

6/9/00

SUBJECT: INFORMATION SYSTEMS SECURITY PROGRAM

-
- 1. PURPOSE.** This order establishes policy and assigns organizational and management responsibilities to ensure implementation of the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources; Department of Transportation (DOT) Handbook, DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM); and Presidential Decision Directive 63 (PDD 63).
 - 2. DISTRIBUTION.** This order is distributed to the division level in Washington headquarters, regions, and centers and a limited distribution to all field offices and facilities.
 - 3. CANCELLATIONS.** This order cancels FAA Order 1600.54B, FAA Automated Information Systems Security Handbook, and FAA Order 1600.66, Telecommunications and Information Systems Security Policy.
 - 4. BACKGROUND.** In accordance with the Computer Security Act of 1987, the FAA must ensure that all information systems are protected from threats to integrity, availability, and confidentiality. The FAA maintains a variety of information systems that support the agency, aviation safety and security, and the National Airspace System (NAS). FAA information systems depend on adequate information security for proper operation and protection from unauthorized access and modification. The increasing number of network-based attacks, the reliance on the internet for quickly communicating information, and the vulnerability of information systems to exploitation by threat agents require a rigorous Information Systems Security (ISS) approach to protect FAA information systems.
 - 5. DEFINITIONS.** Appendix 1, Definitions, contains terms used in this order.
 - 6. SCOPE** This order applies to all:
 - a.** FAA information (including classified) collected, stored, processed, disseminated, or transmitted using FAA or non-FAA information systems. Information systems located at airports or on air carriers must protect information in accordance with 14 Code of Federal Regulations (CFR), Part 191.
 - b.** FAA information systems (administrative, NAS, and mission support); all information systems funded by the FAA; all prototypes connected to operational systems.
 - c.** Information systems, including those located within non-FAA facilities where these information systems are developed, housed, or operated.
 - d.** FAA employees, contractors, subcontractors, and other users of FAA information systems or those connected to an FAA information system.
 - 7. PRECEDENCE AND INTERPRETATION.** This order has precedence over other FAA orders that contain conflicting, incomplete, or obsolete ISS policy, guidance, or instruction. This order does not supercede any applicable requirements of FAA orders issued for classified National Security and Communications Security Information. The Assistant Administrator for Information Services and Chief Information Officer, AIO-1, is authorized to interpret the provisions of this order; resolve any apparent conflicts with other orders; modify this order to be consistent with significant changes in Federal, departmental, and FAA mandates; and issue detailed ISS implementation orders, procedures, and guidance for executing this order.

8. EXPLANATION OF CHANGES. This order:

- a.** Identifies the ISS responsibilities transferred from the Associate Administrator for Civil Aviation Security, ACS-1, to the Assistant Administrator for Information Services and Chief Information Officer, AIO-1.
- b.** Returns Designated Approving Authority (DAA) responsibilities from ACS-1 to the Administrator, who hereby delegates responsibility to those members of the Management Board who own or operate systems as specified herein.
- c.** Transfers the responsibilities of the ISS certifier from the ACS organization to developing organizations for new systems or to system owners for other systems.
- d.** Changes the documentation requirement for obtaining ISS certification and authorization from Sensitive Application Certification (SAC) and accreditation documentation to a Security Certification and Authorization Package (SCAP).
- e.** Expands the requirement to conduct ISS activities from only national information systems acquisitions to all information systems acquisitions within the FAA.
- f.** Changes the baseline security level for information systems from the Department of Defense 5200.28-STD, Trusted Computer System Evaluation Criteria, Class C2, to a baseline founded on protection profiles published by the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA) or under Common Criteria Mutual Recognition Arrangements (MRA) with either agency.
- g.** Updates the requirement to conduct ISS compliance reviews and site surveys from only those information systems located in FAA facilities to all FAA information systems. These systems include systems in non-FAA facilities where FAA information systems, or any portion of FAA information systems, will be developed, housed, or operated or where FAA information is collected, stored, processed, or transmitted for or on behalf of the FAA. The FAA need not own the equipment if it is operated on behalf of the FAA.
- h.** Updates the awareness and training requirements to be consistent with OMB Circular A-130, Appendix III.
- i.** Phases in required ISS activities based on an annual FAA Critical Infrastructure Protection Remediation Plan consistent with annual appropriations.

9. STATUTORY, POLICY, AND REGULATORY MANDATES.

a. Computer Security Act. The Computer Security Act of 1987, Public Law 100-235, dated January 8, 1988, is the cornerstone of computer security within the Federal Government and is the basis for the development of the FAA ISS policy. Public Law 100-235 requires Federal agencies to identify sensitive systems, provide security training, and develop and implement an ISS plan for each sensitive system.

b. Presidential Decision Directive (PDD) 63. PDD 63, Critical Infrastructure Protection (May 1998), requires Federal agencies to develop and implement a comprehensive security program to protect their critical infrastructure. The NAS is specifically mentioned as part of the transportation sector of the national critical infrastructure. The FAA responded to this requirement with the publication of the FAA Critical Infrastructure Protection Plan (CIPP), dated March 26, 1999. The CIPP serves as the ISS mission statement for the FAA, as it relates to ISS. PDD 63 addresses the cyber and physical infrastructure vulnerabilities of the Federal Government by requiring each department and agency to work to reduce its exposure to new and existing threats.

c. Federal Policy Requirements. In accordance with OMB Circular A-130, the ISS Program shall implement policies, standards, and procedures that are consistent with government wide policies, standards, and procedures issued by OMB, the Department of Commerce, and the Office of Personnel Management (OPM). The DOT implements these policies and standards and supplements them through procedural handbooks. The FAA ISS Program implements the DOT policy and standards and adopts the DOT procedural handbooks as the basis for FAA orders.

(1) OMB issues Federal policy for information management and security of information systems.

(2) The Department of Commerce, in accordance with the Computer Security Act of 1987, is responsible for developing computer security standards and guidelines for Federal unclassified systems. Accordingly, OMB Circular A-130 states each agency shall implement policies, standards, and procedures that are consistent with standards and guidance issued by NIST. These publications may be obtained from the NIST Internet web page.

(3) OPM has the responsibility, as assigned by the Computer Security Act of 1987, to issue security training guidance. OMB Circular A-130 specifies training for all Federal employees who manage and use Federal computer systems that process U.S. Government information. Specific amounts, types, and intervals of security training are identified for Federal computer users, administrators, technicians, managers, and executives in OMB Circular A-130. OPM also specifies the procedures for designating sensitive positions and screening incumbents as stated in FAA Order 1600.1, Personnel Security Program.

(4) DOT ISS policies, directives, and handbooks shall be implemented as appropriate. DOT ISS policy is designed to satisfy Federal requirements, protect information technology, provide ISS awareness training, and provide ISS program planning guidance.

(5) FAA ISS implementation orders and guidelines are documents issued by AIO-1 in coordination with the members of the Management Board. These orders and guidelines contain details for implementation of the ISS policy and shall be used in implementing the agency's ISS Program.

10. POLICY. The FAA shall ensure that security is provided commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information for all agency information collected, processed, transmitted, stored, or disseminated in FAA information systems and in information systems used on behalf of the FAA. The FAA shall also ensure that systems and applications used by or for the FAA provide appropriate confidentiality, integrity, authenticity, and availability. This policy shall be executed consistent with annual appropriations and shall be phased in to allow for orderly improvement in information systems security.

11. DELEGATION OF AUTHORITY. The Administrator is the DAA for the agency and hereby delegates to each member of the Management Board the responsibility to authorize FAA information systems owned or operated by that member, if those information systems collect, store, process, disseminate, or transmit information in the performance of the FAA mission. This authority may be further delegated one level below each member of the Management Board. No further delegation is authorized. Additionally, the Administrator hereby designates AIO-1 as the agency focal point for all ISS in accordance with the Clinger-Cohen Act and OMB Circular A-130.

12. POLICY IMPLEMENTATION. The FAA shall:

a. Implement and maintain a program to ensure that all NAS, mission support, and administrative systems are appropriately secured, using a combination of techniques that include physical and personnel security, compartmentalization of information, site adaptation, redundancy, and other procedural and technical means.

b. Prioritize activities and funding to protect critical information systems before protecting noncritical information systems.

c. Ensure ISS requirements and costs are included as part of any acquisition and throughout the life cycle for systems and services, including service-life extension and decommissioning activities.

d. Implement security enhancements, as feasible, on existing critical systems within the resource constraints of funding, schedules, and cost effectiveness, so as to be certified and authorized by May 2003 in accordance with PDD 63.

e. Implement security features in new critical systems so as to be certified before installation and authorized before operational use.

f. Include funding for ISS requirements in each information system budget baseline for fiscal years 2003 and beyond.

g. Require that each member of the Management Board who owns or operates one or more information systems be designated as a DAA.

h. Develop and maintain the FAA CIPP in accordance with PDD 62 and PDD 63.

i. Designate the position security sensitivity and/or clearance level of employee and contractor positions associated with the management or operation of information systems in accordance with FAA Order 1600.1, Personnel Security Program.

j. Require that all FAA personnel, contractors, and subcontractors working for, on behalf of, or connected to, FAA information systems take measures commensurate with the sensitivity level of the information and the risk and magnitude of harm to provide for:

(1) The integrity, availability, confidentiality, authenticity, and accountability of information and source code.

(2) The protection of information and the information systems that store, process, disseminate, or transmit this information.

k. Require that other users working for, on behalf of, or connected to an FAA information system enter into formal agreements with the FAA through contract clauses or memoranda of agreement (MOA) to ensure that appropriate measures are taken to protect the information and information systems commensurate with its sensitivity level and the risk and magnitude of harm.

l. Prepare an appropriate protection profile and security target for each information system. Each protection profile shall be tailored from protection profiles published by NIST or NSA or under Common Criteria MRA with either agency.

m. Require that information system owners update the SCAP and ensure recertification and reauthorization of their systems every 3 years or sooner, if there is a major system or environmental change that impacts the security posture of the system, including new or additional connectivity to other information systems, major hardware/software changes, or whenever a major security breach has occurred.

n. Implement countermeasures to reduce the effectiveness of threats, including computer viruses and other forms of unauthorized or malicious codes.

o. Participate in the development of ISS strategies for internal and external information sharing.

p. Ensure that an incident monitoring, tracking, and response capability is implemented.

q. Ensure that ISS training requirements are implemented.

r. Ensure that contractors and subcontractors meet FAA ISS training requirements.

s. Identify, inventory, and report all information systems the agency owns or operates and identify the sensitivity level of each system in accordance with OMB Circular A-130 and DOT Order 1350.2, Chapter 11, Information Systems Security Program. This inventory shall be maintained and updated annually.

13. RESPONSIBILITIES. Effective ISS depends on the involvement of all FAA organizations that acquire, develop, own, operate, or replace information systems components. Appendix 2 depicts the operational reporting relationship between the key ISS functions within the FAA. These organizations shall participate in the formulation and approval of FAA ISS orders, requirements, procedures, and risk mitigation controls for ISS. These organizations shall comply with this order and carry out responsibilities as follows:

a. Each member of the FAA Management Board shall:

(1) Implement an FAA ISS Program within their respective organization according to the requirements of this order, in a manner consistent with annual appropriations.

(2) Ensure that all information systems within their organization are ISS certified and authorized as described in paragraph 12 of this order.

(3) Ensure that information collected, stored, disseminated, or transmitted by an information system owned or operated on behalf of the Management Board member is properly protected against unauthorized access, use, modification, destruction, or denial of service through the integration of management, operational, and technical controls consistent with agency policy.

(4) Coordinate with AIO those internal ISS activities that impact FAA-wide ISS initiatives, such as training and incident response.

(5) Appoint, in writing, Federal employees as the DAA and alternate DAA, who shall authorize system operation and accept identified risks for information systems owned by the line-of-business or staff office. DAA responsibilities may be delegated in writing to a Federal employee manager one level below the Management Board member. No further delegation is authorized. Normally, the organizational deputy to the DAA will be the alternate DAA. These appointments shall be forwarded to AIO-1.

(6) Appoint, in writing, Federal employees as the Information Systems Security Manager (ISSM) and, optionally, one or more associate ISSM's who are responsible for implementing the agency's ISS Program within the line-of-business or staff office. The scope of responsibility for an associate ISSM may be a portion of the line-of-business or staff office. The ISSM shall be empowered to represent and make decisions relating to ISS for the organization at all management levels. The DAA and ISSM may not be the same person.

(7) Appoint, in writing, one or more Federal employees as Information Systems Security Officer(s) (ISSO) to assist the ISSM with implementation of the agency's ISS Program within their line-of-business or staff office, in accordance with FAA guidance.

(8) Appoint, in writing, one or more Federal employees from the system owner's organization as ISS Certifier(s) (ISSC), responsible for certifying that system security technical controls are present and functional, management and physical controls are described and in place, and risk has been mitigated commensurate with the magnitude of harm. The ISSC shall not be the DAA.

(9) Review existing line-of-business or staff office policies, guidelines, procedures, and international agreements for compliance with this order and modify those policies, procedures, and agreements accordingly at the next update.

(10) Include references to this order in new contracts, MOA's, and memoranda of understanding (MOU). For existing contracts, include references to this order at the time of contract modification or renewal.

(11) Ensure that all information system acquisition and contracting actions, including service life extension and decommissioning activities, include ISS as appropriate and comply with FAA and DOT ISS policies.

(12) Ensure that owners of new systems and any systems that are to be authorized after January 1, 2002, develop a protection profile and security target that provides adequate protection (per OMB Circular A-130) for each information system and coordinate with the DAA and AIO for acceptance of the protection profile and security target as the approved security baseline. During the agency's transition to the use of protection profiles and security targets for other systems, the system owner shall negotiate with the DAA and AIO for a comparable means to identify security risks and requirements.

(13) Participate in updating the annual FAA Critical Infrastructure Protection Remediation Plan.

(14) Conduct ISS activities that are identified in the annual FAA Critical Infrastructure Protection Remediation Plan for execution by the line-of-business or staff office.

(15) Ensure that security test and evaluation is conducted for all ISS requirements and risk mitigation controls. Test scenarios will include typical variations to exercise the security countermeasures.

(16) Plan and provide ISS resources for any new developmental starts as of the date of this order and for all other information systems beginning in fiscal year 2003.

(17) Prioritize resources commensurate with the sensitivity level of the information and the risk and magnitude of harm associated with the information systems. Manage ISS activities in the best interest of the FAA, as well as their own organization.

(a) Consult with AIO in formulating agency ISS budget and resource requirements.

(b) Consult with AIO in prioritizing the allocation of agency ISS budget and resources upon receipt of annual agency appropriation.

(c) Consult with AIO in annually updating the FAA Critical Infrastructure Protection Remediation Plan.

(d) Provide to AIO a statement of ISS resource requirements and ISS program status.

(e) Participate in responding to the DOT, OMB, GAO, and other inquiring entities.

(18) Ensure that FAA and contractor personnel occupying positions designated Computer/Automated Data Processing (ADP) sensitive comply with FAA Order 1600.1D, Personnel Security Program.

(19) Ensure that access to an FAA information system is terminated when an FAA employee or contractor no longer needs such access.

(20) Ensure that ISS training is incorporated into the policies and procedures for the organization in accordance with this order.

(21) Ensure that all ISS incidents are reported to the appropriate ISSO and to the FAA Computer Security Incident Response Capability (CSIRC).

(22) Identify, inventory, and report all information systems owned or operated by the line-of-business or staff office, and identify the sensitivity level of each system in accordance with OMB Circular A-130 and DOT Order 1350.2, Chapter 11, Information Systems Security Program. This inventory shall be updated and submitted to AIO annually. With ongoing contracts, where ISS is not specifically defined as a deliverable, resources shall be estimated unless new ISS requirements cause a contract change.

(23) Participate in developing, maintaining, and implementing the overall FAA ISS Recruitment and Retention Plan.

b. Assistant Administrator for Information Services and Chief Information Officer (AIO). AIO-1 is designated as the agency focal point and has overall responsibility for the FAA ISS Program. AIO-1 shall:

(1) Oversee the development and implementation of the FAA ISS Program and be the primary advocate for the agency's ISS Program.

(2) Oversee ISS policies, protection profiles, architectures, investment analyses, concepts of operation, procedures, processes, methodologies, standards, training, and plans.

(3) Ensure that information, which is collected, stored, disseminated, or transmitted by information systems owned or operated on behalf of the FAA, is properly protected against unauthorized access, use, modification, destruction, or denial of service through the integration of management, operational, and technical controls.

(4) Serve as the ISS Certification Agent for all FAA information systems, ensuring that information systems are certified and authorized in accordance with this order. ISS Certification Agent responsibilities may be delegated, in writing, to a manager one level below AIO-1. No further delegation is authorized.

- (5) In consultation with the Management Board members, develop and issue agencywide ISS implementation orders, procedures, and guidance in support of this policy.
- (6) Authorize the release of sensitive security information developed, generated, stored, or transmitted within the scope of the ISS Program. The release of all other sensitive security information remains with ACS-1.
- (7) Advise the Administrator and Management Board members of status and issues concerning the ISS Program.
- (8) Serve as ISS liaison to external organizations.
- (9) Collaborate with appropriate Management Board members to prioritize ISS activities and resource allocation.
- (10) Lead formulation and justification of the agency ISS budget, in consultation with appropriate Management Board members.
- (11) Update the FAA Critical Infrastructure Protection Remediation Plan in consultation with appropriate members of the Management Board. That plan shall identify major ISS activities to be conducted during the fiscal year and allocate ISS funds and resources consistent with annual appropriations. With ongoing contracts, where ISS is not specifically defined as a deliverable, Management Board members shall estimate resources for the annual plan.
- (12) Consolidate and develop ISS responses to congressional, OMB, GAO, DOT, and other inquiries, with inputs from the Management Board members.
- (13) Oversee the development and operation of a CSIRC.
- (14) Ensure that ISS Program implications resulting from technology or budget changes are communicated to the Management Board members.
- (15) Develop, maintain, and oversee the implementation of an FAA-wide ISS Training Program, in consultation with the Management Board members.
- (16) Develop, maintain, and oversee the implementation of an FAA-wide ISS Recruitment and Retention Plan in consultation with the lines-of-business and staff offices, including the Office of Human Resource Management (AHR).
- (17) Establish and manage a process for conducting ISS compliance reviews in collaboration with the ISSM's at FAA facilities and site surveys at non-FAA facilities. Conduct compliance reviews and make recommendations to the DAA for appropriate procedural, contractual, technical, or programmatic actions to correct any deficiencies within a specified timeframe.
- (18) Authorize penetration testing on FAA information systems with advanced coordination with the DAA for the line-of-business or staff office that owns the system, the information owner (if not the same as the system owner), and the Office of Chief Counsel. If the penetration test could impact one or more systems for which other DAA's are responsible, then coordination must include all affected DAA's.
- (19) Ensure an information-sharing capability for common vulnerabilities and threats. This capability shall share information with other internal and external organizations, consistent with DOT, FAA, National Infrastructure Protection Center (NIPC), and NIST policies and procedures.
- (20) Maintain and update, at least annually, an inventory of all agency information systems and identify the sensitivity level of each system in accordance with OMB Circular A-130 and DOT Order 1350.2, Chapter 11, Information Systems Security Program.
- (21) Review external policies, alerts, guidance, and technical standards and advise lines-of-business and staff offices of changes that may impact the FAA ISS Program.

(22) Plan and provide resources up through and including fiscal year 2002 for the certification and authorization of existing systems across the agency, prioritizing resources commensurate with the sensitivity level of the information and the risk and magnitude of harm associated with the information systems.

(23) Annually plan and provide resources for agencywide ISS activities not limited to a single line-of-business or staff office, including the CSIRC, ISS research and development, ISS architecture, ISS systems engineering, and ISS training.

c. Information Systems Security Certifier (ISSC). A senior manager in the developmental or operational organization that owns the system and is responsible for certifying that system security technical controls are present and functional, management and physical controls are described and in place, and risk has been mitigated commensurate with magnitude of harm. The ISSC for an information system shall:

(1) Appoint the team responsible for development of the SCAP and shall be accountable for its development, content, and quality.

(2) Certify that information system security technical controls are present and functional, management and physical controls are described and in place, and risk has been mitigated commensurate with the magnitude of harm.

(3) Sign the final ISS certification together with the Certification Agent and forward it to the ISSM for review prior to the DAA deciding whether or not to authorize the system.

(4) Not be the DAA or ISSO, but may be the ISSM.

(5) Occupy a position that shall be designated as a high-risk, public trust position in accordance with agency policy. All persons occupying these positions shall be Federal employees and shall be subject to a background investigation in accordance with FAA Order 1600.1D, Personnel Security Program.

d. Information Systems Security Certification Agent (ISSCA). A senior level manager responsible for ensuring an impartial, quality control review of the SCAP, who makes recommendations to the ISS Certifier and the DAA, as appropriate. The ISSCA signs the final ISS certification document before forwarding it to the ISSM for review prior to the DAA deciding whether or not to authorize the system. The ISSCA shall:

(1) Ensure impartial quality control review of the SCAP and make recommendations to the ISSC and DAA, as appropriate.

(2) Sign the final ISS certification together with the ISSC and forward it to the ISSM for review prior to the DAA deciding whether or not to authorize the system.

(3) Occupy a position that shall be designated as a high-risk, public trust position in accordance with agency policy. All persons occupying these positions shall be Federal employees and shall be subject to a background investigation in accordance with FAA Order 1600.1D, Personnel Security Program.

e. Designated Approving Authority (DAA). The DAA for a line-of-business or staff office shall:

(1) Determine whether or not to authorize for operation or continue operation for any information system owned by the line-of-business or staff office. Such authorization will be based on information provided in the SCAP and shall mean that the DAA has determined that the risks associated with the operation of the system have been reduced to an acceptable level. The DAA makes a formal declaration that an information system is approved to operate in a particular security mode using a prescribed set of countermeasures. The authorization statement affixes security responsibility with the DAA and shows that due care has been taken for security.

(2) Coordinate the authorization of penetration testing on information systems owned by their line-of-business or staff office. Also coordinate when the system being tested is not owned by the line-of-business or staff office, but could be impacted by the test.

(3) Ensure that when authorizing an information system it does not compromise the security of any other system to which it is connected.

(4) Authorize an interconnection between information systems, based upon information provided in the SCAP, prior to establishing that interconnection. If the interconnection is with a system for which another DAA is responsible, then both DAA's must authorize the interconnection.

(5) Withdraw previously granted authorizations or authorize disconnection of an information system, if it is determined that the system is not meeting specified conditions stated in the SCAP or poses a safety or security threat to the FAA, other Federal agencies, or the aviation community. The DAA shall ensure that impacted system and information users are provided timely notification of the intent to withdraw the authorization or disconnect the system and give a specific timeframe in which the system owner may correct the deficiencies to eliminate the withdrawal or disconnection. Under extenuating circumstances, the DAA may authorize an immediate disconnection.

(6) Affirm that an information system meets all applicable Federal ISS policies, regulations, and standards and that the results of system security tests demonstrate that the installed security countermeasures provide adequate protection.

(7) Occupy a position that shall be designated as a high-risk, public trust position in accordance with agency policy. All persons occupying these positions shall be Federal employees and shall be subject to a background investigation in accordance with FAA Order 1600.1D, Personnel Security Program.

f. Information Systems Security Manager (ISSM). The ISSM is an FAA employee who is responsible for implementing the agency's ISS Program within a single line-of-business or staff office. The ISSM (and any associate ISSM) for a line-of-business or staff office shall:

(1) Implement the agency's ISS Program within the line-of-business or staff office. This individual shall be empowered to represent and make decisions relating to ISS for the organization at all management levels.

(2) Implement ISS mitigation countermeasures identified through ISS alerts or bulletins, as applicable.

(3) Ensure that ISS countermeasures and procedures specified in the information system authorization are implemented and sustained.

(4) Carry out additional implementation responsibilities as delegated by the Management Board member.

(5) Serve as the Management Board member's primary point of contact for coordination of the FAA Critical Infrastructure Protection Remediation Plan, training, resources, funding, dissemination of ISS information and alerts, and other elements of ISS implementation.

(6) Direct the ISSO's in their performance of ISS activities.

(7) Ensure that adequate operational, contingency, emergency, and incident response plans are in place and being executed.

(8) Review the SCAP for each certified information system and advise the DAA whether or not to authorize the system.

(9) Coordinate, in advance, with other ISSM's when a system connection or change of ownership impacts information systems security in one or more lines-of-business or staff offices.

(10) Participate in ISS compliance reviews and threat assessments and advise the DAA on changes in risk and recommend appropriate action, including withdrawing system authorization.

(11) Be a Federal employee and shall be subject to a background investigation in accordance with FAA Order 1600.1D, Personnel Security Program.

g. Information Systems Security Officer (ISSO). Within the scope of their appointment in a line-of-business or staff office, an ISSO shall:

- (1) Implement the agency's ISS Program. This individual shall be empowered to represent and make decisions relating to ISS at all management levels.
- (2) Implement ISS mitigation countermeasures identified through ISS alerts or bulletins, as applicable.
- (3) Ensure that ISS countermeasures and procedures specified in the information system authorization are implemented and sustained.
- (4) Carry out additional implementation responsibilities as delegated by their Management Board member.
- (5) Support the ISSM on the FAA Critical Infrastructure Protection Remediation Plan, training, resources, funding, dissemination of ISS information and alerts, and other elements of ISS implementation.
- (6) Follow the direction of the ISSM in performing ISS activities.
- (7) Prepare and execute adequate operational, contingency, emergency, and incident response plans.
- (8) Assist the system owner and system developer with developing the SCAP for each information system and recommend to the ISSC whether or not to certify the system and to the ISSM whether or not the DAA should authorize the system.
- (9) Participate in ISS compliance reviews and threat assessments, advise the ISSM on changes in risk, and recommend appropriate action, including withdrawing system authorization.
- (10) Occupy a position designated as a high-risk, public trust position in accordance with agency policy. All persons occupying these positions shall be Federal employees and shall be subject to a background investigation in accordance with FAA Order 1600.1D, Personnel Security Program.

h. Contracting Officer and Contracting Officer Technical Representative (COTR). A Contracting Officer and COTR shall:

- (1) Ensure that new contracts include appropriate language and clauses to enable the enforcement of this order and that existing contracts include appropriate language when they are modified.
- (2) Ensure that all new or modified FAA contracts include the statement -- "This order applies to all non-FAA facilities where FAA information systems, or any portion of FAA information systems are developed, housed, or operated and that collect, store, process, disseminate, or transmit FAA information, regardless of the equipment used."
- (3) Ensure that all new or modified FAA contracts include a clause requiring ISS basic awareness training or performance training in accordance with paragraph 12.
- (4) Ensure that ISS functional and assurance requirements are incorporated in information system procurement documents in accordance with this order.
- (5) Ensure that contractors and subcontractors provide copies of their internal security plans and procedures to the FAA.
- (6) Ensure that existing and future contracts include requirements to conduct site surveys at non-FAA facilities by AIO representatives or other designated FAA personnel. The site surveys will be prearranged with the Contracting Officer and the ISSM. Site surveys will encompass ISS and may also include physical and personnel security, with prior ACS-1 agreement. The surveys will be based on contractor and subcontractor internal security plans and procedures. A final report, with any recommendations, will be sent to the appropriate program office and Contracting Officer for review and/or action. All documents received from the contractor or subcontractor will be marked as sensitive security information, if appropriate, and will be handled accordingly.
- (7) Enforce all ISS-related conditions in any contract.

i. FAA Managers, Supervisors, and Employees shall:

- (1) Comply with this order and apply its principles to daily work activities.
- (2) Be accountable for protection of sensitive information under their control in accordance with this order.
- (3) Attend annual ISS awareness training.
- (4) Report ISS incidents, including virus and malicious code attacks, according to procedures established by their line-of-business or staff office.
- (5) Cooperate with computer security incident response team members.
- (6) Implement ISS mitigation countermeasures identified through ISS alerts or bulletins, as applicable.
- (7) Cooperate with AIO representatives or other designated FAA personnel during conduct of security compliance reviews at FAA facilities and site surveys at non-FAA facilities.



Jane F. Garvey
Administrator

APPENDIX 1. DEFINITION OF TERMS

Acceptable Level of Risk. A judicious and carefully considered assessment by the appropriate DAA that an information system(s) meets the minimum requirements of applicable security directives. The assessment should take into account the sensitivity and criticality of information, threats and vulnerabilities, countermeasures and their effectiveness in compensating for vulnerabilities, and operational requirements.

Accountability. The quality or state that enables violations or attempted violations of ISS to be traced to individuals who may then be held responsible.

Adequate Protection. (OMB Circular A-130) Protection that is commensurate with the risk and magnitude of the potential harm resulting from the loss, misuse, or unauthorized access to or modification of information resources. This protection includes ensuring that systems and applications used by the FAA operate effectively and provide appropriate confidentiality, integrity, availability, and accountability by using cost-effective management, personnel, operational, physical, and technical controls commensurate with an information system's sensitivity level.

Assurance. Policies and procedures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This assurance includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Availability. Timely, reliable access to data and information services for authorized users.

Classified Information System. An information system operated in the interest of national security that requires protection against unauthorized disclosure as determined under Executive Order 12598. Such information system is classified as top secret, secret, or confidential.

Common Criteria. A multi-part standard (ISO/IEC 15408) that defines criteria that are to be used as the basis for evaluating security properties of information technology products and systems. By establishing such a common criteria base, the results of an information technology security evaluation are meaningful to a wider audience.

Confidentiality. A requirement that private or confidential information not be disclosed to unauthorized individuals.

Contingency Measures. Measures maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Countermeasures. The protective measures for an information system, whether technical, physical, or personnel.

Critical Infrastructure Protection Plan (CIPP). The FAA's plan that defines the ISS Program in accordance with the requirements of Presidential Decision Directive 63.

Critical Infrastructure Protection Remediation Plan. The annually updated plan that details how the CIPP will be executed.

Critical System. A system whose information, if modified or denied, could significantly increase the risk of placing someone in jeopardy of injury or death or could significantly increase the risk of violating public trust.

Designated Approving Authority (DAA). A senior FAA management official, appointed in writing by a Management Board member, who determines whether or not to authorize a system for operation or to remove that authorization.

Developer or Developing Organization. An organization with primary responsibility for developing or acquiring an information system. If a contractor develops a system, the FAA organization responsible for that contract is the developing organization.

FAA Facility. Any facility that is owned, leased, or loaned to the FAA, where FAA information systems, or any portion of FAA information systems, will be developed, housed, or operated, or where FAA information is collected, stored, processed, disseminated, or transmitted using FAA or non-FAA equipment.

General Support System. An interconnected set of information resources that share a common functionality under the same direct management control. These systems, which include software, host computers (e.g. mainframes, minis, workstations), and networks (LAN and WAN), provide support for a variety of users and applications.

Government Information. Information that is created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. FAA information is categorized as follows:

- a. Classified Information.** Information that, in the interest of national security, requires protection against unauthorized disclosure as determined under Executive Order 12958. Such information is classified as top secret, secret, or confidential.
- b. Other Sensitive Security Information.** Information whose unauthorized disclosure, modification, or unavailability would harm the agency. Other sensitive security information includes:
 - (1) Essential or critical air traffic control information and any other information that must be protected in performance of the FAA mission to ensure confidentiality, integrity, or availability of information.
 - (2) Information requiring protection under the provisions of the Privacy Act of 1974.
 - (3) Information designated "For Official Use Only" (FOUO).
 - (4) Information whose disclosure or modification might impact the contractual or resource management function.
 - (5) Information that is proprietary.
 - (6) Information identified in the Clinger-Cohen Act.
 - (7) Information falling under the auspices of the Computer Security Act of 1987.
 - (8) Information protected under the Sensitive Security Information rule, 14 CFR Part 191.
 - (9) Information relating to financial management.
 - (10) Information exempt from disclosure under the Freedom of Information Act.

Information Owner. For information originating within the FAA, the information owner is the manager responsible for establishing the rules for the use and protection of the subject information. For information originating elsewhere, the information owner is the originating entity, represented by a designated individual. The information owner retains responsibility for its security, even when the information is shared with other organizations.

Information System. A discrete set of information resources, either in stand-alone or networked configurations, that is organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems are of two types:

- a. General Support Systems.** Interconnected information resources that are under the same direct management control and share common functionality, e.g. telecommunications and networks.
- b. Major Application Systems.** Systems that require special management attention because of their importance to the agency's mission; their high-maintenance, development, or operating costs; or their significant role in dealing with the agency's programs, finances, property, or other resources.

Information System Owner. See **System Owner.**

Information Systems Security (ISS). The collected attributes that describe the security measures taken to protect information systems and the information of FAA information resources, either individually or collectively.

Information Technology (IT). The hardware, software, and networks that process information, regardless of the technology involved, whether computers, telecommunications, or other.

ISS Certification. Comprehensive evaluation of the technical and non-technical security features of an information system and other countermeasures made in support of the authorization process. The evaluation establishes the extent to which a particular design and implementation meet a set of specified security requirements and that risk has been mitigated commensurate with magnitude of harm.

ISS Certification Agent (ISSCA). A senior level manager responsible for ensuring an impartial, quality control review of the SCAP, who makes recommendations to the ISS Certifier and the DAA, as appropriate. The certification agent signs the final ISS certification document before forwarding to the ISSM for review prior to the DAA deciding whether or not to authorize the system.

ISS Certifier (ISSC). A senior manager in the developmental or operational organization that owns the information system and is responsible for certifying that system security technical controls are present and functional, management and physical controls are described and in place, and risk has been mitigated commensurate with magnitude of harm.

ISS Manager (ISSM). A Federal employee who is responsible for implementing the agency's ISS Program within a single line-of-business or staff office.

ISS Plan (ISSP). A document that identifies the information system components; operational environment; sensitivity and risks; and detailed, cost-effective measures to protect a system or group of systems. The ISS plan must be maintained throughout the system life cycle and is complete when selected controls are tested and the responsible FAA official signs the SCAP.

Life Cycle. There are two categories of life cycle:

- a. **Information.** The stages through which information passes typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.
- b. **Information System.** The phases through which an information system passes typically characterized as initiation, development, operation, termination, and decommissioning.

Major Application. An application that requires special attention to security because of the risk and magnitude of the harm that could result from the loss, misuse, or unauthorized access to, or modification of, the information in the application. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components.

Management Board. The FAA Management Board is chaired by the Administrator, and its membership consists of the Deputy Administrator, Assistant and Associate Administrators, and other staff members as designated by the Administrator.

Mission Support System. Systems that are not used for operational air traffic control services, but are unique to the performance of the FAA's mission.

Mutual Recognition Arrangement (MRA). An agreement between two or more entities to accept Common Criteria certifications and validations completed by the other members of the arrangement

Network. Communications hardware and software that allow one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area networks (LAN), or wide area networks (WAN), and public networks like the Internet.

Non-critical System. Any information system that is not a critical system.

Non-FAA Facility. Any facility that is not owned or leased by the FAA where FAA information systems, or any portion of FAA information systems, will be developed, housed, or operated or where FAA information is collected, stored, processed, or transmitted. It is not necessary that the equipment used is owned by the FAA, only operated on behalf of or connected to FAA information systems.

Operational Controls or Operations. The day-to-day administrative, physical, technical, and procedural mechanisms used to protect operational systems and applications.

Penetration Testing. Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

Personnel Security Program. This program provides a basis for security determinations for sensitive positions, clearances for access to classified material, and suitability for Federal employment. The authority for this program is the same as that for the investigations program. Order 1600.1, Personnel Security Program, provides internal guidance.

Physical Security. The combination of security controls that bar, detect, monitor, restrict, or otherwise control access to sensitive areas. Physical security also refers to the measures for protecting a facility that houses ISS assets and its contents from damage by accident, malicious intent, fire, loss of utilities, environmental hazards, and unauthorized access. FAA Order 1600.69, FAA Facility Security Management Program, defines the physical security program.

Protection Profile. A combination of security requirements, including assurance and functional requirements, with the associated rationale and target environment to meet identified security needs. A protection profile is included in the SCAP.

Protection Profile Certification. Certification issued by an accredited Common Criteria evaluation facility that the protection profile contains requirements that are justifiably included to counter stated threats and meet realistic security objectives, internally consistent and coherent, and technically sound.

Public Trust Position. A position that has the potential for action or inaction by an incumbent to affect the integrity, efficiency, or effectiveness of assigned Government activities.

Risk. The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack.

Risk Acceptance. Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the sensitivity and criticality of the information protected.

Security Certification and Authorization Package (SCAP). A document presented to the DAA for final authorization of the system. The SCAP includes the ISS plan, vulnerability assessment report, risk assessment, security test plan and security test results, disaster recovery and contingency measures, and ISS certification and authorization statements.

Security Compliance Review. Assessments at FAA facilities, which are coordinated with a DAA, facility management, and, if applicable, the Contracting Officer, that examine operational assurance as to whether a system is meeting stated or implied security requirements, including system and organizational policies.

Security Target. A set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified product or system in response to a chosen protection profile.

Sensitive Security Information. See **Information**.

Site Surveys. A visit to a non-FAA facility to assess the level of implementation of the FAA ISS Program and compliance to FAA orders, policies and procedures as stated in a contract, MOU, MOA, or agreement, or any

internal security plans requested by the FAA. These surveys are led by AIO and coordinated with the developer, facility management, and contracting officer.

System. An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, or controlling information with a minimum of human interventions.

System Authorization. A formal declaration by the DAA who has fiscal and operational responsibility that an information system is approved to operate in a particular security mode using a prescribed set of countermeasures. This is the official management authorization for operation and is based on information provided in the Security Certification and Authorization Package (SCAP) as well as other management considerations. The authorization statement affixes security responsibility with the DAA and shows that due care has been taken for security.

System Certification. Comprehensive evaluation of the technical and non-technical security features of an information system and other countermeasures, made in support of the authorization process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

System Owner. The manager responsible for the organization that sets policy, direction, and manages funds for an information system. Systems under development are owned by the developing organization until accepted and authorized by the operating organization.

Threat. Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

User. An employee, contractor, subcontractor; Federal, State, and local government agencies; authorized domestic and international aviation industry partners; and authorized foreign governments having access and use of FAA information or FAA information systems, nationally or internationally.

Vulnerability. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to an information system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow an information system or activity to be harmed by an attack.

APPENDIX 2. OPERATIONAL REPORTING RELATIONSHIP BETWEEN KEY ISS FUNCTIONS

This chart depicts the operational reporting relationship between the key ISS functions in the FAA.

