CHANGE REQUEST COVER SHEET

Change Request Number: 13-96 **Date Received:** 11/4/2013

Title: AMS Section 4.11 Security Policy Update

Name: David Lankford

Phone: 202-267-8407

Policy OR Guidance: Policy

Section/Text Location Affected: Section 4.11

Summary of Change: Updates existing order numbers and adds a reference to new privacy policy.

Reason for Change: Several security policy changes have occurred since the 2009 update.

Development, Review, and/or Concurrence: A workgroup was empaneled at the direction of the AEB.

Target Audience: Acquisition Workforce

Potential Links within FAST for the Change: N/A

Briefing Planned: Yes

ASAG Responsibilities: Review and Comment

Potential Links within FAST for the Change: N/A

Links for New/Modified Forms (or) Documents (LINK 1)

Links for New/Modified Forms (or) Documents (LINK 2)

Links for New/Modified Forms (or) Documents (LINK 3)

SECTIONS EDITED:

Acquisition Management Policy:
Section 4.11 : Security [Old Content][New Content] [RedLine Content]

SECTIONS EDITED:

Section 4.11 : Security

Old Content: Acquisition Management Policy:
Section 4.11 : Security

The FAA must conform with national policy related to the 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. In addition, physical security applies to staffed facilities that the FAA leases, owns, and operates. For more information concerning physical security, see FAA Order 1600.69, FAA Facility Security Management Program, as amended.

Personnel security applies to all FAA positions and FAA employees, contractors, subcontractors, and other users of FAA information systems. Each position must be designated as to the level of risk in terms of suitability and access to FAA facilities, sensitive information, and/or resources, and also designated as to the level of sensitivity in terms of national security and public trust responsibilities related to the efficiency of the service.

The FAA is required by Executive Orders 13292 and 12968 to protect classified information from unauthorized disclosure. The FAA is also required by law to protect sensitive unclassified information from public disclosure. FAA policy for information security is found in FAA Orders 1600.2E and 1600.72A.

The FAA is required by law (PL 100-235, Federal Information Security Management Act, 2002 (FISMA)), OMB Circular A-130, and other federal standards to provide security for all information that is collected, stored, processed, disseminated, or transmitted using FAA or non-FAA-owned information systems. Information system security (ISS) requirements must be integrated into each phase of a program's lifecycle (see ISS system process flowchart). The acquisition program baseline and planning documents for each investment program must include the cost of complying with national security policy and must allow sufficient time for compliance. FAA ISS program policy is contained in FAA Order 1370.82A (FAA only), as amended. This order supersedes FAA Order 1600.54B (FAA Automated Information Systems Security Handbook).

New Content: Acquisition Management Policy:
Section 4.11 : Security

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, facility, 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 Act, 2002 (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. 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. Investment programs should consult the Security Authorization Handbook and coordinate with the ISS manager for their line of business at each 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 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 Information and Personally Identifiable Information Policy

The FAA is required by Executive Orders 13526 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 Sensitive Unclassified Information provides both policy and guidance.

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 both the policy and guidance. In addition it establishes the position of FAA Privacy Officer with respect to information technology.

Red Line Content: Acquisition Management Policy:
Section 4.11 : Security

~~The~~***Introduction***

Service ~~FAA~~***organizations and program offices*** must ~~conform with national policy related~~***allow sufficient time and resources*** to ~~the physical~~***address*** security ~~of~~***laws.*** ~~the~~***policies.*** ~~aviation infrastructure~~***and orders*** including ~~leased~~***the*** ~~and owned~~***cost of*** ~~facilities,~~***implementing*** ~~the~~***required*** security ~~of~~***controls*** ~~all information~~***into acquired*** ~~associated~~***components.*** ~~with operation of~~***Security policy within*** the FAA ~~and~~***is*** ~~aircraft~~***divided*** ~~operations~~***into information security; physical, facility***, and personnel security~~. The~~***; and*** ~~FAA~~***sensitive information and personally identifiable information. There*** is ~~also~~***overlap*** ~~obligated~~***between the disciplines (for example, physical security is employed*** to protect ~~proprietary~~***classified*** ~~information~~***materials), so all areas of security policy must be evaluated*** to ~~which it has~~***ensure full compliance*** ~~access~~***with the various orders and policies***.

Physical*Information* **security***Security* **is***Policy*

The directly applicable to aviation*Federal Information Security Management* industry*Act,* operations*2002 (FISMA), Office of Management* and activities*Budget Circular A-130, Management of Federal Information Resources*, *National Institute of Standards* and to*Technology* supporting*(NIST)* infrastructure*guidance,* such as communications*and other federal*, sensors*departmental*, and information*agency-level* processing.*guidance* In*and* addition*standards as amended*, physical*describe information system* security applies*(ISS) needed* to staffed facilities that*for all FAA information* the*systems.* FAA leases*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*, owns*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 operates*federal information processing standards*. For more information concerning physical*Because the NAS is* security*classified as critical infrastructure*, see FAA Order*NAS systems must* 1600*comply with additional ISS requirements as defined by Air Traffic Organization Policies*.69, *These ATO policies can be found on the* FAA*'s* Facility Security Management*Website under policy* Program,*and* as*guidance* amended*and are designated with the letters "JO"*.

Personnel*To* security*receive a* applies*successful* to*in-service decision,* all FAA positions and FAA*investment programs must* employees,*undergo* contractors,*a* subcontractors,*security authorization that assesses outputs* and other users*products against* of*mandatory security requirements. The security authorization process is defined in* FAA information systems*Order 1370*.*82,* Each position must*Information Systems Security* be*Program.* designated as*The Security* to*Authorization Handbook details* the level of risk in terms*process for compliance with ISS* of*requirements.* suitability and access to FAA*Investment programs should consult the* facilities,*Security* sensitive*Authorization* information,*Handbook* and/or resources,*coordinate* and also designated as to the level*with the ISS manager for their line* of sensitivity*business* in*at each* terms*phase* of national*the AMS lifecycle to ensure information* security *requirements* and public*related information* trust responsibilities*are included* related*in acquisition artifacts, and* to *ensure* the efficiency of the*investment program is* service*on track for a successful security authorization*.

Physical, Facility and Personnel Security Policy

The FAA is required by Executive*must conform with national* Orders*policy related* 13292*to physical security of the aviation infrastructure including leased* and 12968*owned* to*facilities,* protect*the* classified*security of all* information from unauthorized*associated with* disclosure*operation of the FAA and aircraft operations, and personnel security*.- The FAA is also required by law*obligated* to protect sensitive unclassified*proprietary* information from public*to which* disclosure. FAA*it* policy*has* for*access.* information*Physical* security is

found*directly* ~~in FAA Orders~~*applicable to aviation* ~~1600.2E~~*industry operations* and ~~1600.72A. The FAA~~*activities, ~~is required by law~~and to supporting infrastructure* ~~(PL~~*such* ~~100-235~~*as communications*, ~~Federal~~*sensors, ~~Information~~and information processing. FAA Order 1600.69, Facility* Security Management ~~Act~~*Program*, ~~2002~~*establishes* ~~(FISMA))~~*both policy and guidance for physical security.*

FAA Orders 1600.1, ~~OMB Circular~~*Personnel Security* ~~A-130~~*Program*, *establishes both policy* and ~~other federal~~*guidance for* ~~standards~~*FAA personnel security. In addition, detailed guidance* to ~~provide~~*implement personnel and physical* security ~~for all information that~~*with respect to contractors* is ~~collected,~~*in* ~~stored,~~*FAA* ~~processed,~~*Order* ~~disseminated~~*1600.72*, ~~or transmitted using FAA~~*Contractor and Industrial Security* ~~or~~*Program.*

Sensitive ~~**non-FAA-owned**~~*Information* ~~**information**~~*and* ~~**systems. Information**~~*Personally* ~~**system security**~~*Identifiable Information* ~~**(ISS)**~~*Policy*

The ~~requirements must be integrated into each phase of a~~*FAA is required by Executive Orders 13526 to protect* ~~program's~~ *~~classified~~* ~~lifecycle~~*national* ~~(see~~*security* ~~ISS system process~~*information from unauthorized* ~~flowchart)~~*disclosure*. ~~The acquisition program baseline and planning documents for each investment program must include the cost of complying with national security policy and must~~*Systems containing or processing classified data are managed by the FAA Office of Security and Hazardous Materials Safety in accordance with FAA Order* ~~allow~~*1600.2,* ~~sufficient time for~~*Safeguarding Classified National* ~~compliance~~*Security Information*. ~~-~~ *The* FAA ~~ISS program policy is contained~~*is also required under 49* ~~in~~*CFR Part 15 to protect sensitive unclassified information from public disclosure.* FAA Order ~~1370~~*1600*.~~82A~~ *75 Protection Sensitive Unclassified Information provides both policy and guidance.*

The Privacy Act of 1974 and the E-Government Act of 2002 (~~FAA~~*Public* ~~only~~*Law 107-347*), ~~as~~*mandate* ~~amended.~~*protection of an individual*&#~~160~~*8217*;~~This~~*s right to privacy and the prevention of unauthorized dissemination of* ~~order~~*personal* ~~supersedes~~*information.* FAA Order ~~1600~~*1280*.~~54B~~*1,* ~~(FAA~~*Protecting Personally* ~~Automated~~*Identifiable* Information, ~~Systems Security~~*establishes both* ~~Handbook)~~*the policy and guidance. In addition it establishes the position of FAA Privacy Officer with respect to information technology*.
