



**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION**

National Policy

**ORDER
1370.112**

**Effective Date
10/05/10**

SUBJ: FAA Application Security Policy

1. Purpose of This Order. This Order establishes policy for the Federal Aviation Administration (FAA) to mandate adherence to the 1) FAA Application Standards for Building Secure Information Systems and 2) FAA Minimum System Development Life Cycle (SDLC) Requirements for Building Secure Applications to promote the implementation of secure information systems throughout the FAA. This policy seeks to ensure:

a. the establishment of the minimum required SDLC activities that must be included in all FAA software system development efforts, regardless of the platform or the lines of business staff office's (LOB/SO) iterative or traditional life cycle process in use; and

b. that the LOB/SOs, all program and project managers, and all software development teams adequately plan for security by properly identifying, assessing and mitigating risks; including security controls in the software system design; adhering to agency and Federal Information Technology (IT) policies and regulations, and continually monitoring and assessing security through system retirement.

2. Whom This Order Affects. This Order applies to all FAA personnel and contractors who initiate, manage, develop or maintain FAA software products, regardless of the front-end user interface (Web or non-Web) to include all agency and LOB/SO executive managers, Chief Information Officers (CIO), Chief Information Security Officers (CISO), Information System Security Managers (ISSM), Information System Security Officers (ISSO), Information System Owners (ISO), Federal Acquisition Executive, and all program/project managers, software developers, quality assurance staff and network and system administrators.

3. Where Can I Find This Order? This Order can be found on MyFAA Website using URL: https://employees.faa.gov/tools_resources/orders_notices/.

4. Background. The Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, Title III, requires that Federal agencies safeguard their information systems. Federal Information Processing Standards Publication (FIPS) 200 further requires that Federal agencies apply the minimum security requirements in Federal information systems as defined in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems and NIST Special Publication 800-64, Security Considerations in the System Development Life Cycle. These Federal standards require that each agency have documented SDLC guidelines that support its business needs and complements its unique culture.

5. Where Can I Find The Application Standards and Minimum SDLC Requirements? The FAA Application Standards for Building Secure Information Systems and the Minimum System Development Life Cycle (SDLC) Requirements for Building Secure Applications can be found on MyFAA Website using URL:

https://intranet.faa.gov/faaemployees/org/staffoffices/aio/programs/ito/app_standards/

6. Scope. This Order applies to all FAA-owned and FAA-controlled information systems, including any customized software acquired from any third party, whether open source, Government-off-the-shelf, or Commercial-off-the-shelf software. This policy does not apply to operating systems.

7. Statutory Policy and Regulatory Mandates.

a. The E-Government Act Public Law 107-347, passed and signed into law by the President in December 2002, established the FISMA.

b. The FISMA requires that Federal agencies perform periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls with a frequency depending on risk, but no less than annually.

c. The Office of Management and Budget (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.

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

9. Definition. For the purposes of this policy, the System Development Life Cycle (SDLC) is defined as the complete project life cycle for the initiation, planning, construction, operations, maintenance, retirement, and disposal of software products, and “new information systems” are defined as applications that have never been approved for development or whose software and/or database are being ported to a new technology.

10. Application Security Policy Statement. All new information systems, which begin after the effective date of this policy, must follow 1) FAA Application Standards for Building Secure Information Systems and 2) FAA Minimum System Development Life Cycle (SDLC) Requirements for Building Secure Applications. During software development or software acquisition, all FAA applications must be assessed to determine compliance with the FAA Application Standards for Building Secure Information Systems. Prior to production operations, the information system will be authorized, and the authorization will be maintained in accordance with the authorization process defined in the FAA Certification and Accreditation (C&A)/Authorization Handbook, led by the LOB/SO ISSO or ISSM.

Any LOB/SO specific software development guidance must be reviewed by a LOB/SO designated information security representative to ensure that the guidance includes these FAA

Application Standards and Minimum SDLC Requirements. The Acquisition Management System (AMS) life cycle process has been reviewed and confirmed to contain these FAA Minimum SDLC Requirements. FAA acquisition projects must continue to follow the AMS life cycle process.

11. 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 the FISMA. Compliance with the policy established by this Order is mandatory.

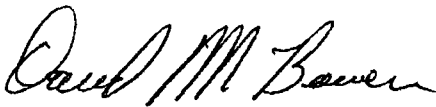
b. The head of a LOB/SO, ISO, or Authorizing Official can request the FAA CIO to grant a waiver of compliance based on a compelling business reason. The request must include: (1) justification, (2) what measures or compensating controls already exist, (3) risk acceptance, (4) risk mitigation measures, (5) waiver period, and (6) milestones to achieve compliance. The certification and accreditation package must include the copy of the request and waiver decision. The FAA CIO will respond to each waiver request within 30 business days.

12. Administrative Information.

a. The Assistant Administrator for Information Services and the Chief Information Officer (AIO-1) can issue changes to the FAA Application and Information Systems Security Programs. 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. All FAA organizations are encouraged to go beyond the requirements of this Order to address business, operational, or security needs; however 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.



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

Appendix A: References

1. Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, Title III
2. Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems
3. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
4. NIST Special Publication 800-53 Rev 2, Recommended Security Controls for Federal Information Systems
5. NIST Special Publication 800-53 Rev 3, Recommended Security Controls for Federal Information Systems
6. NIST Special Publication 800-64, Security Considerations in the System Development Life Cycle (SDLC)
7. Section 208 of the E-Government Act and accompanying OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003
8. Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources