AMS CHANGE REQUEST (CR) COVERSHEET

Change Request Number: 15-20A
Date Received: 9/9/15
Title: Information Security Guidance for System Acquisitions (ISGSA)

Initiator Name: James Daum
Initiator Organization Name / Routing Code: NextGen Safety & Information Security Division / ANG-B3
Initiator Phone: 202-507-2259

ASAG Member Name: Hugene Fields
ASAG Member Phone: 202-267-1550

Guidance and Policy must be submitted with separate CR coversheets.

- ○ Policy

Or

- ○ Procurement Guidance
- ○ Real Estate Guidance
- ◉ Other Guidance

Summary of Change: The ISGSA provides guidance for investment initiatives at each AMS planning phase to ensure the identification of information security requirements are an integral part of the acquisition process of new systems/services, the technology refresh of existing ones, and the partial or full replacement of existing ones. The guidance identifies tasks, stakeholders, and the process for conducting the security risk assessments on which the security requirements are based, and it includes four templates to document the assessment results. In addition the security assessments facilitate: (1) the identification of information security risk for use in the cloud suitability assessment and as an input factor to determine the acquisition category category (ACAT), (2) the preparation of security cost and benefit factors for the investment analysis phase which in turn will help budgeting the implementation of the ISS requirements on the chosen alternative system solution, and (3) the prioritization of common controls over system specific controls whenever appropriate which will foster economies of scale and standardized security. Changes to the ISS Flowchart in FAST are also proposed to reflect introduction of the ISGSA.

Reason for Change: The ISGSA will fill an AMS gap: The lack of information security specific guidance in the AMS planning phases for the acquisition of new information systems/services and any new AMS investment on existing systems or services often times lead to the acquisition of systems with security that is not commensurate to their information security risk or a costly retrofitting of security safeguards during or after implementation. The changes proposed for the ISS Flowchart in FAST are necessary to reflect the ISGSA.

Development, Review, and Concurrence: The ISGSA has been developed by ANG-B3 in close consultation with an FAA cross-organizational group, the Acquisition Executive Board (AEB) Security Risk Work Group. The AEB Security Risk Work Group has: (1) provided input in the progressive development of the ISGSA and assessment templates, (2) provided review and comment of the product drafts, and (3) participated in the adjudication of concerns originated within and outside the group. Progress and concurrence of the AEB Security Risk WG has been reported to the ASAG and the AEB as part of the AEB and ASAG Security Risk WG status reports. The proposed changes to the ISS Flowchart have also been developed in consultation and with feedback from the AEB Security Risk Work Group.

Target Audience: Service organizations seeking to acquire new information systems or seeking to make AMS investment on existing information systems or services.

Briefing Planned: Yes.

ASAG Responsibilities: Review and comment.

Section / Text Location: Under the FAST section http://fast.faa.gov/Security.cfm, add a link for the ISGSA and an indented link for each of the ISGSA appendices as follows:

Information Security Guidance for System Acquisitions (ISGSA)
- Appendix 1 Risk Factors Assessment Template
- Appendix 2 Preliminary ISS Assessment Template
- Appendix 3 Initial ISS Assessment Template
- Appendix 4 Final ISS Assessment Template

Under the same FAST section, update the contents referenced by the link:
Information Systems Security Process Flowchart
(http://fast.faa.gov/flowcharts/grid_platform.cfm)
with the attachment: ISS_Process_Flowchart_CleanCopy.

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: None.

Attachments: nformation Security Guidance for System Acquisitions (ISGSA)
Appendix 1 Risk Factors Assessment Template
Appendix 2 Preliminary ISS Assessment Template
Appendix 3 Initial ISS Assessment Template
Appendix 4 Final ISS Assessment Template

ISS_Process_Flowchart_redlines
ISS_Process_Flowchart_Picture_redline

ISS_Process_Flowchart_final

Other Files: None.

Redline(s):

Section Revised: Flowchart ISS Platform

FAA Lifecycle Management Process Flowchart

Information Systems Security **(ISS)** Overview

~~**Security / Privacy Policy:**~~ The FAA is required by ~~law to provide security for its facilities, equipment, personnel,~~ federal laws and ~~information. The~~ regulations, e.g., the Office of Management and Budget Circular A-130 and the Federal Information Security Management Act ~~of 2002 and amendments (FISMA),~~ (FISMA), to provide security protections to information systems used or operated by the FAA, its contractors, or other organizations on behalf of the FAA. The protections need to be commensurate with the information security risk as determined by security assessments and they must be provided throughout the service lifecycle:

FISMA Clause 3544a
(a) IN GENERAL.—The head of each agency shall— ‘‘(1) be responsible for— ‘‘(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of— ‘‘(i) information collected or maintained by or on behalf of the agency; and ‘‘(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
FISMA Clause 3544b
*‘‘(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency wide information security program, approved by the (*OMB ~~Circular A-130, and federal government standards establish the extent of~~ *) Director under section 3543(a)(5), to provide* information security for ~~all agency~~*the* information *and information systems* that *support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— ‘‘(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency; ‘‘(2) policies and procedures that— ‘‘(A) are based on the risk assessments required by paragraph (1); ‘‘(B) cost-effectively reduce information security risks to an acceptable level; ‘‘(C) ensure that information security* is ~~collected, stored, processed, disseminated, or transmitted~~ *addressed throughout the lifecycle of each agency information system;*

Accordingly the FAA –using ~~agency or non-agency owned information systems or technology (IT). FISMA has assigned responsibility to the~~ National Institute of Standards and Technology ~~(NIST) to produce standards and guidelines for protecting government information and information systems. The Office of Management and Budget (OMB) has made NIST~~ guidance ~~mandatory for~~ and Department of Transportation policy –has established the FAA Information Security Program (FAA Order 1370.82) and supporting procedures to comply with these federal

~~agencies.~~laws and regulations in all information systems other than national security information systems. The procedures have been formulated in terms of security assessment templates and guidance which can be found in the Information Security Guidance for System Acquisitions (ISGSA) and the Security Authorization Handbook . The Security Authorization Handbook details the process for compliance with ISS requirements during the 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. The ISS assessments and other activities to carry out these procedures at each of the lifecycle management phases are summarized in the remainder of this document. FAA systems that qualify as national security systems are managed by the Security and Hazardous Materials Safety (ASH) organization according to FAA Order 1600.2 "Safeguarding Classified National Security Information" and their procurement are subject to FAA Order 1600.73 "Contractor and Industrial Security Program Operating Procedures".

~~FAA's national directives (orders and notices) and Acquisition Management System (AMS) as policy direct the implementation of these statutes and guidance. The FAA Acquisition System Tool (FAST) provides process-level guidance for the program office to implement those policies during acquisition of facilities, equipment, processes, services, and/or information. Workflow tasks below describe who does the work (Performer column), what the outputs are (Products column), who provides validation and verification (V&V) (Approver column) and reference to detailed guidance for security and privacy practitioners (Tools and Aids column). The tasks also provide a short description of the activity and its intended benefits or constraints at high level for the program office.~~

~~FAA Order 1370.82, Information System Security (ISS) Program and other orders in the national directives 1370 series establish the requirements for ISS including the acquisition, operation, decommissioning and disposal of information systems and their information including records retention requirements. The FAA Certification & Authorization (C&A) Handbook has been revised and retitled as the FAA Security Authorization Handbook and Templates. This Authorization Handbook and its line of business (LoB) interpretations provide the guidance for ISS staff to implement ISS policy in the 1370 Order series. The Handbook was needed separately from policy to apply rapidly evolving NIST and other government ISS guidance, reducing the need for frequent policy changes. The Authorization Handbook also incorporates privacy and contingency planning (previously, catastrophe / disaster recovery planning) requirements into ISS activities. This ensures that FAA systems processing, transmitting or storing privacy impact data are cost effectively protected from threats to confidentiality, integrity, and availability.~~

~~Systems containing or processing classified data are managed by ASH in accordance with FAA Order 1600.2, Safeguarding Classified National Security Information. In addition, many agency information systems process sensitive or personally identifiable information (S/PII). FAA Order 1280.1 establishes policy and guidance for the privacy program coordinated with FAA Order 1370.82 and the Authorization Handbook. S/PII is just one type of sensitive but unclassified (security) information that FAA uses and therefore stores, transmits, or processes. Sensitive security information is information that if disclosed, altered, forged, or rendered unavailable or unreliable, could adversely impact the ability of the FAA to perform its mission and result in any of the following (see FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI)):~~

- ~~Seriously inhibited system operation~~
- ~~Serious and widespread delays~~
- ~~Damage to the public perception of air traffic control~~
- ~~Expenditure of significant resources by the FAA or users to reestablish NAS operations~~

- Invasion of personal privacy
- Release of trade secret or privileged, confidential commercial , and/or financial information
- Be detrimental to the security of transportation
- Possible loss of life

FAA Orders 1600.1, Personnel Security Program, 1600.72, Contractor and Industrial Security Program, and 1600.69, Facility Security Management Program establish both the policy and guidance for personnel and physical security. In addition, detailed guidance to implement personnel and physical security with respect to contractors may be found in FAA Order 1600.73, Procedures for Contractor and Industrial Security. Many personnel and physical security controls are listed in the Authorization Handbook as part of the ISS controls that System Security Plan (SSP) prescribes. To accommodate the overlap efficiently, physical, personnel and cyber security together with Privacy have been incorporated into this composite security workflow within the AMS life cycle as they are combined in AMS policy paragraphs 4.11 (Security) and 4.13 (Risk Management - Security Risk Management).

Most investment programs have to rely on ASH to perform or acquire support such as guards to perform the physical and personnel security activities listed. Thus in the security workflow the performing agent will be listed as AIN or security staff with an ASH or facility manager approver. However, program office activities such as allowing / contributing to rapid contractor staff turnover has an unplanned workload impact on ASH, so physical and personnel security staff need to be informed or involved in decisions that affect facilities changes, equipment movement, and personnel changes, including those affecting what information that staff will need that will use or operate and maintain the program's solution.

The primary security document for an information system during its life cycle is the System Security Plan. The SSP provides an overview of the security requirements for an information system or a LoB's information security program and describes the technical, programmatic and administrative security controls in place or planned for meeting those requirements. The SSP for an organization-wide information security program also describes the program management controls for the information security program and identifies any common controls in place or planned to meet the program security requirements. A common control is a security control that is inherited by one or more organizational information systems from the environment or infrastructure. Many of the controls that protect FAA information systems (e.g., contingency planning, incident response, information security training and awareness, personnel security, physical security, environmental protection, and intrusion detection) are common controls. Economies of scale and elimination of duplication are achieved by centrally acquiring and managing common controls. Partitioning information security controls into common, hybrid, and system-specific controls results in more consistent application of information security across the Agency that may result in significant savings.

In most system or software application acquisition programs a contractor or team develops the solution to be deployed in one or more FAA data centers inside the FAA or NAS firewalls. The contractor has the technical details to complete many key sections of documents required by the Security Authorization process, but most of those documents also require significant amounts of FAA-specific information. That information can only be obtained from FAA Information Technology (IT) data center, network or ISS staff that knows what the operational environment provides in terms of common and hybrid controls for the system or application. The contractor team can only provide all of the documents when the system will be operated and maintained by a contractor for FAA in a non-government data center. The documents that are likely to have portions completed by the contractor include the System Characterization Document (SCD) that describes the system in its operational environment leading to a determination of how secure it must be, and the set of documents that depend on the SCD determination for the correct template to be used: the SSP, the Information System Contingency Plan (ISCP), the ISCP Test Plan and Recovery Report (TPR) and the Plan of Action and Milestones (POA&M). It is unlikely that a contractor could efficiently make arrangements to obtain inter-system connection agreements, or required signatures that the Program Office can obtain by asking.

For additional information regarding ISS policy and guidance, contact the Office of Information Systems Security (AIS-1) or your LoB information system security manager (ISSM): https://intranet.faa.gov/faaemployees/org/staffoffices/aio/partnerships/issm/

For additional information on privacy requirements or the handling of privacy data, contact the Privacy Office (AIO/AES).

For additional information on physical or personnel security or the handling of classified information, contact the Office of Security and Hazardous Materials Handling (ASH-1), or your local facility or personnel security officer.

Improving Security: Security is a dynamic process, not just a set of products. The environment is constantly evolving due to changes in threats and protection mechanisms. The FAA must maintain awareness of threats, attack vectors, newly discovered latent flaws, remediation (fixes), guidance from vendors and federal agencies, commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products, and special needs of special purpose systems, such as the National Airspace System (NAS). General-purpose, mass market IT and facilities products and services are mostly acquired, in part or whole, from external sources and their personnel. Industrial Control Systems (ICS) such as those used in the NAS require additional caution in applying products and services that can result in adverse impact to the ICS, and therefore, FAA mission. Acquiring and maintaining products and services that support cybersecurity strengthen the Agency's mission assurance posture, transfer or mitigate risk, and reduce overall operational and maintenance costs; however, there are risks associated with the global supply chain (e.g., commercial outsourcing of software development and remote access) that can adversely impact the security of the Agency's information systems.

The FAA has adopted a disciplined process for its acquisitions, including a system development life cycle (SDLC), that manage the impact to critical mission and business operations by ensuring security requirements are designed into, developed, implemented, and maintained throughout the acquisition lifecycle. The objective is that FAA IT systems operate as intended, that software defects are minimized and remediated expeditiously, and configuration changes are managed in an efficient and timely manner. By integrating security activities into all phases of the acquisition life cycle, program managers will not only ensure the security and resiliency of the FAA information systems and facilities; but also save costs associated with evolving security threats during in-service management. Constant attention to security is required because characteristics of attacks evolve; discovery and exploitation of latent flaws occurs in shorter time frames; the unauthorized flow of information from government computer systems to destinations in countries known to be hostile (exfiltration) occurs undetected without impacting current operations, but potentially setting the stage for future attacks. Security investments can also result in cost avoidance (insurance aspect) and savings (not having to pay for some requirements) from;

- Program alternative solutions analysis comparisons
- Taking advantage of economy-of-scale security in the FAA infrastructure instead of developing and validating equivalent security mechanisms
- Leveraging results from external sources; and employing known-secure GOTS and COTS products and services.

Service-Level Analysis (including aspects of Research for Service Analysis)

Physical, personnel, and information system security (ISS) and privacy are each service areas (SA). Each SA engages periodically, or as indicator events occur, in a service analysis as described in the service-level analysis of AMS. Using strategic planning methods, the strengths and weaknesses of the service-level analysis as it exists are examined, as well as the opportunities and threats that direct both the immediate and the long-term environment, technology, processes and people skills needed by each SA. Other activities or the development of non-security focused new programs may also identify security-related opportunities or threats.

Those security needs that are deemed significant due to urgency or importance are proposed as activities in the annual processes that result in the EA roadmaps and Destination 2025. The security service area needs must be prioritized, time-phased, and integrated with the other FAA service area needs. This is the annual business planning work. The security SA

analysis and business planning result in approved security activities that are in the FAA strategic or business unit plans in part or whole, funded or unfunded. At this point the activity becomes synonymous with a candidate project or program.

The deliberations about technology and methods include a dialog with the enterprise architecture (EA) staff about how the needs can be represented best in the EA. The conceptual solution for those security needs that become plan activities are then described as security service gaps and their outputs or outcomes are added to the SA's or its business unit's to-be enterprise architecture and roadmap. The SA executive alerts the appropriate governance bodies to the impending project or program as part of the decision to enter Concept and Requirements Definition (CRD). An ISS security architecture that is consistent with the EA describes the procedures and mechanisms for implementing and maintaining cyber security controls. While the service-gap analysis process is applicable to define economy-of-scale, program level solutions for common security needs, the highly dynamic nature of the cyber security space requires that problems and solutions often be identified and implemented within the annual service analysis cycle.

The service analysis need description indicates questions to be addressed by the Research for Service Analysis (RSA) activities. An RSA activity may include concept exploration, development and/or evaluation activities. In concept exploration, typically a capability survey identifies state-of-the-art and state-of-practice policies, procedures, products, and systems available within both public and private environments that can provide economy of scale and direct security benefits to FAA in the long and mid-term investment horizons. The cognizant security SA management reviews and determines if any of the COTS or GOTS products and/or changes in policies and procedures might provide solutions to FAA security gaps while providing sufficient risk reduction, security cost savings, or large enough security benefits in specific situations to merit investment. If a product or service is not sufficiently mature to incorporate immediately but offers sufficient promise, the security SA executive proposes a Research Engineering and Development (RE&D) program to investigate the product(s) as security environment, technology, process or skills solution for FAA adoption. Common controls receive special attention because of their potential for economies of scale, elimination of duplication, and significant savings in implementation and assessment costs as well as a more consistent application of the information security controls across the FAA. Common control RSA activities may be conducted within a single LoB, a combination of LoBs, or by AIO as an FAA ISS program activity. If the RE&D project or pilot indicates appropriate benefits are likely, the security SA may request additional RE&D or facilities and equipment (F&E) funds, or apply its own operations funding to mature the solution as appropriate. The pilot project provides not only an adoptable, affordable, life-cycle, security solution; but also a technology insertion plan that describes how the solution will be deployed, operated and sustained. The project or pilot staff keeps the LoB EA staff informed for the purpose of updating the products and dependencies between them in the to-be EA, roadmap and the ISS Architecture. The actual solution deployment may occur during one or more other investment programs' solution implementation phases or during in-service management as a preplanned product improvement depending upon allocation of resources.

ISS activities during Service Analysis (SA)

During service analysis, the service organization identifies a service or capability shortfall and prepares a preliminary shortfall analysis report as a first step toward validating an investment initiative as an agency priority. Additionally, the service organization must assess the information security risk factors for those service or capability shortfalls with an information service component. A service or capability shortfall is said to have an information service component if the service need is concerned with sending, receiving, processing, or storing operational information. If the information service component is uncertain during service analysis, the information risk assessment may be postponed to concept and requirements definition once the nature of the shortfall becomes clear.

Perform the ISS Risk Factors Assessment**

Responsible Agent	Products	Approval Authority	Tools and Aids
• Service organization investment initiative lead • Service organization security lead*	• Provisional Security Category • Provisional Security Threat Profile • Preliminary Capability Description	• The originating organization Authorizing Official Designated Representative	• The Information Security Guidance for System Acquisitions (ISGSA) • The ISS Risk Factors Assessment Template

Description:

The ISS risk factors assessment is the basis for determining the provisional security category and threat profile. It is a precursor to the CRD readiness decision, and must be prepared using the ISGSA, the ISS risk factors assessment template, and information prepared separately by the service organization for the preliminary shortfall analysis report. The products of this assessment are provisional because of the limited and preliminary nature of the information available, but they are necessary inputs to the cloud suitability assessment performed by the Enterprise Infrastructure Services (EIS).

*Each organization will follow FAA policy and internal procedures to select an information security lead.

** Not all investment initiatives require this assessment; the requirement criteria are found in section 3.5 of the ISGSA.

ISS activities during Concept & Requirements Definition (CRD~~), (including aspects of RSA~~)

~~During the RE&D activity (initial, project, or pilot), the security SA management or program management keeps the LoB EA staff informed, who in turn, update the to-be EA and roadmap security activity within programs. This continues during the CRD when the solution concept of operations, preliminary requirements, and initial alternative solution candidates are defined. For investment programs that provide systems, ISS requirements derive from the system categorization described in the FAA Security Authorization Handbook. The initial System Security Plan (SSP) and Information System Continuity Plan (ISCP) are developed in accordance with the FAA ISS Authorization Handbook. The SSP and ISCP are updated throughout the investment life cycle. Depending on the solution concept's security categorization and representation in the EA, the investment program will incorporate infrastructure safeguards and countermeasures leaving only system-specific or hybrid security~~

~~requirements for the program to implement. At the end of the CRD, a complete set of potential security requirements and controls based upon the system categorization is fully described and annotated in the system SSP. For investment programs that provide common controls as systems or services, the SSP contains a functional description of the common control (including planned inputs, expected behavior, and expected outputs), an implementation plan, and plans for continuous monitoring and periodic assessments of common controls carried out by qualified assessors with an appropriate level of independence. SSPs are approved or disapproved by the cognizant, authorizing official (AO), who determines whether these plans are complete, consistent, and satisfy the information security requirements for the investment program and the FAA.~~

~~During CRD physical security needs to be kept informed of likely facilities and location in facilities changes that might affect security in order to update facility security assessment documentation. Personnel security needs to be informed of changes in personnel number (federal employees and contractors) to plan for badging and FAA IT accounts. If there is concurrent large-scale hiring anywhere in government, competition for security resources can cause delays of weeks. Some changes in qualifications for personnel at sites change the security clearance required. Background checks cost thousands of dollars and can take four months, so early alert to personnel security is a win-win action for programs.~~

During CRD, the service organization determines what functional and performance requirements must be satisfied in order to resolve the service shortfall or opportunity and identifies which alternative solutions will be evaluated during initial investment analysis.

A definitive shortfall is established as the service organization puts forward a final shortfall analysis report, a solution concept of operations, and other supporting documents such as a functional analysis and the Enterprise Architecture connectivity (OV-2) and information exchange (OV-3) views. As these documents are prepared and completed, the service organization should be able to determine whether the shortfall has an information service component, if it was not able to do so during the service analysis. If the service shortfall has no service information component, the investment initiative will not require an ISS assessment; otherwise the service organization will perform the preliminary ISS assessment during CRD.

Perform the Preliminary ISS Assessment

Responsible Agent	Products	Approval Authority	Tools and Aids
• Service organization investment initiative lead • Service organization security lead*	• Final Security Category • Final Security Threat Profile • Partially tailored ISS requirements • The ISS cost and benefit factors	• The originating organization Authorizing Official Designated Representative	• The Information Security Guidance for System Acquisitions (ISGSA) • The ISS Risk Factors Assessment Report • The Preliminary ISS Assessment Template

Description:

The preliminary ISS assessment is one precursor to the investment analysis readiness decision. It is prepared using the ISGSA, the preliminary ISS assessment template, the ISS risk factors assessment report, and other information prepared separately by the service organization. The products of this assessment include: (1) a set of ISS requirements for inclusion in the preliminary program requirements document (pPRD); (2) final security category and the security threat profile; and (3) the factors for estimation of ISS cost and benefit.

- The ISS requirements in the pPRD will be used: (i) to document which requirements are met

and which are not met by each alternative solution, and (ii) by the Enterprise Infrastructure Services organization to assess the telecommunications/network, SWIM, and cloud services for each alternative.

- The security category and the security threat profile are inputs to the acquisition category determination request. In addition the security category is used to select (or confirm) the NIST SP 800-53 requirements baseline.
- The ISS cost and benefit factors are input to the range of alternatives report and are used during investment analysis to evaluate the costs and benefits of each alternative solution.

For some investments, this assessment may be omitted or postponed and performed in conjunction with the ISS assessment for the next AMS decision gate as prescribed in Section 3.5 of the ISGSA.

*Each organization will follow FAA policy and internal procedures to select an information security lead.

ISS activities during Initial Investment Analysis (IIA) ~~and Final Investment Analysis (FIA) (including aspects of RSA)~~

~~During Initial Investment Analysis several alternative ways to address the service gap to be satisfied by the investment program are analyzed. The consequences for security of each alternative are input elements to the analysis to find the best option. The ISS, physical and personnel risk analysis results and associated cost estimates to address security requirements for each alternative are necessarily high level, but must be rigorous enough to describe the potential benefits and prevent significant cost and schedule impacts if the alternative is selected for implementation.~~

~~During Final Investment Analysis, the recommended solution's security requirements are allocated to the environment / infrastructure as common controls, and to facilities, personnel and the to-be-developed system in the final requirements document and associated configuration management documentation as specific or hybrid controls. Common controls may be technical, management, or operational security controls employed within and inherited by the information system in accordance with the ISS architecture. Physical and personnel security controls are generally common controls provided by ASH or the operating LoB. Their costs are estimated in the planning and risk management documents. As part of investment analysis, costs for common controls may be allocated by the applicable FAA investment board to the specific investment program, or to the common control program separately. A final risk analysis for the recommended solution is completed and both the SSP and the ISCP are updated. The security EA and roadmap entries are also updated as investment decisions are made by the applicable FAA investment board.~~

~~Solution Implementation (SI)~~

~~During solution implementation, security requirements are realized with the rest of the system. Feedback on the security requirements is provided to the solution developers by independent assessors, design plans (including the SSP and ISCP) are updated, and the result is approved by the AO. Requirements may be implemented by facilities construction or renovation; personnel skills via training, hiring or contracting; hardware; software; infrastructure or other environmental components. Security experts, who are independent assessors, review design plans in the SSP and as-built documentation as part of validation and verification (V&V) for the program. During and at the end of the solution implementation phase, security compliance activities determine if the solution is compliant with applicable Federal, DOT, and FAA policy, standards, and requirements. When solution implementation is complete, the AO makes the determination whether the implementation conforms to FAA Order 1370.82, and Policy and Authorization Handbook standards, meets the protection needs, reduces residual risk to an acceptable level based on assessment report, plan of action and milestones (POAM), and other inputs. Based on the AO determination, the site manager or LoB executive approves a facility or system for operations and the SSP and ISCP are updated.~~

~~In-Service Management~~

~~During in-service management, security activities focus on continuous monitoring, flaw remediation, configuration management (change control activities), conducting security impact analysis for system/environment changes, and the assessment of selected security controls that support continuous authorization. Security activities address changes to the fielded asset (new functions and updates such as the latest version of a data base) and its environment (e.g., the asset is relocated to a different facility) and monitoring for security vulnerabilities to support near real-time remediation activities. In some instances, economy-of-scale add-ons or pre-planned upgrades are deployed to address functional and security requirements results from existing and new threats. Assessments are conducted depending upon those controls identified in the results of the security impact analysis (SIA). Compliance reviews also support continuous monitoring as part of the in-service management activities by serving to remind operations of the evolving nature of threats and vulnerabilities to the investments for which they are stewards. The SSP, ISCP, and facilities security plans are updated, and new action plans for facilities, and plans of action and milestones (POA&M) monitor vulnerabilities and their remediations. These physical / personnel security action plans and POA&Ms become a part of operational plans and budgets.~~

~~Towards the end of the useful life of an investment as well as periodically during ongoing operations and maintenance, the operating organization reviews the plans for real property, media and equipment disposal upon termination. System media containing sensitive, especially privacy, or classified data must be appropriately disposed of by erasure or destruction. Facilities and equipment containing hazardous material or in areas requiring special handling for removal may exceed estimated costs from investment analysis causing operational problems. The requirement to dispose of obsolete and decommissioned facilities and equipment must be addressed in the cost-benefit analysis for new or replacement investments.~~

~~The following security activities are executed during the AMS lifecycle management.~~

~~Perform Security / Privacy Service Analyses~~

During initial investment analysis, the various alternatives are evaluated comparatively for cost, benefits, risk, schedule, and other relevant factors to identify the best overall solution given funding constraints and operational need. During IIA, the service organization will complete the tailoring of the security controls baseline and define the ISS cost and benefit factors as part of the initial ISS assessment.

Perform the Initial ISS Assessment

Responsible Agent	Products	Approval Authority	Tools and Aids
• Service organization investment initiative lead • Service organization security lead*	• Fully tailored ISS requirements • Cost and benefit factors applicable to each alternative	• The originating organization Authorizing Official Designated Representative	• The Information Security Guidance for System Acquisitions (ISGSA) • The Preliminary ISS Assessment Report • The Initial ISS Assessment Template

Description:
The initial ISS assessment is a precursor to the initial investment decision. It is prepared using the ISGSA, the initial ISS assessment template, the preliminary ISS assessment report, and other information prepared by the service organization. The products of this assessment include: (1) a set of fully tailored ISS requirements for inclusion in the initial program

requirements document, and (2) updated factors for the estimation of ISS costs and benefits the basis for preparing the business case of each solution alternative.

- ISS requirements in the iPRD will be used: (i) during the evaluation of each alternative solution to document which ISS requirements are met and which are not, (ii) as an input to the initial screening information request for a market capability survey, and (iii) by Enterprise Infrastructure Services to assess the telecommunications/network, SWIM, and cloud services for each solution.
- The updated ISS cost and benefit factors are input to the business case analysis which will determine the ISS costs and benefits of each alternative solution.

For some investments, this assessment may be omitted or postponed and performed in conjunction with the ISS assessment for the next AMS decision gate as prescribed in Section 3.5 of the ISGSA.

*Each organization will follow FAA policy and internal procedures to select an information security lead.

ISS activities during Final Investment Analysis (FIA)

The objective of final investment analysis is to mature the proposed investment into a low-risk, well-planned investment program ready for solution implementation. During FIA, the service organization finalizes security requirements in the fPRD based on vendor responses to the screening information request and any changes in funding. Finalized ISS requirements and updated ISS cost and benefit factors are also inputs to the solution implementation planning process.

Perform the Final ISS Assessment

Responsible Agent	Product	Approval Authority	Tools and Aids
~~Physical security staff~~ ~~Personnel security staff~~ ~~Cyber security and Privacy staff~~ ~~IT (AIO) and NAS Enterprise Architect security architecture delegates~~ • Service organization ~~planning staff~~investment initiative lead ~~LoB/SO program management staff~~ • ~~Non-security programs or staff that identify a new security requirement~~	~~Physical Security shortfall analysis~~ ~~Personnel Security shortfall analysis~~ ~~Information System Security and Privacy shortfall analysis~~ ~~Security shortfall-solving programs & inter-dependencies listed on a roadmap and in supporting ISS Architecture~~ • ~~Work plans for concepts to enter CRD~~Final ISS requirements • Revised ISS cost and benefit factors	~~Assistant Administrator for Security and Hazardous Materials (ASH-1)~~ ~~Chief Information Security Officer (AIS-1). FAA CIO. CIO Council and ISSM forum~~ ~~Chief Privacy Officer~~ ~~LoB CIO. ISSM or senior LoB ISS official~~ • ~~Service~~The originating organization ~~and LoB executives~~Authorizing Official Designated Representative	~~AMS Service Analysis section~~ ~~AMS Enterprise Architecture section~~ ~~Annual EA and roadmap guidance~~ • ~~FAST process for Research for Service Analysis description and templates for outputs~~The Information Security Guidance for System Acquisitions (ISGSA) • The Initial ISS Assessment Report • The Final ISS Assessment Template

~~or capability~~Service organization security lead*			

Description:

~~Annually, the FAA Chief Information Security Officer (CISO), who is also the director of the Office of Information Security (AIS), ASH-1, or the LoB senior ISS official establish small teams to perform a service-level analysis for their respective types and scopes of security. The service-level analysis identifies long-range security risks requiring identification of potential solutions, and also considers customer and operational measurements about the value and quality of operational facilities, personnel, and systems to determine which will need replacement, renovation or refresh, retirement or in some cases re-use. The security service-level analysis describes the security needs to address currently applicable federal policies and standards and those expected in the near future. The analysis also identifies security needs in operational FAA systems in terms of the effectiveness of security controls that do not satisfy FAA security policy, and recommends which needs should be addressed in the short and long term. The information system security (ISS) service-level analysis report is coordinated with the CIO Council and ISSMs. Personnel and physical security needs are coordinated by the Assistant Administrator for Security and Hazmat (ASH-1) and the affected LoB executives.~~

~~Those security needs that are deemed significant due to urgency or importance are proposed as activities in the annual processes that result in EA roadmaps and Destination 2025. Security service needs must be prioritized, time-phased, and integrated with the all of the other service needs of all of the FAA service organizations. This is the annual business planning work by FAA. The CSPI results in approved security activities that are in the FAA strategic or business unit plans in part or whole, funded or unfunded. At this point the activity becomes synonymous with a candidate project or program.~~

~~Those security needs that become plan activities are then described as security service gaps and their outputs or outcomes are added to the service organization or its business unit's enterprise architecture (EA) and roadmap. The information technology (IT) and/or National Aerospace System (NAS) enterprise architects use the results of the security service analyses and any corresponding R&D to update the to-be EA and annual roadmaps with security-related products and services. Identification on a roadmap is required for an investment to be funded whether paid for by capital facilities and equipment or operating funds.~~

~~The SO or business unit's program management staff develop a draft business case at the appropriate level of detail for the Acquisition Category (ACAT) of those activities in the plan. The SO or LoB planning or program management staff also documents an appropriate level of detail plan for each activity that passes the readiness gate to enter the Concept and Requirements Definition (CRD).~~

~~FAA programs or SO's may identify new concepts (systems and/or services) that are not captured in the FAA strategic plan or EA. Concepts may originate from external organizations (e.g., OMB, NIST). A concept document, separate from the analysis performed by personnel, physical, or information security organizations, may be generated that identifies how this new concept impacts security either in the relationships between systems or in the NAS's or FAA's overall ability to provide services.~~The final ISS assessment is as a precursor to the final investment decision. The assessment must be prepared using the ISGSA, the final ISS assessment template, the initial ISS assessment report, and other information prepared by the service organization. The products of this assessment include: (1) final ISS requirements for inclusion in the final program requirements document, and (2) any updated factors for the estimation of ISS costs and benefits.

The products of this assessment are also used to support: (i) the solicitation and evaluation of

offers from industry for the solution selected by the JRC for implementation, and (ii) preparation of the acquisition program baseline, in-service review checklist, implementation strategy and planning document, and system security plan.

*Each organization will follow FAA policy and internal procedures to select an information security lead.

Perform Security / Privacy Service Analyses

Perform Security Assessment During Research for Service Analysis

Responsible Agent	Product	Approval Authority	Tools and Aids
Security systems engineer Research & Development (R&D) teams	Survey of state of the art/practice security policies (both private and public sources) Survey of state of the art/practice security technologies (both private and public sources) (Option) A report on R&D project results (Option) Adapted or improved security products ready for deployment	AIS-1 for ISS service gap and R&D ASH-1 for physical and personnel security service gap and R&D LoB Security programs FAA Chief Privacy Officer for privacy-related studies and products (Jointly for joint application products)	AMS Research for Service Analysis section FAST process for Research for Service Analysis description and templates for outputs

Description:

If a significant security service need has been identified, ASH-1, AIS-1, or the LoB senior ISS official commissions a concept exploration, and then if successful, development and/or evaluation set of studies. Concept exploration may be accomplished by abstract methods, modeling, or a survey of the state of the art and state of practice policies, procedures, systems, and services that identify the gap between current security posture and that required currently or in the future. The study compares and contrasts state of the art and state of practice products against the service need. If a combination of one or more products, services, policies, or procedures surveyed is, or can be, adapted or improved to satisfy an appropriate set of the gap requirements, then the concept exploration report may be used as basis of a request for a research engineering & development (RE&D) project to verify that the product, service, policy, or procedure, as is, adapted or improved, can be provided cost-effectively. Depending on the results of the RE&D project, a further RE&D project may be commissioned to mature the product(s) or develop additional products needed to transition the product(s) into practice. The information emerging from RSA has global impact rather than being specific to a single facility or equipment program. The information may initiate a program to develop a security solution for FAA, or provide a design or component solution to incorporate into other programs' solutions.

Other service organizations (both security and non-security) may also identify a new product, service, policy, or procedures that address a service gap. One of these programs or organizations may also perform a survey of the current security environment. This survey, just as those commissioned by ASH or AIS, may be used as the basis for an RE&D project

Perform Security Assessment During Research for Service Analysis

Draft Security / Privacy Categorization, Requirements and Plans

Responsible Agent	Product	Approval Authority	Tools and Aids
Local physical and personnel security staff or AIN-100 and AIN-400 LoB or Program security systems engineering (SSE)	Initial System Characterization Document (SCD) (Security Categorization) Initial security requirements Initial I System Security and Contingency Plans (SSP, ISCP) Privacy Threshold and if needed, Impact Assessment (PTA/PIA)	AJP (NAS) or ARD-300 Systems Engineering (security requirements) Receiving LoB ISSM, security authorization team, and senior ISS official (review of security categorization, requirements, SSP and ISCP) Chief Privacy Officer or delegate (review PTA/PIA) Optional: if recommended controls include unique personnel or physical security concepts, then ASH-1 assigns review and approval staff	FAA or LoB Security Authorization Handbook and Templates

Description:

The program office for all investments for facilities or major movement of equipment within them must include local or AIN-100 physical security review at each AMS Phase gate as part of validation & verification (V&V) to assist their planning of facility inspections.

The program office for all investments in equipment (IT or other) that have the potential to add new or change the knowledge or skill requirements of current users or maintainers must notify local personnel security or AIN-400 for review to see if federal or contractor personnel security requirements will change as a result, and to aid Security Office planning for federal and contractor clearances, badging and IT accounts.

The information systems security (ISS) baseline for a technology investment evolves from the initial security categorization of the information systems solution by the program or LoB SSE and ISSO or ISO. Then the SSE and ISSO ensure that FAA and LOB/SO ISS policies and standards are addressed in the preliminary security requirements as part of the security control tailoring process. At this stage, security requirements may be high-level and incomplete. The SSE also initiates and documents a security risk assessment and documents all progress in the initial information systems Systems Security Plan (SSP) and/or IS Contingency Plan (ISCP). The FAA or LoB Security Authorization Handbook and Templates provide guidance for tailoring of security controls and content / format of the System Characterization Document (SCD), SSP, ISCP, and Risk Assessment Report. It also provides a link to the privacy web site for the PTA and if needed, PIA. If the FAA privacy officer determines that the solution will create, store, transmit, or process sensitive personally identifiable information (S/PII), then a Privacy Impact Assessment (PIA) must also be completed.

The security controls for a system are tailored depending upon:

- S/PII Confidentiality Impact Analysis
- Availability of Common and Hybrid Security Controls provided by the Infrastructure and/or hosting facility, including

tailoring to address any Industrial Control System (ICS) system components

- The anticipated user community (e.g., FAA users only or other government or non-government users) and stakeholders (including representatives of FAA and other connected information systems or facility residents if shared with FAA)
- Types of technologies to be considered for use (e.g. wireless)
- E-Authentication Risk Analysis related to Electronic Government Act, if applicable
- Acquisition of COTS, GOTS, or outsourced products or services
- Risk assessment based in large part on environmental factors, including interconnections to FAA Telecommunications Infrastructure and other information systems

Draft Security / Privacy Categorization, Requirements and Plans

Perform Initial Risk Analysis for Alternatives and Update ISSP and ISCP

Responsible Agent	Product	Approval Authority	Tools and Aids
Program or LoB Systems Security Engineer (SSE) ISO/ISSO of the intended operating office or service unit Local physical and personnel security staff or AIN-100 and AIN-400	Security Risk Assessments of alternative solutions	LoB/SO ISSM. Senior ISS official AIN-1	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates

Description:

As part of the development and evaluation of solution alternatives, systems engineering develops the system architecture and technical description of hardware, software, communications, and interfaces for each alternative in sufficient detail to allow the SSE to identify potential vulnerabilities requiring security controls.

Common and hybrid controls may be technical, management, and operational security controls employed within and inherited by the information system in accordance with the existing or newly defined ISS Architecture. Physical and personnel security controls are generally common controls provided by ASH or the LoB. Their costs are estimated in the planning and risk documents.

Facility and personnel security staff review each alternative and current description of facilities and personnel that would be affected by the solution if the alternative were selected. They determine the impacts on security and provide rough cost, schedule and security value estimates for the alternatives as input to the alternatives analysis. If all alternatives have basically the same impact, the physical and personnel security analysts may simply indicate that there is no security preference for or against an alternative.

Evaluating and documenting the information system security risks of each alternative solution involves the following steps:

- Vulnerability assessment
- Risk assessment

- Risk mitigation planning
- Residual risk assessment
- Cost and schedule estimation of tasks to acquire/implement safeguards and countermeasures

These steps are conducted to the appropriate level of detail sufficient to have confidence in the capability of each alternative solution to meet ISS requirements. The steps include coordination with the systems engineering staff to ensure program staff has appropriate input to compare with other data in the alternatives analysis. Cost, performance, and if useful schedule program impact estimates are prepared for each alternative to determine the most efficient and effective means to achieve security safeguards and countermeasures.

Perform Initial Risk Analysis for Alternatives and Update ISSP and ISCP

Perform Risk Analysis for Recommended Solution and Update SSP and ISCP

Responsible Agent	Product	Approval Authority	Tools and Aids
ISO/ISSO of the intended operating office or service unit Program or LoB Systems Security Engineer (SSE) Local physical and personnel security staff or AIN-100 and AIN-400	Updated SSP and ISCP Final Information System (including Privacy), physical, and personnel security requirements update to Final Requirements Document Updated Acquisition Program Baseline and program planning and risk management documents Updated Risk Assessment Report	Program systems engineering Program manager or delegate for cost / schedule LoB ISSM or senior ISS official	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates

Description:

The Final Requirements Document (FRD) includes the security requirements that will be satisfied during solution implementation. Security costs and schedule for activities during solution implementation.

As part of the investment analysis, costs for common controls may be allocated by the applicable FAA investment board to the specific investment program, or to the common control program separately.

An updated Risk Assessment Report and plan of action and milestones (POA&M) identify any remaining ISS risks that will not be protected. These residual risks are explicitly acknowledged and accepted by the system's LoB authorizing official at the final investment decision. The residual risks are identified in the SSP, and are candidates for preplanned product improvements, environmental modifications, and platform, infrastructure or common service upgrades.

Program systems engineering must include residual security requirements in the System Specification to allow vendors to bid system designs that meet these requirements as part of acceptance criteria (best-value award) by the FAA. If so, satisfaction of these residual requirements must be identified as an evaluation factor in the Screening Information Request. ISS requirements met by other NAS or infrastructure systems, such as networks, servers and workstations, are annotated and

~~then omitted from the specification.~~

~~As part of contracting, the COTR must coordinate program or operations management and security (ISSM and facility / AIN-100 staff) to ensure that contractor staff have access to, and only to, those FAA systems and facilities for which they have routine need-to-know or need-to-go. One of the most expensive and highest potential risks to security is unnecessary access to FAA assets by unverified personnel. In addition, closing out terminated contractors' access to systems and facilities can be difficult and time-consuming for COTRs, program / operations personnel who may have to be queried, security staff and system administrators.~~

~~Perform Risk Analysis for Recommended Solution and Update SSP and ISCP~~

Provide Risk Feedback on Design

Responsible Agent	Product	Approval Authority	Tools and Aids
Security systems engineer ISO/ISSO of the intended operating office or service unit LoB Privacy Officer AIN-100 (facility) and/or AIN-400 (personnel) security staff	Feedback as to compliance with security requirements and consequences of any non-compliance of the design of the program IT or facility solution Updated SSP and ISCP	Program Change Control Board with input from SMEs LoB ISSM or senior ISS official	FAA Order 1600.72, Contractor and Industrial Security Program FAST Validation & Verification process and templates FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates

Description:

If any contract involves provision of IT services and products to FAA or requires contractors to use FAA IT resources, the SSE and ISSO evaluate each contractor's security authorization documentation to provide risk input to the selection process. The winning proposal may not be capable of satisfying all physical, personnel, privacy and ISS requirements in the SOW. In that case, the program office in consultation with the LoB ISSM and SSE negotiates and determines the changes in the SSP and program plan to build in alternative safeguards or countermeasures.

If the contract requires the vendor to develop or acquire software for the FAA, then the contract must contain government acceptance criteria ensuring compliance with all applicable FAA security and privacy policy, standards, and requirements including cooperation with the receiving LoB security program for software security assurance (application vulnerability scanning and remediation). These criteria include independent verification and validation of the vendor's development, test, and product operational environments throughout system life cycle to include initial authorization, associated documentation, continuous monitoring, and related activities to support FISMA reporting. The contract must also specify that vendor must cooperate with the LoB program during ISS compliance review, including software assurance activities.

External IT service providers must demonstrate that their operations will not degrade the security posture of the FAA before they initiate operations for FAA. That is, they must consent to compliance reviews as specified in the contract, MOA/SLA or other security interconnection agreement. The requirement for independent assessment in the V&V of the contractor's development, test, and production environments must be part of the contract and agreed to in bidder proposals.

If the FAA security program (cyber, physical or personnel) has developed environmental protection, technology, or methods in the RSA phase for the security service area that positively affects the authorization of the facility, system or application resulting from an investment program, then the program office and contractor must either include the improvement in its design and construction of the investment output or show in a cost-benefit analysis that it is not cost-effective to do so.

Provide Risk Feedback on Design

Provide Risk Feedback on As-Built

Responsible Agent	Product	Approval Authority	Tools and Aids
Independent assessment team Security systems engineer/test staff AIN-100 (facility) and/or AIN-400 (personnel) security staff LoB/SO ISS security staff (ISO/ISSO)	Updated SSP, including POA&M, ISCP, PTA/PIA Facility/Personnel Security Assessment Risk Assessment Report ISCP Test Plan and Recovery Report (TPR)		FAA Order 1600.72, Contractor and Industrial Security Program FAST Validation & Verification process and templates FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates

Description:

Any changes to an information technology configuration item description during solution implementation will be documented in the SSP, SCD, and in any other appropriate security documentation.

The program will obtain qualified independent assessors to act as V&V agents (testers) for program solution in-process construction / development tests. Coordinated with the program schedule, they will in part assess compliance of evolving components and the delivered solution with security requirements. The review process is described in the V&V process in FAST. When a system or application being acquired is to be owned and operated by a contractor or other government agency at a contractor or other government agency's IT site, e.g., in cloud computing, the contractor or other government agency must provide the security documentation for the development, test and production environments to the FAA COTR to provide to LoB security personnel for review and approval as specified in the contract, service-level, memorandum of, or other agreement (SLA / MOA / MOU). The security documentation includes SSP, ISCP, privacy threshold and if applicable impact assessment (PTA / PIA), and complete authorization to operate package including vulnerability and risk analyses and controls for the IT installations providing the operations. The reviewers include the LoB ISSM or senior ISS official of the LoB receiving the solution or application services; the ISSM of the LoB providing network connectivity to the externally operated system; and the cognizant AO(s).

External IT service providers must demonstrate that their operations will not degrade the security posture of the FAA before they initiate operations for FAA. That is, they must consent to compliance reviews as specified in the contract, MOA/SLA or other security interconnection agreement. The requirement for independent assessment via V&V of contractor development, test, and production environments must be part of the contract and agreed to in the bidder proposals.

Provide Risk Feedback on As-Built

Perform Security Assessments and Contingency Tests

Responsible Agent	Product	Approval Authority	Tools and Aids
Independent assessment team Security systems engineer/test staff ISO/ISSO of the intended operating office or service unit	Security Assessment Report (SAR) Facility Security Assessment ISCP Test Plan and Recovery Report (TPR)	LoB ISSM or senior ISS official AIN-1 or delegate LoB Authorizing Official	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management

AIN-100 (facility) and/or AIN-400 (personnel) security staff			Program FAA or LoB Security Authorization Handbook and Templates

Description:

The solution provided by the program undergoes testing to ensure it complies with security and privacy requirements in the system specification, facility blueprints, personnel security checks, the SSP and ISCP. The security assessment (i.e., testing) assesses compliance with security requirements to determine the risk associated with the vulnerabilities of the solution to threats. COTS, GOTS, and outsourced compiled source code must undergo independent assessment by V&V to identify vulnerabilities using FAA-approved tools or scanning service. Program management ensures that security staff as V&V agents conduct planned test, demonstration, inspection and analysis activities.

The Facility Security Assessment (FSA) provides the results of physical security analysis on any facility where changes are substantial enough to warrant. The program and facility manager must jointly develop and show progress remediating any unsatisfied physical security requirements via an action plan. In addition a suitability check for federal employees and contractors at any deployment facility is conducted by AIN-400 to ensure that appropriate clearances and physical access constraints have been realized before the in-service decision for the site.

The Security Assessment Report (SAR) contains the results of the ISS testing. The SAR also provides recommendations for failed test results that may include risk acceptance, remediation, corrective actions, or improvements. The System Characterization Document, SSP, PTA/PIAs, Risk Assessment Report, ISCP, ISCP Test Report, SAR, and any resultant program of action and milestones (POA&Ms) are attached to the evolved system authorization package. All other activities necessary to provide the security authorization package for AO approval decision are also produced during this task that is done in collaboration with the LoB/SO ISS program office.

Perform Security Assessments and Contingency Tests

Authorize Operation

Responsible Agent	Product	Approval Authority	Tools and Aids
Program or LoB Systems Security Engineer (SSE) ISO/ISSO of intended operating LoB or staff office Local Security Office (both facility and federal/contractor personnel security activities)	Security Authorization Package, including AO signed Authorization to Operate Approval to operate facility Appropriate clearances for personnel, federal and contractor	Authorizing Official (AO) of the receiving organization ISSCA (AIS-1) Facility manager and AIN-1 or delegate	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates

Description:

As part of the authorization package the Security and Contingency Plans (SSP / ISCP) are updated. The final security action of solution implementation is approval to operate (facility decision) and / or authority to operate (ISS decision by the LoB authorizing official).

The authorizing official (AO) for the operating LoB/SO accepts the risk for the new solution to operate by signing the Authority to Operate (ATO) with the ISSM, ISSCA (AIS-1), project manager, and information system owner / information steward. The system authorization package contains the following: SSP, System Characterization Document, PTA/PIA (the latter if applicable), ISCP,ISCP TPR, Risk Assessment Report,, Security Assessment Report, POA&Ms, and an Executive Summary providing the AO signature approving system operator or denial of authority to operate, including:

Summary description of the solution, including its security categorizations and whether it contains PII

Summary of assessment results
Table identifying POA&Ms, including those recommended for risk acceptance
A statement of the risk being accepted
Justification for the risk acceptance
Statement of completion for the ISCP test
AO's signature with the expiration date of the authorization
Continuous monitoring approach and schedule

Authorize Operation

Security Upgrade Insertion

Responsible Agent	Product	Approval Authority	Tools and Aids
Security systems engineer ISO/ISSO and ISSM of operating LoB/SO	(Option) NAS Change Proposal (NCP) Updated Authorization Package (as required) Facility Security Assessment (as required) Security training	LoB/SO ISSM. Senior ISS official ASH-1 or delegate Project CM	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates NAS CM Best Practices (fast.faa.gov)

Description:

The solution implementation program office, security service area, or LoB operations and maintenance management may develop preplanned product improvements or require other upgrades or flaw remediation, some of which may reduce vulnerabilities or satisfy residual security or privacy requirements. When sufficiently significant, usually when additional funding is required, the program or facility manager prepares for a re-baselining investment decision to obtain approval and funding, including security requirements. The improved solution may not need to be re-authorized based on the results of the SIA or FSA that was conducted to address the upgrade. For facilities, the facility manager and AIN-1 or delegate determines whether an immediate FSA will be needed. For IT the AO reviews the SIA and associated documentation and determine whether a security re-authorization package will be required before implementing the product/upgrade on the production system. The output of the SIA will determine the focus of the assessment to ensure there is no impact on the security controls as a result of the change.

NAS Change Proposal only: All modifications to in-service hardware and software require approval of a NAS Change Proposal according to procedures found on the NAS Configuration Management website. This website can be accessed from FAST at http://fast.faa.gov.

Security Upgrade Insertion

Continuous Monitoring and Patching

Responsible Agent	Product	Approval Authority	Tools and Aids
ISO/ISSO of operating	Continuous monitoring	LoB ISSM	FAA Order 1600.1,

LoB/SO System administrator AIN-100 (facility) and/or AIN-400 (personnel) security staff	records (e.g. annual security status reports including vulnerability scanning results) Flaw remediation records (e.g., security patches applied) Configuration Management records Security Impact Assessment (SIA) Updated SSP, ISCP, and POA&Ms if needed AO letter for continued Authorization to Operate Facility Authority to Operate Personnel clearances	AIN-1 or delegate LoB Authorizing Official	Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates
Description: During in-service management, continuous monitoring activities may detect system, facility, personnel or environmental vulnerabilities. Continuous monitoring includes periodic scans of operational systems to discover information system vulnerabilities or unauthorized privacy data. The ISSO uses the solution CM plan to maintain the configuration baseline, ensure that patches are current and applied; and to ensure that the solution is securely configured to its applicable secure baseline configuration and consistent with system change documentation. A security impact analysis (SIA) is conducted on any proposed changes to determine the impact of the change on the security status of the solution. The SIA focuses on the impact of changes on the security controls. The SIA also serves to direct the focus of the subsequent assessment. Security control assessments are conducted on a subset of the security controls such that each applicable control is assessed at least once over the 3-year authorization period. Facility security staff members walk the fences and buildings and continually review facility security readiness. Events such as hurricanes, earthquakes or vandalism may cause damage to a facility resulting in incident reports that require an update to the Facility Security Assessment or action plan. Likewise personnel security staff members review changing federal and contractor personnel and their position descriptions for appropriate clearance and badging to discharge their responsibilities.			

Continuous Monitoring and Patching

Periodic Assessment and Re-Authorization

Responsible Agent	Product	Approval Authority	Tools and Aids
LoB/SO ISS security staff (ISO/ISSO) Independent assessment team AIN-100 (facility) and/or AIN-400 (personnel) security staff	Security Authorization Package (triennial) SAR and Risk Assessment Report and POA&Ms Facility Security Assessment (annually or biannually) Clearances (at five years)	ASH-1 or delegate LoB ISO LoB Authorizing Official ISSCA (AIS-1)	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates
Description:			

ISS: Every operational system must undergo an annual security assessment (formerly known as annual self-assessment) that supports annual security status reporting and continuous monitoring. The system's SCD, SSP, and other supporting documents are updated in accordance with findings in compliance with the FAA ISS Authorization Handbook and Templates.

Even if no changes have taken place, every fielded solution must be reauthorized as part of continuous authorization process of continuous monitoring. Reauthorization must occur within a three year period.

Physical security: Annually for most, and biannually for minor sites, facilities undergo physical safety and security re-certification. Findings and the actions to close them are tracked in the EOSH and facilities security databases operated by ASH. The actions needed to satisfy physical security requirements become part of the action plan for the facility and are input to the facility budget proposal or Corporate Work Plan (CWP) as appropriate.

Personnel security: Upon initiation of employment and at five-year intervals, AIN-400 conducts a background investigation on every employee and contractor staff authorized to be on-site at FAA sites. The investigation may be as simple as credit and FBI criminal database checks, or as extensive as 15-year or longer, formal background investigations for secret or top-secret clearances as required for the job that the person performs. FAA and other federal personnel, as described in FAA Order 1600.1, and contractors, as described by FAA Order 1600.72, transferring to work at FAA from other agencies may have a current investigation that may be accepted in lieu of FAA investigation. The cost of security background checks is significant and often time-consuming (up to four months routinely). Therefore the program and the facility or equipment operations management office should be concerned for FAA and contractor personnel turnover. Excessive turnover of contractor staff may result in the program being charged for contractor background checks and other clearance activities.

Periodic Assessment and Re-Authorization

Termination and Disposal of Investment and Data

Responsible Agent	Product	Approval Authority	Tools and Aids
AIN-100 (facility) and/or AIN-400 (personnel) security staff LoB/SO ISS security staff (ISO/ISSO) LoB/SO Enterprise Architect Facility manager	CM records of system peripheral termination Data media erasure or destruction records Real property disposal records Personal property disposal records Personnel clearance records	LoB/SO ISSM LoB/SO Authorizing Official (AO) EAB (NAS) or ARB (non-NAS) Operating LoB executive (facilities and personnel) AIN-1 or delegate	FAA Order 1600.1, Personnel Security Program FAA Order 1600.72, Contractor and Industrial Security Program FAA Order 1600.69, Facility Security Management Program FAA or LoB Security Authorization Handbook and Templates FAA Order 1370.100, Media Sanitization and Destruction

Description:

At intervals established for different acquisition categories (ACATs) the operating LoB / SO or service units review their applications and systems to determine if they are still needed and/or operating according to specifications. If an application is terminated, the information system owner initiates the appropriate notification and addresses any user counterproposals prior to termination of operations. When the application is deactivated, all code, documentation and copies of databases are archived to media for storage. The platform on which the application resided including production, test and development servers and workstation clients will have their media erased or removed and disposed of in accordance with FAA media and disposal policies and guidelines. The FAA EA is updated as of the action date, and the National Service Center (NSC) or equivalent helpdesk uses scripts prepared under CM to notify all affected stakeholders that the termination, archive and disposal have been completed.

Requirements for facility termination and real and personal property disposal, including equipment, furniture, books / manuals and hard copy or non-electronic media data, is described in FAA Order 1600.69. Hazardous materials and sensitive privacy impact information (S/PII) require exceptional and often expensive disposal mechanisms. The costs for these are input to the alternatives analysis and program planning for a solution early in the investment lifecycle but must be considered in the annual budget for the planned termination event.

Personnel terminating the FAA and other federal employees with access to FAA sites and systems are reported to AIN-400 for termination of badge access rights. AIN-400 also contacts the ISSM of the organizational element for the program or system operations so terminating personnel systems access can also be removed. When contractors or their subcontractors terminate service on FAA programs or in operations, the COTR is responsible to inform AIN-400 so that their badges and access are terminated and their access removed. This is difficult when access to KSN and other tools may be requested and provided independently of core IT services such as email. Nonetheless it is required and audited by the Department of Transportation Inspector General, so care must be taken to limit access to systems and sites where the contractor / other government employee has a solid, recurring need to know or have access.

Termination and Disposal of Investment and Data