AMS CHANGE REQUEST (CR) COVERSHEET

Change Request Number: 16-29

Date Received: 9/21/16

Title: Cybersecurity - Policy Changes

Initiator Name: Tim Eckert

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

Initiator Phone: 202.267.7527

ASAG Member Name*:* Eugene Scott

ASAG Member Phone*:* 202.267.3207

Policy and Guidance: (check all that apply)

- ☒ Policy
- ☐ Procurement Guidance
- ☐ Real Estate Guidance
- ☐ Other Guidance

Summary of Change: Changes to policy addressing cyberscurity concerns

Reason for Change: Changes are in response to new security requirements from OMB, Congress, Executive Orders, etc.

Development, Review, and Concurrence: Office of Information Security & Privacy, Acquisition Policy, Procurement Legal, and Contracts

Target Audience: Program Offices and Contracting Personnel

Briefing Planned: Discussed at the March 15 and May 17 ASAG Meeting. Electronically approved on September 15.

ASAG Responsibilities: Review and comment.

Section / Text Location: 3.7, 3.8.2.5, 3.14.2.1, 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.pdf

Attachments: Redline and final documents.

Other Files: N/A

Redline(s):

Section Revised: 3.7.2 – Policy

Acquisition Management Policy - (~~7/2016~~ 10/2016)

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

3.7 Protection of Privacy and Freedom of Information

3.7.1 Applicability

Protection of privacy and freedom of information are applicable to all FAA procurements, agreements, real property, utilities, credit cards, commercial and simplified purchase method.

3.7.2 Policy **Revised 10/2016**

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

The FAA shall 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.

Section Added: 3.8.2.5 – Cloud Computing Services Contracts

Acquisition Management Policy - (~~7/2016~~ 10/2016)

3.8 Special Categories of Contracting
- 3.8.1 Agreements
  - 3.8.1.1 Applicability
  - 3.8.1.2 Use of Agreements Revised 1/2012
  - 3.8.1.3 Principles for Agreements
- 3.8.2 Service Contracting
  - 3.8.2.1 Applicability
  - 3.8.2.2 Policy
  - 3.8.2.3 Personal Services Contracts
    - 3.8.2.3.1 Reserved
    - 3.8.2.3.2 Determination
  - 3.8.2.4 Performance Based Service Contracts
  - 3.8.2.5 Cloud Computing Services Contracts Added 10/2016
- 3.8.3 Federal Supply Schedule Contracts
  - 3.8.3.1 Applicability
  - 3.8.3.2 Policy
- 3.8.4 Required Sources of Products/Services and Use of Government Sources
  - 3.8.4.1 Applicability Revised 2/2005
  - 3.8.4.2 Government Sources for Products and Services Revised 10/2014
- 3.8.5 Leases Added 1/2006
  - 3.8.5.1 Applicability Added 1/2006
  - 3.8.5.2 Policy Added 1/2006
- 3.8.6 Strategic Sourcing Revised 7/2007
- 3.8.7 Construction Contracting Added 7/2007
  - 3.8.7.1 Applicability Added 7/2007
  - 3.8.7.2 Policy Added 7/2007

3.8 Special Categories of Contracting

3.8.1 Agreements

3.8.1.1 Applicability

3.8.1.2 Use of Agreements Revised 1/2012

It is FAA's policy to use various agreements, other than procurement contracts, to obtain or provide services and supplies when necessary to accomplish the mission of FAA. These agreements may be made with another Federal agency or instrumentality of the Federal government, a modal administration within the Department of Transportation, a state, local government, municipality, or other public entity, and private entities. (See 49 U.S.C. 106(l)). The following is a list of the more commonly used agreements (other than procurement contracts):

- Interagency agreements;
- Intra-agency agreements;
- Reimbursable agreements;
- Agreements with other public entities; and
- Agreements to provide services to a private entity on an individualized basis.

3.8.1.3 Principles for Agreements

Agreements with other Federal Agencies (as defined in section 551(1) of title 5) are appropriate where FAA provides services or supplies or facilities to another Federal agency, or where FAA is the requesting agency to receive services, or supplies, or facilities from another Federal agency or that agency's contractor. Where the FAA and the Department of Defense are engaged in joint actions to improve or replenish the national air traffic system, the AMS policies governing FAA acquisitions are applicable. In those instances where the FAA acquires goods or services through the Department of Defense or other agencies, the FAA is bound by the acquisition laws governing those agencies.

3.8.2 Service Contracting

3.8.2.1 Applicability

This section applies to advisory and assistance contracts and other services, including personal services such as employees support service as provided for in FAA's Personnel Management System. This section does not apply to FAA employees, temporary, part-time or permanent appointed or hired in accordance with the other applicable portions of the FAA Personnel Management System.

3.8.2.2 Policy

The FAA shall generally rely on the private sector for commercial services (see OMB Circular No. A-76, Policies for Acquiring Commercial or Industrial Products and Services Need by the Government). In no event may a contract be awarded for the performance of an inherently governmental function. Advisory and assistance contracts shall comply with all applicable laws concerning post-employment and other conflict of interest and ethics laws and policies.

3.8.2.3 Personal Services Contracts

3.8.2.3.1 Reserved

3.8.2.3.2 Determination

The FAA may award personal services contracts when the head of a line of business determines that a personal service contract is in the best interest of the agency after thorough evaluation, which includes, but is not limited to the following factors:

- Worker's compensation payments and other tax implications;
- Government's potential liability for services performed;
- Availability of temporary hires to perform the desired services;
- Demonstration of tangible benefits to the agency;
- Detailed cost comparison demonstrating a financial advantage to the Government from such contract;
- Potential post employment restrictions applicable to former employees;
- Legal determination that the work to be performed is not inherently governmental; and
- Potential post employment restrictions pursuant to Federal Workforce Restructuring Act of 1994 Public Law 103-226.

Although personal service contracts are permitted, they should be used only when there is a clear demonstrated financial and program benefit to the FAA. The determination required herein is non-delegable and shall be reviewed for legal sufficiency by the Office of the Chief Counsel.

3.8.2.4 Performance Based Service Contracts

Service contracts should incorporate performance based contracting methods to encourage contractor innovation and efficiency, and to help ensure contractors provide timely, cost- effective, and quality performance with measurable outcomes as opposed to either the manner by which the work is to be performed or broad and imprecise statements of work.

3.8.2.5 Cloud Computing Services Contracts **Added 10/2016**

All cloud computing services contracts will be conducted in accordance with Federal Risk and Authorization Management Program (FedRAMP) requirements. Further information on FedRAMP may be found at www.fedramp.gov.

3.8.3 Federal Supply Schedule Contracts

3.8.3.1 Applicability

This section is applicable when FAA awards Federal Supply Schedule delivery orders for recurring products and services. Additionally, this section addresses requirements to utilize Federal Supply Schedules awarded by GSA, when the FAA is identified in the schedule as a mandatory/non-mandatory user of any supply/service on the schedule.

3.8.3.2 Policy

The FAA may consider awarding Federal Supply Schedule contracts, or placing orders against Federal Supply Schedules awarded by GSA, for recurring products and services when it is determined to be in the best interest of the FAA.

3.8.4 Required Sources of Products/Services and Use of Government Sources

3.8.4.1 Applicability Revised 2/2005

This section applies to procurement of all products and services, except for real property, utilities, and construction.

3.8.4.2 Government Sources for Products and Services Revised 10/2014

The CO may use available Government sources when they offer the best value to satisfy FAA's mission need. However, pursuant to FAA policy, the CO must acquire products and services offered through the Randolph-Sheppard Vending Facilities Program (20 U.S.C. 107) and AbilityOne (formerly the Javits-Wagner-O'Day Program) (41 U.S.C.§§ 8501-8506).

FAA policy also requires that FAA purchase products offered by Federal Prison Industries (FPI) when the FPI's product represents the best value to FAA, unless an exception below applies. In making a best value determination for FPI products, the CO must utilize the procedures in AMS Procurement Guidance T3.8.4.A.4. The CO must post an announcement for any procurement for products available from FPI in accordance with AMS Policy 3.2.1.3.12. This policy concerning FPI does not apply if:

(a) The monetary value of the procurement would not require a competitive procurement process under AMS Policy 3.2.2.4;

(b) A market analysis would not be required under AMS Policy 3.2.2.4 to support a single-source procurement of the product;

(c) Suitable used or excess products are available from the government; (d)

The products are acquired and used outside the United States;

(e) Services are being acquired; or

(f) FAA has obtained a waiver from FPI with respect to the particular product or class of products at issue in the procurement.

The CO may allow contractors with cost-reimbursement contracts to use Government sources when in FAA's best interest and the products or services are available. Contractors with fixed- price contracts to protect classified information may acquire security equipment through GSA sources after CO approval.

3.8.5 Leases **Added 1/2006**

3.8.5.1 Applicability **Added 1/2006**

This section applies to products, services and real property to the extent authorized by law. For Real Property specific policy and Guidance see Section 4.2 Real Property.

3.8.5.2 Policy **Added 1/2006**

It is the policy of the FAA to enter into leases for various products, services or real property when it is determined by the Contracting Officer, based on financial and other considerations, to be in the best interest of the Government compared to the outright purchase of such assets, real property, or services.

It is also FAA policy to avoid establishment of capital leases or lease purchases unless the requesting organization demonstrates they have complied with the requirements of OMB Circular A-11, Part 8, Appendix B "Scoring of Lease Purchases and Leases of Capital Assets".

3.8.6 Strategic Sourcing **Revised 7/2007**

The FAA is leveraging its spending through strategic sourcing and will award contracts for products and services to help the agency optimize performance and minimize price to increase the value of each dollar spent. Therefore, when a needed product or service is available through a strategic sourcing contract, purchasing employees must use a strategic sourcing contract.

All strategic sourcing contracts are established following the AMS Policy and Guidance. To increase achievement of socio-economic acquisition goals, all strategic sourcing procurements must be balanced with socio-economic goals for small businesses, small disadvantaged businesses,

women-owned small businesses, veteran-owned businesses, and service-disabled veteran-owned businesses in accordance with AMS Policy 3.6.1 Small Business Development Program.

When performance of any strategic sourcing contract requires access to FAA facilities and/or requires handling of sensitive material, the contract must include all of the appropriate clauses and/or restrictions and comply with FAA Order 1600.72A, Contractor and Industrial Security Program and FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI).

When an organization is going to strategically source a product or service, it must use mandatory government sources as described in AMS Policy 3.8.4 and Procurement Guidance T3.8.4A.

3.8.7 Construction Contracting Added 7/2007

3.8.7.1 Applicability Added 7/2007

This section applies to construction contracts, contracts for dismantling, demolition, or removal of improvements, and to the construction portion of contracts for products or services.

3.8.7.2 Policy Added 7/2007

If portions of multipurpose contracts are so commingled that priced deliverables for construction, service, or supply cannot be segregated and the predominant purpose of the contract is construction, the contract will be classified as construction.

Sections Revised: 3.14.2.1 – Contractor Personnel Security Program
3.14.6 – Information and System Security

Acquisition Management Policy - (~~7/2016~~ 10/2016)

3.14 Security
- 3.14.1 Applicability
- 3.14.2 Policy
  - 3.14.2.1 Contractor Personnel Security Program Revised ~~7/2007~~ 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 ~~7/2007~~ 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 ~~FAA is required by law,~~ Federal Information Security ~~Management~~Modernization Act, ~~2002~~2014 (FISMA), OMB Circular A-130, and other federal standards and regulations ~~to provide~~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.

Sections Revised: 4.11 – Security

Acquisition Management Policy - (~~7/2016~~ 10/2016)

4.11 Security Revised ~~10/2015~~ 10/2016

4.11 Security Revised ~~10/2015~~ 10/2016

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 Policy

The Federal Information Security ~~Management~~Modernization Act, ~~2002~~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) 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 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. 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 ~~Orders~~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.

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

~~The FAA is required by~~In order to meet the spirit of Executive ~~Orders~~Order 13526 and 32 CFR Part 2001 to protect classified national security information from unauthorized disclosure. Systems containing or processing classified data are managed by the FAA Office of Security and Hazardous Materials Safety in accordance with FAA Order 1600.2, Safeguarding Classified National Security Information. ~~The FAA is also required under 49 CFR Part 15 to protect sensitive unclassified information from public disclosure.~~ FAA Order 1600.75 ~~Protection~~Protecting Sensitive Unclassified Information ~~provides both policy and guidance~~(SUI) is in effect.

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~~, establishes~~ 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.