



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

ORDER
1370.113

Effective Date:
04/16/12

SUBJ: Web Security Management Policy

1. Purpose of This Order. This Order establishes the Federal Aviation Administration's (FAA) enterprise-wide Web Security Management Policy. This order outlines the policies, roles and responsibilities for developing, managing and maintaining web systems. This order will assign the framework, mandatory standards, procedures, and security and privacy requirements for the FAA web environment.

2. Whom This Order Affects. This Order applies to anyone with the responsibility to develop, manage, and maintain websites (Internet, Intranet and Extranet). This Order also applies to anyone who is responsible for or has authorized access to the FAA information systems including Sensitive Unclassified Information (SUI), Sensitive Security Information (SSI), and Personally Identifiable Information (PII). This does not include systems that process or store classified information.

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

4. Background.

a. The FAA Web refers to all FAA web systems including websites available to the public (Internet); access controlled websites for external audiences that require authentication (Extranet); and Intranet websites for which FAA organizations have primary content responsibility, whether they are on the faa.gov server, another FAA-owned or leased server, an Intranet server or a server belonging to a contractor supporting an FAA website.

b. The FAA websites provide FAA employees and the public with access to information and services. These websites must be properly configured and maintained in order to protect the integrity of FAA information. The FAA public facing websites present a highly accessible point of entry and attack to FAA information resources. As a result, it is essential to secure web servers and the network infrastructure that supports them. The FAA must apply effective security controls upon configuration, deployment, and during ongoing maintenance. This Order provides web security requirements that will protect FAA information and data being used on the web o avoid data security breaches.

5. Scope. This policy is designed to assist FAA employees and contract personnel with the secure development, management, maintenance, and use of the FAA websites/services (Internet, Intranet, Extranet) to enhance security on web systems. Any third party websites and social media websites are not within the scope of this policy. This policy addresses:

- a. Implementing and maintaining security controls for web servers, such as those that provide Internet and email services;
- b. Protecting FAA web information and data from unauthorized access, use, disclosure, disruption, modification, or destruction;
- c. Protecting the FAA network from external threats delivered over the web, such as viruses, malicious attacks, data leaks, etc;
- d. The System Authorization process for web systems as part of the FAA-wide Information Systems Security (ISS) Program;
- e. Ensuring that authentication processes are in place that provide the appropriate level of assurance for web-based access and FAA online services;
- f. Ensuring that security controls are implemented in all phases of the System Development Lifecycle (SDLC) for systems within the FAA web environment; and
- g. Establishing and implementing clear privacy policies for the FAA web environment.

6. Web Security Management Policy. The implementation of adequate security controls to protect web servers, database servers, and communication protocols from unauthorized access, denial of service attacks, command injection attacks, malicious attacks, and phishing etc. Below are the minimum security/privacy requirements and management controls that must be met for the FAA web environment:

- a. Each FAA website being developed by the Line of Business (LOB)/Staff Office (SO) must be registered with the Office of Communications (AOC) prior to deployment;
- b. The FAA must use only .gov, .mil, or Fed.us domains unless explicitly authorized by the AOC. All FAA domains must be registered with the AOC prior to deployment. This is required in accordance with the domain naming conventions as defined in the Office of Management and Budget (OMB) Memorandum M-05-04, Policies for Federal Agency Public Websites that requires Federal agency public websites to be a part of the agency's information resource management program;
- c. All FAA employees developing content for web pages or applications for FAA websites must comply with FAA Order 1370.93, FAA Web Management Policy;
- d. An information sensitivity determination must be conducted on the type of information being published to determine the level of protection for the information. Information is categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, the Information Systems Security Plan and the Information Systems Security Authorization Handbook;

e. Each FAA LOB/SO that designs, develops, or implements web applications must ensure that a minimum set of security requirements are implemented as part of their SDLC as defined in FAA Order 1370.112, FAA Application Security Policy, and the FAA Order 1370.109, Software Assurance Policy, as well as, FAA application standards for building secure information systems;

f. The FAA must implement security controls as required in OMB Circular A-130, Appendix III. All FAA-owned and operated web servers and web applications must secure the systems utilizing guidelines contained in FAA Orders and the National Institute of Standards and Technology (NIST) Special Publications (SP). The FAA Order 1370.82A, Information Systems Security Program, establishes the FAA policy on information and information systems security and the minimum security controls that must be in place. The minimum security controls for the systems must be documented in the ISSP;

g. Adherence to the minimally acceptable system baseline configurations as required by the Federal Information Security Management Act (FISMA), the Change Control Boards for each LOB/SO, and the FAA Information Security Standards published by the Office of Information Systems Security (AIS) and web infrastructure standards approved by the Information Technology Shared Services Committee and NIST 800-44, Guidelines on Securing Public Web Servers;

h. Websites using electronic authentication (e-authentication) for web-based access must have controls properly implemented that allow an individual person to remotely authenticate his/her identity to a Federal IT system. The FAA must follow the OMB Memorandum M04-04 for e-authentication, that provides guidance to ensure that online government services are secure and protect privacy, and that some type of identity verification or authentication is implemented;

i. A system authorization, in accordance with the FAA Information Systems Security Authorization Handbook, must be conducted for all new web applications or those undergoing significant changes in compliance with FISMA. This must include conducting security risk assessments (including when significant changes to the system configuration or to the operational/threat environment occur) and security vulnerability assessments;

j. Websites must display an approved system use notification message or banner before granting access to the system in accordance with the FAA Order 1370.79A, Internet Use Policy, and the FAA Order 1370.102, System Use and Notification Disclaimer Statement;

k. Websites must display appropriate privacy statements in accordance with FAA Order 1280.1B, Protecting Personally Identifiable Information (PII) and FAA Privacy and Website policy located at <http://www.faa.gov/privacy/>. A link to the official privacy policy must be posted on all the FAA public websites, each FAA web-based system, and all major entry points to the FAA network. If applicable, a Privacy Threshold Analysis, a Privacy Impact Assessment (PIA), and System of Record Notice (SORN) may be required and posted in accordance with the FAA privacy policy;

l. Use of tracking cookies shall be utilized in accordance with OMB M-00-13, Privacy Policies and Data Collection on Federal Websites and FAA Order 1280.1B, Protecting Personally Identifiable Information (PII) and Website policy;

m. If using a non.gov presence or third party content application, the FAA website must display a warning banner that explains that the website is not a government site, and that it is controlled or operated by a third party, and that the FAA privacy policy does not apply. This regulation is in accordance with OMB M -10-23, Guidance for Agency Use of Third-Party Websites and Applications;

n. The FAA must examine the third party's privacy policy to evaluate risks and determine whether the website or application is appropriate for use, monitor any changes to the third party's privacy policy, and minimally reassess the risks on an annual basis or when there is a change in system configuration; and

o. The FAA must encrypt all SUI, SSI, and PII in accordance with FAA Order 1370.103, Encryption Policy.

7. Roles and Responsibilities. All FAA organizations must comply with the roles and responsibilities in accordance with FAA Order 1370.82A, FAA Information Systems Security Program and carry out additional responsibilities as follows:

a. The Federal Aviation Administration Chief Information Officer (CIO) must:

(1) Provide Agency-wide information systems security leadership, policy, guidance, and oversight of the FAA Web Security Management Policy; and

(2) Ensure that information owned or maintained by the FAA is protected against unauthorized access, use, modification, or destruction, using Agency-administered security controls.

b. The Lines of Business / Staff Offices must:

(1) Designate in writing a single high level Federal employee to serve as the LOB/SO designated information security representative to ensure that the web systems adhere to the FAA application standards for building secure information systems;

(2) Ensure minimum SDLC requirements for building secure applications;

(3) Follow procedures issued by the AOC to register all websites before launching them. The registration of the websites must be in accordance with requirements detailed in the FAA Order 1370.93, FAA Web Management Policy and the FAA Order 1370.84, Internet Services;

(4) Implement and manage organization-specific, web-enabled applications consistent with the content, design, and development standards established by the AOC; and web infrastructure standards approved by the ITEB;

(5) Ensure that Information Systems Security Officers (ISSO)/Information Systems Security Managers (ISSM) follow the minimally acceptable system baseline configurations established by their Change Control Boards and the FAA Information Security Standards published by AIS; and

(6) Ensure the LOB/SO ISSM examine the third party's privacy policy to evaluate risks and determine whether the website or application is appropriate for use.

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

(1) Oversee the implementation of this order and ensure compliance with FISMA, all FAA, Department of Transportation (DOT) systems security policies, standards, requirements and guidelines; and

(2) Conduct regular ISS compliance reviews to ensure the LOB/SOs have implemented secure web security.

d. The FAA Privacy Officer must:

(1) Ensure appropriate privacy protections exist for PII that are collected, stored, disseminated, transmitted, or disposed of by information systems owned or operated by or for the FAA;

(2) Ensure compliance with all privacy requirements imposed on the FAA under Federal laws, policies, standards, regulations, and guidelines; and

(3) Serve as the principle advocate for FAA employees when PII has been compromised, disclosed, or released to unauthorized persons.

e. The Information Systems Security Managers (ISSMs) must:

(1) Ensure that the appropriate operational security posture is implemented and maintained for the information systems or programs within their LOB/SO;

(2) Ensure the implementation of security controls and requirements to protect information stored on websites;

(3) Coordinate security incidents with the Cyber Security Management Center (CSMC) regarding compromised websites;

(4) Ensure that any deviations from the common security configurations are documented;

(5) Ensure that all security postures are implemented via signed Memorandums of Understanding (MoUs) or Interconnection Service Agreements (ISA) between the hosting facility and the application owner, when one LOB/SO relies on another LOB/SO (or within the same LOB/SO) to host their applications;

(6) Ensure the appropriate implementation of e-authentication for web-based access where required;

(7) Ensure a system authorization is conducted for all new web applications or those undergoing significant changes in compliance with FISMA and the FAA System Security Authorization Handbook;

(8) Ensure that websites display appropriate privacy statements;

(9) Examine any third party privacy policy to ensure risks are evaluated and if the third party website or application is appropriate for use; and

(10) Verify that for a non.gov presence or third party content application, the FAA website displays a warning banner that explains that the website is not a government site, and that it is controlled or operated by a third party, and that the FAA privacy policy does not apply.

f. Information System Owner (ISO) must:

(1) Ensure the development of the websites/applications is in accordance with FAA web content standards, AIS security standards and web infrastructure standards as determined by the ITEB;

(2) Ensure that only .gov, .mil, or Fed.us domains are used;

(3) Conduct an information sensitivity determination of the information being published to determine the level of protection needed;

(4) Ensure that the web security risk management addresses minimum security configurations on web servers' user input validation controls to secure data in storage and transit, session management, and regular maintenance of web servers;

(5) Ensure the documentation of deviations from the common security configurations;
and

(6) Ensure that for a non.gov presence or third party content application, the FAA website displays an alert that explains that the website is not a government site and that and that it is controlled or operated by a third party, and that the FAA privacy policy does not apply.

g. System and Network Administrators must:

(1) Utilize identified security controls and requirements as prescribed in NIST SP 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations to protect websites and web applications; and

(2) Utilize minimum security configurations on web servers' user input validation controls to secure data in storage and transit, session management, and regular maintenance of web servers.

8. Statutory Policy and Regulatory Mandates.

a. The E-Government Act, Public Law 107-347, established the Federal Information Security Management Act (FISMA). The FISMA states that each Federal department and agency must maintain an information security program that is consistent with policies, standards, requirements, and guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and other designated Federal agencies.

b. The Privacy Act of 1974, 5 U.S.C. § 552a, is concerned with the protection of privacy records. Federal agencies must establish controls that safeguard PII and privacy records through the deployment of physical, technical, and administrative controls.

c. The OMB Circular A-130, Appendix III, Management of Federal Information Resources, states that Federal departments and agencies must implement policies, standards, requirements, and procedures that are consistent with standards and guidance issued by the NIST.

d. The OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, states that Federal departments and agencies must appropriately safeguard sensitive personally identifiable information and train employees of their responsibilities in this area.

e. The OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, addresses the implementation and requirements for cookies on Federal websites.

f. The OMB M -10-23, Guidance for Agency Use of Third-Party Websites and Applications, requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public.

g. The OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, requires that the management of agencies' public websites should be in compliance with Federal information resource management law and policy.

h. The OMB Circular A-130, OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (67 FR 5365).

i. FAA Order 1370.82A, Information Systems Security Program, addresses compliance with agency-wide ISS policies, standards, and requirements.

j. FAA Order 1370.93, FAA Web Management, addresses mandatory standards, procedures, and requirements for the FAA web that all FAA Lines of Business (LOB) and Staff Offices must follow.

k. FAA Order 1600.75, Protecting Sensitive Unclassified Information, (SUI) addresses guidance for identifying and protecting sensitive unclassified information.

l. FAA Order 1280.1B Protecting Personally Identifiable Information, (PII) and Website policy that permits the use of cookies and the limitations.

m. FAA Order 1370.79A, Internet Use Policy, establishes policies on the appropriate use of the Internet.

n. FAA Order 1370.102 System Use and Notification Disclaimer Statement.

9. References. References are contained in Appendix A of this Order.

10. Definitions. Definitions of specialized terms used in this subject area, with relevant abbreviations and acronyms, are contained in Appendix B of this Order. All information systems security definitions used in this Order are stated in the FAA Order 1370.82A, Information Systems Security Program, Appendix B.

11. Notice of Exception or Noncompliance.

a. The head of a LOB/SO, ISO, or AO can request the FAA CIO to grant a waiver of compliance. The request must include: (1) justification, (2) what measures or compensating controls already exist, (3) risk acceptance, (4) risk mitigation measures, (5) waiver period, and (6) milestones to achieve compliance. The Authorization Package must include the copy of the request and waiver decision.

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 Employee Relations 4.1, Standards of Conduct, and the accompanying Human Resources Operating Instructions Table of Penalties or if applicable, Federal Aviation Personnel Manual (FAPM) 2635. 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 system security policy or order as appropriate.

12. Administrative Information.

a. The Assistant Administrator for Information Services and the Chief Information Officer (AIO-1) can issue changes to the FAA Information Systems Security Program. The AIO CIO's office approves changes that set policy, delegate authority, and assign responsibility.

b. Each LOB/SO may develop additional guidance and procedures to ensure compliance with this Order. To address individual business, operational, or security needs, FAA

organizations are encouraged to implement more stringent security requirements than those stated in this Order, but the requirements of this Order must not be reduced.

13. 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.

Steve Cooper
Acting Deputy Assistant Administrator
for Information Services and Deputy Chief Information Officer

Appendix A. References

- a.** FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- b.** NIST SP 800-44 version 2, Guidelines on Securing Public Web Servers, September 2007 defines the controls that should be in place to secure public facing websites.
- c.** NIST SP 800-63, version 1.0.2 Electronic Authentication Guideline, April 2006.
- d.** The Department of Transportation (DOT) Order 1351.24, Departmental Web Policy, establishes policies and responsibilities for creating, managing and maintaining the DOT websites for both internal and external audiences.
- e.** The DOT Information Technology and Information Assurance Policy Number 2006-22 (rev 1): Implementation of DOT's Protection of Sensitive Personally Identifiable Information (SPII).
- f.** FAA Order 1370.82, FAA Information Systems Security Program.
- g.** FAA Order 1370.90, Internet Access Point Configuration Management.
- h.** FAA Order 1370.103, Encryption Policy.
- i.** FAA Order 1370.107, Rules of Behavior/System Use Policy.
- j.** FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI).
- k.** FAA Order 1370.112, FAA Application Security Policy.
- l.** FAA Order 1370.109, Software Assurance Policy.
- m.** FAA Information Systems Security Authorization Handbook.
- n.** Minimum System Development Lifecycle (SDLC) Requirements for Building Secure Applications.
- o.** FAA Order 1370.102, ATO Information Security Incident Reporting and Response Policy.

Appendix B. Definitions

Extranet: An extranet is a computer network that allows controlled access from the outside, for specific business or educational purposes. An extranet can be viewed as an extension of a company's intranet that is extended to users outside the company, usually partners, vendors, and suppliers.

FAA-Owned: Equipment or assets that belong to FAA and are used to store FAA specific information / data.

FIPS 140-2, Security Requirements for Cryptographic Modules: This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Intranet: An intranet is a private computer network that uses Internet Protocol technologies to share any part of an organization's information or network operating system within that organization.

Internet: A global public network of independent hosts and communication facilities, which connect users to those hosts. The term internet may refer to the content presented on hosts or transmitted through the network.

Personally Identifiable Information (PII): Any information about a human being, living or deceased, regardless of nationality, that is maintained by an agency. This includes information that permits identification of that individual to be reasonably identified by either direct or indirect means (i.e., as in data mining). The following types of information are included, but not limited to: name, home address, social security number, driver's license identification number, date and place of birth, mother's maiden name, biometric records, education, financial transactions, medical information, non-work telephone numbers, and criminal or employment history (including any other personal information that is linked or linkable to an individual).

Sensitive Security Information (SSI): SSI is a designation *unique* to the DOT and DOT's operating administrations and to the Department of Homeland Security (DHS). It applies to information we obtain or develop while conducting *security activities*, including research and development activities. Title 49 CFR Part 15 governs the maintenance, safeguarding, and disclosure of records and information that the Secretary of DOT has determined to be Sensitive Security Information.

Sensitive Unclassified Information (SUI): Any unclassified information in any form including: print, electronic, and visual and audio forms that must be protected from unauthorized disclosure outside of the FAA. The SUI is subject to limited, controlled distribution within the FAA as determined by the information steward. This includes personally identifiable information, aviation and homeland security, and protected critical infrastructure information, all of which may qualify for withholding from the public under the FOIA, 5 USC § 552.