



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

NextGen Organization

ORDER

NG 1600.31

Effective Date:
06/15/2017

SUBJ: Laboratory Information Security Continuous Monitoring (ISCM) Program at the William J. Hughes Technical Center

1. Purpose of This Order. This Order defines policy for the implementation and operation of the Information Security Continuous Monitoring (ISCM) program for laboratories managed by the FAA William J. Hughes Technical Center (WJHTC).

2. Audience. This Order applies to all employees and contractors, who operate, maintain, support or use Information Systems (IS) within WJHTC laboratories.

3. Where to Find This Order.

a. You can find this Order on the MyFAA Employee website. Use "Tools & Resources" tab and select "[Orders & Notices](#)."

b. You can also find guidance for this Order at the MyFAA Employee website. Use the "Organizations" tab and select "[William J. Hughes Technical Center](#)". Under "Tools & Resources", select "WJHTC Laboratory Information Security Continuous Monitoring (ISCM) Guidance (PDF)". Alternately, you can contact Laboratory Services Division, ANG-E1, for a copy of the guidance document.

4. Background.

a. The Office of Management and Budget (OMB) Memorandum M-14-03, issued November 18, 2013, requires managing information security risk on a continuous basis by monitoring the security controls in Federal information systems and the environments in which those systems operate on an ongoing basis. OMB M-14-03 also identifies programs at the Department of Homeland Security (DHS) and the General Services Administration (GSA) that WJHTC can leverage to deploy a basic set of ISCM capabilities using a phased approach. The guidance document referred to in paragraph 3b of this order contains information regarding the DHS program and its phases.

b. OMB M-14-03 focuses on ISCM as part of the authorization to operate for federal information systems. This Order extends ISCM to information systems in FAA WJHTC laboratories that have not been granted an authorization to operate.

c. The WJHTC is committed to the protection of its laboratories and their connecting infrastructure and will comply with OMB requirements for ISCM in a way that integrates with

DOT and FAA information security policy. Applicable DOT and FAA policies are listed in *Paragraph 9-Applicable Laws, Guidance, and Programs* of this Order.

5. Scope. This Order applies to all Information Systems in WJHTC laboratories that are used for research, development, test, or second-level engineering support. This Order does not apply to systems used for NAS and non-NAS real-time operations and other WJHTC laboratory systems that have an Authorization to Operate. The scope of this Order comprises:

- a. Which laboratories are covered or included;
- b. Which technologies and mechanisms are covered or included;
- c. How this Order relates to other FAA Orders, DOT guides, and related programs at DHS and OMB.
- d. Responsibilities for developing and maintaining a phased implementation plan for the WJHTC Laboratory ISCM Program are specified in this Order.

A list of WJHTC laboratory systems that fall outside the scope of this order is maintained by the manager of the WJHTC Laboratory Services Division.

6. Policy.

a. The WJHTC shall define an ISCM strategy as the primary way to manage WJHTC laboratory information systems in support of risk management. The strategy will ensure laboratory asset risks are incrementally reduced with the implementation of each ISCM phase.

b. The WJHTC ISCM program shall be established to:

- (1) Maintain clear visibility into laboratory assets, awareness of vulnerabilities and up-to-date threat information;
- (2) Determine metrics, status monitoring frequencies and an ISCM technical architecture;
- (3) Collect the security-related asset information required for metrics, assessments, and reporting;
- (4) Analyze the data collected, report findings and determine the appropriate response which can be technical, management, and procedural mitigating activities or acceptance, transference/sharing, or avoidance/rejection;
- (5) Review and update the monitoring program, adjusting the ISCM strategy and capabilities to increase visibility into assets and awareness of vulnerabilities to further enable data-driven control of the security of the WJHTC information infrastructure.

c. Specific procedures and mechanisms for the implementation of ISCM are provided in “WJHTC Laboratory Information Security Continuous Monitoring (ISCM) Guidance”.

7. Roles and Responsibilities.

a. Director, William J. Hughes Technical Center.

(1) Plans, coordinates and allocates sufficient resources, funding, and personnel to the operation and maintenance of the WJHTC ISCM Program and oversees its management.

(2) Approves WJHTC ISCM Program policy and strategy recommended by the WJHTC Laboratory Manager.

(3) Reviews, forwards, and takes appropriate action on reports and recommended response to findings from the WJHTC Laboratory Manager.

b. WJHTC Laboratory Manager.

(1) Tailors the WJHTC ISCM Program strategy, defined by the NextGen Information Systems Security Manager (ISSM), to the WJHTC laboratory environment.

(2) Develops phased schedules, policies and practices in accordance with applicable OMB and FAA Orders to implement the WJHTC ISCM Program strategy.

(3) Develops the WJHTC ISCM architecture.

(4) Establishes security-focused configuration management of information systems affected by the WJHTC ISCM Program (e.g., configuration settings).

(5) Manages the WJHTC ISCM Program in order to facilitate:

(a) Provision of ISCM program tools for laboratory information systems to the extent that funding is available.

(b) Implementation of tools and processes associated with common services and monitoring (e.g., asset discovery, configuration management, asset management).

(6) Responds to requests from authorized officials.

(7) Supports the NextGen and associated LOB ISSMs in analyzing ISCM data and prepares findings in the context of:

(a) Potential impact of vulnerabilities on WJHTC processes.

(b) Potential impact/costs of mitigation options (vs. other response actions).

(8) Periodically provides reports and recommends responses to findings, as appropriate with prioritized remediation actions, to the WJHTC Director or NextGen and associated LOB ISSMs. Examples of responses include (but are not limited to): permit or deny permission to connect laboratory information system to WJHTC infrastructure, take remediation action, accept the risk, reject the risk, and transfer/share the risk.

(9) Supports the NextGen ISSM with the monitoring of the ISCM data.

(10) Maintains a “List of Excepted Systems” document consisting of the WJHTC laboratory systems that are not subject to this Order; reviews and updates the “List of Excepted Systems” document on an annual basis.

c. NextGen Information System Security Manager (ISSM).

(1) Ensures the security risk of systems under his or her purview are identified and prioritized, risk assessments are completed, and risk mitigation plans are developed and maintained.

(2) Defines the WJHTC ISCM Program strategy.

(3) Determines NextGen ISCM metrics and monitoring frequencies.

(4) Supports the WJHTC Laboratory Manager in the security-focused configuration management of information systems affected by the WJHTC ISCM Program.

(5) Supports the WJHTC Laboratory Manager in the management of the WJHTC ISCM Program.

(6) Performs the following functions:

(a) Provides ISCM program tools for laboratory information systems to the extent that funding is available.

(b) Implements and operates ISCM tools and processes associated with common services and monitoring (e.g., asset discovery, configuration management, asset management).

(c) Monitors and analyzes ISCM data, using automation to the extent possible, and prepares findings and periodically provides reports to the WJHTC Laboratory Manager and FAA Chief Information Security Officer.

(d) Provides training on the NextGen ISCM program and process and provides support to the information system owners on how to implement ISCM for their information systems.

d. Line of Business (LOB) Information System Security Manager (ISSM).

(1) Ensures the security risk of systems under his or her purview are identified and prioritized, risk assessments are completed, and risk mitigation plans are developed and maintained.

(2) Determines LOB ISCM metrics and monitoring frequencies for WJHTC laboratory systems under his or her purview.

(3) Supports implementation of ISCM tools for information systems affected by the WJHTC ISCM Program.

(4) Supports the WJHTC Laboratory Manager in the security-focused configuration management of information systems affected by the WJHTC ISCM Program.

e. Laboratory Administrator and Information System Owners (ISOs).

(1) Assist WJHTC Laboratory Manager to implement the ISCM program, define strategy, policies, use, and technical architecture.

(2) Develop procedures/templates to support ISCM strategy and provide additional support as needed.

(3) Support WJHTC Laboratory Manager in analyzing system data, using automation to the extent possible.

(4) Support implementation of ISCM tools locally.

f. Laboratory Information Systems Security Officers (ISSOs).

(1) Establish information system-level procedures.

(2) Implement system-specific tools and processes associated with the implementation of ISCM.

(3) Support Laboratory Administrator and ISO in analyzing system data using automation to the extent possible.

8. Applicable Laws, Guidance, and Programs. The following public laws and federal guidance are applicable to this policy:

a. Federal Information Security Management (FISMA) Act of 2002, Public Law 107-347, December 17, 2002; <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

b. OMB Circular A-130, Management of Federal Information Resources, November 28, 2000; https://www.whitehouse.gov/omb/circulars_a130_a130trans4/

c. OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, August 23, 2004; <http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-25.pdf>

d. OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006; <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf>

e. OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, November 18, 2013; <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf>

f. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004;

<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

g. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006; <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

h. National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013; <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

i. NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal information Systems and Organizations, September 2011; <http://dx.doi.org/10.6028/NIST.SP.800-137>

j. DHS Continuous Diagnostics and Mitigation (ISCM) program, <http://www.dhs.gov/cdm> and <http://www.dhs.gov/cdm-implementation>;

k. US-CERT Continuous Diagnostics and Mitigation (ISCM) program, <https://www.us-cert.gov/cdm>;

l. GSA Continuous Diagnostics and Mitigation (ISCM) program Blanket Purchase Agreement (BPA), <http://www.gsa.gov/cdm>;

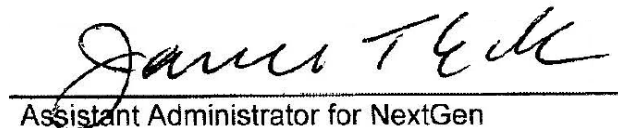
m. DOT Cybersecurity Compendium, Supplement to DOT Order 1351.37, June 2015;

n. DOT Security Authorization & Continuous Monitoring Performance Guide, January 2013.

o. FAA Order 1370.121, FAA Information Security and Privacy Program & Policy, December 2016.

9. Exceptions. Based on the recommendations of the WJHTC Laboratory Manager, the WJHTC Director may grant exceptions to this Order. Excepted systems are documented in the “List of Excepted Systems” maintained by the WJHTC Laboratory Manager.

10. Distribution. This Order is available electronically as described in paragraph 3.



Assistant Administrator for NextGen