4.11 Security Revised 10/2016

4.11 Security Revised 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 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) 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 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. 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. FAA Order 1600.75 Protecting Sensitive Unclassified Information (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 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.