U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
National Policy

ORDER 1370.106

Effective Date:
06/16/09

SUBJ: Information Systems Security Awareness and Training Policy

1. Purpose of This Order. This Order establishes the Federal Aviation Administration (FAA) Policy for an agency-wide Information Systems Security (ISS) Awareness and Training Program. This Order assigns the framework, roles, and responsibilities for the ISS Awareness and Training Program. Employees represent one of the most significant vulnerabilities to security, and individuals' actions can positively or negatively affect the confidentiality, integrity, and availability of information and information systems.

2. Whom This Order Affects. This Order applies to all FAA employees, contractor personnel, and others who are responsible for or have access to the FAA information systems and the sensitive data and information contained therein; such as, FAA lines of business and staff office (LOBs/SOs), Assistant and Associate Administrators. "Others" include FAA employees paid by FAA and/or private entity; Federal employees, including the Department of Defense, who have access to the FAA information systems; and grantees, consultants, licensees, and any person or entity, domestic or foreign, that have a formal written agreement with the FAA.

3. Where Can I Find This Order? This Order is available on the FAA's Intranet website at the URL https://employees.faa.gov/tools_resources/orders_notices/.

4. Scope.

a. This Order establishes an agency-wide ISS approach that supports the FAA's ISS Awareness and Training Program. Federal statutes and regulatory requirements defined in the National Institute of Standards and Technology (NIST) Special Publications (SP) establish the requirements and recommendations of this Order. This Order does not address facility, personnel, or privacy awareness training or National Security Systems (NSS), computer systems that process classified information. Any questions regarding NSS should be directed to the Assistant Administrator for Security and Hazardous materials (ASH-1).

b. This Order applies to all personnel accessing FAA-owned or FAA-controlled information systems. An FAA-controlled information system or device is one that, although may be owned by another entity (such as a contractor), is used in performing agency work.

5. General. In accordance with the Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, annual security training and the Rules of Behavior for system users will be tailored to what a user needs to know to use the system securely, given the sensitivity of the information. As stated in OMB A-130, Appendix III, "Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system." The OMB A-130, Appendix III, ensures

that security is incorporated into agency systems and budgets, authorizes NIST to provide guidance for security efforts, and gives agencies responsibility for establishing minimum security controls.

6. Statutory Policy and Regulatory Mandates.

a. The Federal Information Security Management Act of 2002 (FISMA) states that each Federal department and agency must include security awareness training within an agency-wide information security program. The security awareness training must inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures to reduce risks. The FISMA also requires each agency to include as part of its performance plan a description of the resources, including budget, staffing, and training, that are necessary to implement the program.

b. The Computer Security Act of 1987 requires that each Federal agency provide "mandatory periodic training in computer security awareness and accepted computer security practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."

c. The OMB Circular A-130, Appendix III, Management of Federal Information Resources, states that personnel be trained in their responsibilities and be addressed in the security plan for each information system. Federal departments and agencies must implement policies, standards, requirements, and procedures that are consistent with standards and guidance issued by NIST. The OMB A-130, Appendix III also requires that: "The head of each agency must ensure that the agency develops a well-trained staff of information resource professionals."

d. The Office of Personnel Management (OPM) Regulation 5 CFR Subpart C 930.301, Information Security Responsibilities for Employees who manage or Use Federal Information Systems, provides specific direction regarding the nature and content of the training for categories of information technology users and supports the requirements established by FISMA.

(1) According to the 5 CFR Part 930, OPM requires that Federal agencies identify employees responsible for the management or use of computer systems that process sensitive information and to provide training to the following groups: executives, program and functional managers, chief information officers (CIO), Information Technology (IT) security program managers, auditors, other security-oriented personnel, IT function management and operations personnel, and end users.

(2) In addition, OPM requires that employees in these groups receive their required training within 60 days of their appointment in accordance with 5 CFR Subpart C 930.301. The OPM also requires that additional training be provided whenever there is a significant change in the agency ISS environment or procedures or when an employee enters a new position involving the handling of sensitive information. The FAA requires annual training to constitute computer security refresher training.

7. References.

a. NIST SP 800-16, Information Technology Security Training Requirements: A Role and Performance Based Model, April 1998.

b. NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006.

c. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

d. NIST SP 800-53, Revision 2, Recommended Security Controls for Federal Information Systems, December 2007.

e. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, December 2007.

f. Department of Transportation Order 1350.2, Departmental Information Resource Management Manual (DIRMM), Chapter 10.

g. FAA Order 1370.82A, Information Systems Security Program, September 11, 2006.

h. FAA Federal Aviation Personnel Manual, Letter 2635, Conduct and Discipline, November 16, 1989.

i. FAA Human Resources Policy Manual (HRPM) Volume 4: Employee Relations (ER) 4.1, July 14, 2008.

8. Definitions. Definitions of specialized terms used in this subject area, with relevant abbreviations and acronyms are listed in this Order below. All other definitions located in this Order that pertain to ISS are stated in the FAA Order 1370.82A, Appendix B.

a. Awareness Training. A learning process intended to focus individual and organizational attitudes, perceptions, and behavior on specific issues or concerns. Awareness can be a precursor to training and often takes the form of a presentation or briefing.

b. Computer Security Training. Training in the specifics of computer security techniques, practices, and concepts.

c. Education. A formal program administered by an accredited college or university that integrates various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (i.e., technological and social).

d. Industry Certification. Professional standards which integrate training, education, and experience with an assessment mechanism to validate knowledge and skills resulting in a "certification" to a predefined level of competence.

e. Industry Based Training. Industry or employer provided training intended to develop competency and understanding in a specific discipline or function. This type of training seeks to teach skills that allow a person to perform a specific function.

f. Professional and Continuing Education. Professional continuing education is a specific learning activity characterized by the issuance of a certificate or continuing education units (CEU). The certificates or CEUs document attendance at a designated seminar or course of instruction. The seminars, or courses of instruction, expand a professional's knowledge base commensurate with their ISS roles and responsibilities and enables them to stay current on new developments. The education can be delivered through college or university course work, extension courses, conferences, and seminar attendance.

g. Specialized or Role-Based Training. Specialized or role-based training provides ISS courses that are tailored to the specific needs of personnel, such as key ISS personnel or managers and supervisors, who have been identified as having significant responsibilities for information security in their organization.

h. Training. The acquisition of knowledge, skills, and competencies as a result of the teaching of vocational or practical skills and knowledge that relate to specific useful competencies.

9. Notice of Exception or Noncompliance.

a. This Order establishes policy to comply with statutory and regulatory requirements, including NIST information systems security publications made mandatory by FISMA. Compliance to the policy established by this Order is mandatory.

b. Penalties for user noncompliance with this Order are subject to actions in accordance with existing policy and regulations, applicable union contracts and/or HRPM ER 4.1, Standards of Conduct, and the accompanying Human Resources Operating Instructions Table of Penalties. These penalties include written reprimands, suspension of system privileges, temporary suspension from duty, and removal from current position or termination of employment. The FAA will enforce the use of penalties against any user who violates the FAA or Federal systems security policy or order as appropriate.

10. Information Systems Security Awareness Policy. A key objective of an effective Federal ISS program is to ensure that all FAA employees and contractor personnel understand their roles and responsibilities and are adequately trained to perform them.

a. All FAA employees and contractor personnel must complete annual security awareness training provided by the agency.

b. The FAA must provide security awareness training for all FAA employees and contractor personnel no later than 30 days after they have accessed any FAA information system. Access will be terminated until ISS awareness training is received.

c. Security awareness training records must be maintained to include name and position, title, type of training received, date, and cost of training.

d. The FAA must continuously reinforce ISS awareness training by facilitating cyber security training events, conferences, and other communication media, such as posters and newsletters.

11. ISS Role-Based Training Policy. The FAA employees and contractor personnel having significant security responsibilities (e.g., Information System Security Officer, System and Network Administrators) must receive role-based training specific to their security responsibilities. The policy statements below promote a consistent understanding of information assurance principles, evolving system security, and network changes.

a. Annual role-based training must commensurate with the FAA employees and/or contractor personnel's roles and responsibilities.

b. Role-based training must be tracked for all FAA employees and contractor personnel.

c. Role-based training records must include: name, ISS job function, training, description of the training received, dates, and cost of training.

d. The FAA employees training records must be maintained in the FAA's enterprise Learning Management System (eLMS) and contractor personnel training records must be maintained in the FAA's Information Systems Business Portal (ISBP).

e. Role-based training may include external training from other resources (i.e., industry certifications, seminars, or formal course work provided by an accredited college or university).

f. Role-based training must be completed within the calendar year of any significant change in the FAA's ISS environment or procedures.

12. ISS Certification and Continuing Education. All FAA organizations are encouraged to support ISS personnel obtaining ISS-related certifications and continuing education from external professional organizations.

a. The level of training required for the certification and continuing education must be appropriate with the individual's duties and responsibilities.

b. Certifications and continuing education must be tracked for all FAA employees in eLMS (i.e., by name, ISS job function, the type of certification and continuing education received, training title and description, dates, and cost of the training).

13. Roles and Responsibilities. All FAA organizations must comply with the roles and responsibilities per the FAA Order 1370.82A and carry out the additional responsibilities as follows:

a. The FAA Associate and Assistant Administrators must:

(1) Complete initial and annual ISS awareness training and other training commensurate with their roles and responsibilities;

(2) Oversee completion of FAA employees' individual training plan, ISS awareness and specialized training documentation; and,

(3) Maintain a separate file of completed training for each individual identified as key ISS personnel, whether FAA employees or contractor personnel.

b. The FAA Chief Information Officer (CIO) is the agency focal point for providing agency-wide ISS training to all personnel.

c. The FAA Chief Information Security Officer (CISO) must:

(1) Review and evaluate ISS awareness training for the FAA as required by Federal statutes, regulatory requirements, and guidance provided by the NIST.

(2) Track and report to the CIO all FAA employees and contractor personnel who have met the FAA agency-wide security awareness and training requirements by the deadline established by the Department of Transportation or FAA.

(3) Develop, evaluate, and maintain the FAA ISS Awareness, Training, and Education Program for the FAA (e.g., ISS annual conference).

(4) Facilitate agency-wide key ISS personnel role-based training (e.g., ISS awareness training cyber security training events, conferences, and other communication media, such as posters and newsletters) or fund alternative role-based training methods.

(5) Determine the appropriate media for providing ISS awareness training (e.g., seminars, presentations, awareness video tapes, and computer-based products delivered via CD-ROM, Intranet, Internet, and LAN).

(6) Track and report all key ISS personnel role-based training annually to the FAA CIO.

d. The LOBs/SOs must ensure:

(1) New FAA personnel and contractors complete security awareness training within 30 days of their appointment.

(2) Key ISS personnel training must be completed within the calendar year of a significant change in the FAA's ISS environment or procedures or when an employee enters a new position involving the handling of sensitive information.

(3) Security awareness training records must be maintained for their affected FAA employees and/or contractor personnel to verify compliance.

(4) Continuous reinforcement and support to the ISS training conferences and events.

e. The ISSMs, in coordination with the AIS-200 division, must ensure that all key ISS personnel role-based ISS training is reported in the AIS-200 Information Systems Business Portal (ISBP).

f. The Supervisors and Managers must:

(1) Include documented roles and responsibilities in key ISS personnel annual performance plan and position description.

(2) Obtain appropriate information regarding system security training requirements for key ISS personnel from their ISSMs before authorizing personnel to gain access to the system or performing their assigned duties.

(3) Provide appropriate ISS training for key ISS personnel.

(4) Ensure that key ISS personnel training is recorded in eLMS.

(5) Maintain training records that include key ISS personnel name and position, title, type of training received, date, and cost of training.

(6) Maintain approved FAA employees' personnel requests for ISS-related professional certifications and continuing education.

(7) Maintain key ISS personnel records for all training received from resources other than those provided by the FAA (e.g., approved industry certifications, seminars or formal course work provided by an accredited college or university) in eLMS or personnel file, as applicable.

g. The key ISS personnel must:

(1) Complete ISS-specific training as defined in their performance management plan.

(2) Review their training records and bring any discrepancies to their supervisor's and manager's attention.

(3) Obtain management approval for all FAA funded professional certifications and continuing education requests.

(4) All key ISS personnel must complete annual role-based ISS training according to job function.

h. All FAA employees and contractor personnel must:

(1) Complete the ISS awareness training no later than 30 days after they have accessed any FAA information system.

(2) All key ISS personnel must complete annual security awareness training.

14. Administrative Information.

a. The Assistant Administrator for Information Services and CIO can issue changes to the FAA Information Systems Security Program.

b. Each LOB and SO may develop additional guidance and procedures to ensure compliance with this Order. All FAA organizations are encouraged to go beyond the requirements of this Order to address business, operational, and security needs; but, the requirements of this Order must not be reduced.

15. Distribution. This Order is distributed to divisions in headquarters, regions, and centers with information systems or information systems security responsibility. Headquarters, regions, and centers must send this Order to all field offices and facilities within 30 days.

David M. Bowen
Assistant Administrator for Information Services
and Chief Information Officer