).

3.14.2.1.1 Employment Suitability Revised 10/2007

Contractor employees (including contractors, subcontractors, or consultants) must 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, must 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 and Privacy (IS &P) Revised ~~10/2016~~ 10/2108

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~~ IS &P Program policy, see FAA Order ~~1370.82A~~1370.121 at https://www.faa.gov/regulations_policies/orders_notices/ (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.

Protection of privacy is applicable to all FAA procurements, including agreements, real property, utilities, credit cards, commercial and simplified purchase method. When the FAA contracts for the design, development, and/or operation of a system of records on individuals, the FAA will apply the requirements of the Privacy Act to the contractor and its employees working on the contract.

Redline(s):
Section Revised:
4.11 Security

Acquisition Management Policy - (~~7/2018~~ 10/2018)

4.11 Security **Revised ~~10/2016~~ 10/2018**

4.11 Security Revised ~~10/2016~~ 10/2018

Introduction

Service organizations and program offices must allow sufficient time and resources to address security laws, policies, and orders including the cost of implementing required security controls into acquired components. Security policy within the FAA is divided into information security; physical security, facility security, and personnel security; and sensitive information and personally identifiable information. There is overlap between the disciplines (for example, physical security is employed to protect classified materials), so all areas of security policy must be evaluated to ensure full compliance with the various orders and policies.

Information Security and Privacy Policy

The Federal Information Security Modernization Act, 2014 (FISMA), Office of Management and Budget Circular A-130, Management of Federal Information Resources, National Institute of Standards and Technology (NIST) guidance, and other federal, departmental, and agency-level guidance and standards as amended, describe information ~~system security (ISS)~~ security & privacy (IS & P) needed for all FAA information systems. FAA information systems reside in one of three domains: national airspace system (NAS), mission support/administrative, and research and development. They may consist of government-owned/managed components, contractor-owned/managed components, or combinations of these types. They are segregated into infrastructure for air traffic operations and infrastructures for information technology administrative support. The infrastructures exchange information via authorized security gateways.

FAA ~~ISS~~ IS & P requirements are derived from NIST special publications and federal information processing standards. The FAA Office of Information Security and Privacy (AIS) defines and maintains the agency enterprise information security and privacy policy. Because the NAS is classified as critical infrastructure, NAS systems must comply with additional ISS requirements as defined by Air Traffic Organization Policies. These ATO policies can be found on the FAA's Website under policy and guidance and are designated with the letters "JO".

To receive a successful in-service decision, all FAA investment programs must undergo a security authorization that assesses outputs and products against mandatory security requirements. The security authorization process is defined in FAA Order ~~1370.82, Information Systems Security Program~~1370.121 FAA Information Security and Privacy Program & Policy. The Security Authorization Handbook details the process for compliance with ISS requirements during solution implementation and in-service management. Investment programs must consult the Information Security Guidance for System Acquisitions (ISGSA) at each planning phase of the AMS lifecycle to ensure information security requirements and related information are included in acquisition artifacts, and to ensure the investment program is on track for a successful security authorization.

Physical, Facility and Personnel Security Policy

The FAA must conform with national policy related to physical security of the aviation infrastructure including leased and owned facilities, the security of all information associated with operation of the FAA and aircraft operations, and personnel security. The FAA is also obligated to protect proprietary information to which it has access. Physical security is directly applicable to aviation industry operations and activities, and to supporting infrastructure such as communications, sensors, and information processing. FAA Order 1600.69, Facility Security Management Program, establishes both policy and guidance for physical security.

FAA Order 1600.1, Personnel Security Program, establishes both policy and guidance for FAA personnel security. In addition, detailed guidance to implement personnel and physical security with respect to contractors is in FAA Order 1600.72, Contractor and Industrial Security Program.

Classified National Security Information (CNSI) and Sensitive Unclassified Information (SUI) Policy

In order to meet the spirit of Executive Order 13526 and 32 CFR Part 2001 to protect classified national security information from unauthorized disclosure~~.~~, ~~S~~systems containing or processing classified data are managed by the FAA Office of Security and Hazardous Materials Safety in accordance with FAA Order 1600.2F, Safeguarding Classified National Security Information. FAA Order 1600.75 Protecting Sensitive Unclassified Information (SUI) is in effect at https://employees.faa.gov/tools_resources/orders_notices/index.cfm (FAA only).

The Privacy Act of 1974 and the E-Government Act of 2002 (Public Law 107-347) mandate protection of an individual's right to privacy and the prevention of unauthorized dissemination of personal information. ~~FAA Order 1280.1, Protecting Personally Identifiable Information established both the policy and guidance for handling this type of SUI. In addition, it establishes the position of the FAA Privacy Officer with respect to information technology.~~ FAA Order 1370.121 Appendices 19-26 establishes the policy and guidance for handling Personally Identifiable Information (PII). The FAA Privacy Office will handle all privacy issues.