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

ORDER 1370.109

Effective Date:
10/23/09

SUBJ: Software Assurance Policy

1. Purpose of This Order. This Order establishes a Security Software Assurance policy for the Federal Aviation Administration (FAA) to protect the confidentiality, integrity, and availability of FAA information systems. Software Assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This policy includes:

a. Establishing a methodology for ensuring software assurance security for software in development, operation, and maintenance phases;

b. Determining if software code designs are securely written, implemented and operating as intended while protecting information systems and their components;

c. Utilizing approved tools purchased for Agency-wide use, to verify and validate the software contained within an information system is compliant with accepted security practices to reduce patch management activities as noted in URL: https://intranet.faa.gov/faaemployees/org/staffoffices/aio/programs/iss/software_code_vulner_scan_serv/ ;

d. Assigning accountability to software developers to provide secure quality deliverable products that perform as expected; and,

e. Assigning responsibility for Federal Acquisition Executive (FAE) to add contractual requirements to ensure quality of delivered software products.

2. Background. The System Development Lifecycle (SDLC) described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64, "Security Considerations in the System Development Life Cycle", defines the systems process into phases for the development and comprehensive testing of system products. This is the basis for the software assurance methodology described in this Order. This approach to systems development leads to well documented systems that are easier to test and maintain. Integrating a software assurance methodology provides for more effective security measures during the development process, and ensures security safeguards are integrated into the system during its design.

3. Whom This Order Affects. This Order applies to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Information System Owners (ISO), software developers, and Federal Acquisition Executive (FAE), who are responsible for developing or maintaining software.

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

5. Scope. This Order applies to all FAA-owned and FAA-controlled information systems software codes, including any customized software code acquired from third party, open source, Government-off-the-shelf (GOTS), or Commercial-off-the-shelf (COTS) software. In addition, this Order sets the criteria for evaluating testing tools that identify software deficiencies so that defects are uncovered and remediated. The scope of this policy includes examination of software as well as execution of that software code in various environments and conditions. This policy does not apply to operating systems, single user applications, and utility software.

6. Statutory Policy and Regulatory Mandates.

a. The E-Government Act Public Law (P.L.) 107-347, passed and signed into law by the President in December 2002, established the Federal Information Security Management Act (FISMA).

b. The Federal Information Security Management Act of 2002, (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 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 National Institute of Standards and Technology (NIST).

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

8. 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.

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

b. The head of a Line of Business/Staff Office (LOB/SO), ISO, or AO 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 (C&A) package must include the copy of the request and waiver decision.

10. Software Assurance Policy. Software assurance assessment is the set of activities that involve the evaluation of software, with the intent of identifying vulnerabilities while providing a level of confidence that the software meets its security requirements. Testing involves operation of a system or application under both normal and abnormal conditions and evaluating the results to ensure identified vulnerabilities are not exploitable within its intended environment. This policy assigns responsibility and accountability to each FAA line of business to determine their critical applications or systems that are to be assessed including frequency of testing and review of code for compliance with this order. For systems under development, the schedule for code reviews must be performed at key intervals (i.e., string testing, system regression/integration testing, and acceptance testing). In order to securely assess software, the FAA must adhere to the following:

a. Software assurance security assessments must have the ability to conduct static and dynamic analysis when possible on the binary executables of software code or can be manually tested at the discretion of the LOB/SO;

b. Software assurance security assessments must comply with the standards from the NIST National Vulnerability Database (NVD) located at URL: http://nvd.nist.gov/;

c. Software assurance assessments must categorize identified vulnerabilities using the Common Vulnerability Scoring System (CVSS) and adhere to the Common Weakness Enumeration (CWE) dictionary for software weakness types. Information about these standards can be found at http://nvd.nist.gov/cvss.cfm and http://nvd.nist.gov/cwe.cfm;

d. Vendor technologies used to perform software assurance assessments are referenced in the NIST Software Assurance Metrics and Tool Evaluation (SAMATE) list; and,

e. Security test planning and/or execution must be performed during the below affected phases of the SDLC, following the NIST Special Publication (SP) 800-64 and FAA guidelines, as stipulated:

(1) Initiation Phase**:**

(a) During the initiation phase of the SDLC, security considerations are key inputs to reliable and early integration, thereby ensuring the information security threats, requirements, and potential constraints in functionality and integration are considered. Key security activities for this phase include:

1. Identify the type of application(s) that will need to be created and determine if these products will be developed in-house, outsourced, GOTS or COTS;

2. Assess business impact categorization characterization of the system requirements, processes, and interdependencies and applies this information to determine contingency requirements;

3. Initial description of business requirements in terms of confidentiality, integrity, and availability; and,

4. Ensure information categorization and identification of known special handling requirements to transmit, store, or create information, such as personally identifiable information and privacy requirements.

(2) Development and Acquisition Phase:

(a) Software developers must regularly review in-house developed code for common programming errors as identified by NIST, CVSS, CWE, and other FAA approved sources. These common errors include: memory leaks, cross-site scripting vulnerabilities, buffer overflows, race conditions, object model violations, poor user input validation, poor error handling, exposed security parameters, passwords in the clear, and violations of stated security policy, models, or architecture;

(b) Assess and include any security testing criteria in the initial software development or during the GOTS or COTS product evaluation process;

(c) All acquisitions of GOTs, COTs, in-house developed or outsourced products within the scope of this policy must undergo an independent third party software assurance assessment;

(d) A software assurance assessment report identifying vulnerabilities in accordance with this policy must be provided to the FAA; and,

(e) Government acceptance criteria must require that all identified security vulnerabilities have a remediation plan that is mutually agreed upon by the FAA and the vendor.

(3) Implementation and Installation Phase:

(a) Prior to initial operations, a software assurance assessment must be conducted to assess the extent to which the software controls are implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;

(b) All software code being developed or being modified, must undergo a final software assurance assessment to ensure that all identified vulnerabilities represent an acceptable level of risk to the FAA prior to being granted authority to operate; and,

(c) Vulnerabilities identified in a software assurance assessment report must be incorporated into a POA&M report for vulnerability acceptance and remediation tracking as part of the C&A process.

(4) Operations and Maintenance Phase:

(a) Periodic testing and evaluation of the effectiveness of all software must be performed with a frequency depending on the level of risk. For existing COTS products, it is acceptable for the vendor to provide an FAA approved third party software assurance assessment to validate that their software code was assessed;

(b) Software modifications require a software assurance assessment, and newly identified vulnerabilities must be remediated or accepted for risk prior to being re-introduced to the FAA operational environment;

(c) Modifications (e.g., upgrades, patches, hot fixes) to the information systems or environment that interacts with the software code may also warrant another software assurance assessment to be conducted. The need for this software assurance assessment will be at the discretion of the system's ISSO;

(d) Software assurance assessments must be conducted on any affected or potentially affected software following a software-related security incident as part of the incident response actions; and

(e) All vulnerabilities identified in a software assurance assessment report must be incorporated into a POA&M for vulnerability acceptance and remediation tracking as part of the C&A process.

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

a. The FAA CIO must:

(1) Provide funding for enterprise tools and/or services for software assurance assessments;

(2) Maintain a list of approved software code services and/or tools as noted on URL https://intranet.faa.gov/faaemployees/org/staffoffices/aio/programs/itrd/it_standards_licenses/ ;

(3) Utilize approved software code services and/or tools that work in FAA's existing environment as noted on URL: https://intranet.faa.gov/faaemployees/org/staffoffices/aio/programs/iss/software_code_vulner_scan_serv/ ;

b. The FAA CISO must:

(1) Provide an annual report to the CIO, on the state of the FAA's process automation supporting software assurance assessment;

(2) Provide technical security training for software developers to ensure software assurance; and,

(3) Approve any Notice of Exception and Noncompliance to this policy.

c. The ISSMs must:

(1) Ensure that software within systems are identified and scheduled for periodic software assurance assessments; and,

(2) Ensure the separation of duties during the performance of software assurance assessments and remediation effort.

d. The ISSOs must:

(1) Ensure the system development environment meets minimum FISMA compliance criteria as expressed in NIST SP 800-53, NIST SP 800-115, CVSS, and CWE;

(2) Provide recommendations concerning software assurance assessments of code contained within the information systems to the ISSM, AO, CISO, and CIO;

(3) Maintain integrity by effective configuration management and regression testing of patches and changes;

(4) Assist the ISOs with software assurance assessment activities;

(5) Ensure the separation of duties during the performance of software assurance assessments and remediation efforts;

(6) Ensure that all components required to successfully complete software assurance security assessments are provided working in collaboration with the ISO.

(7) Ensure that the execution and analysis of software assurance assessments are properly documented and retained working in collaboration with the ISO; and

(8) Determine if modifications (e.g., upgrades, patches, hot fixes) to the information systems or environment that interacts with the software code may also warrant another software assurance security assessment to be conducted.

e. The ISOs must:

(1) Identify and assign the team responsible for providing the binary executables (compiled or byte code) including all libraries and components of the software code for the software assurance assessment process;

(2) Maintain integrity by effective configuration management and regression testing of patches and changes;

(3) Assist the ISSO with software assurance assessment activities;

(4) Ensure the execution of software assurance assessments during each phase of the software development lifecycle and periodically thereafter as identified in this Order and by the LOB/SO;

(5) Identify and inform the ISSO of any system changes that may affect the security of software code, so the appropriate decisions on the performance of software assurance can be made;

(6) Disseminate software assurance assessment reports to authorized personnel; and,

(7) Implement the remediation activities from the POA&M.

f. Software Developers must:

(1) Ensure compliance with Federal and industry security practices when developing software;

(2) Conduct preliminary testing of common vulnerabilities identified by NIST, CVSS, and CWE to reduce or eliminate issues earlier in the development cycle;

(3) Implement software code changes in compliance with software assurance assessment report recommendations;

(4) Ensure that software code operates as intended on the system in compliance with the industry standard benchmarks for security; and,

(5) Maintain knowledge of current and emerging secure software technologies, techniques, and standards in addition to formal technical training as appropriate;

g. **FAEs must**:

(1) Ensure appropriate verbiage is placed in FAA contracts statement of work to comply with this Order; and,

(2) Ensure this Order is accessible in the Acquisition Management System (AMS) FAA Acquisition System Toolset (FAST).

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. All FAA organizations are encouraged to go beyond the requirements of this Order to address business, operational, or security needs 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.

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

Appendix A. References

a. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

b. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

c. NIST SP 800-37, Guide for the Security Certification and Accreditation, May 2004.

d. NIST SP 800-40, Creating a Patch and Vulnerability Management Program, Version 2.0, November 2005.

e. NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

f. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008.

g. NIST SP 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008.

h. NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008.

i. NIST SP 800-95, Guide to Secure Web Services, August 2007.

j. NIST SP 800-115, Technical Guide to Information Security Testing, October 2008.

k. FAA Order 1200.22D, FAA National Airspace System (NAS) Data and Interface Equipment Used by Outside Interests, February 26, 2008.

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

m. FAA Order 1370.89, Information Operations Conditions, August 25, 2003.

n. FAA Order 1370.91, Information Systems Security Patch Management, May 19, 2004.

o. FAA Order 1370.106, Information Systems Security Awareness and Training Policy, June 16, 2009.

p. FAA ATO Order JO 1370.99, ATO NAS Information Systems Security Patch Management, February 6, 2002.

q. FAA Order 1800.66, Configuration Management Policy, September 19, 2007.

r. FAA Acquisition Management Policy, August 2009.

Appendix B. Definitions

Common Vulnerability Scoring System (CVSS). A vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organize, prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal, and environmental properties of vulnerability.

Common Weakness Enumeration (CWE). A list of software weaknesses as a result of collaboration between the SANS Institute, MITRE, and many other top software security experts in the United States (U.S.) and Europe.

Dynamic Code Analysis. This process identifies vulnerabilities at runtime and does not require source code. It identifies false negatives from static analysis and servers to validate static analysis findings.

National Vulnerability Database (NVD). The U.S. government repository of standard based vulnerability management data that enables automation of vulnerability management, security measures, and compliance.

Static Code Analysis. The process of reviewing software code, without the need of source code and without executing the actual program.

Software Assurance Metrics and Tool Evaluation (SAMATE). A project sponsored by the Department of Homeland Security and NIST to improve software assurance by developing methods to enable software tool evaluations, measuring the effectiveness tools and techniques, and identifying gaps in tools and methods.

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.