State of Maine
Department of Administrative and Financial Services
Office of Information Technology (OIT)

Vulnerability Scanning Procedure (RA-5)

Table of Contents

1.0. Purpose

The purpose of this document is to define the Office of Information Technology's (OIT's) procedures for assessing cybersecurity vulnerabilities through proactive scanning of information assets (see Definitions) and addressing vulnerabilities in a timely fashion. It falls under the umbrella Risk Assessment Policy. More specifically, this document corresponds to the Control RA-5, Vulnerability Scanning, including Control Enhancement (CE) numbers 1 through 3, and 5, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. This document applies to:

2.1.1. All State of Maine personnel, both employees and contractors;

2.1.2. Executive Branch Agency information assets, irrespective of location; and

2.1.2. Information assets from other State government branches that use the State network.

3.0. Conflict

If this document conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Procedures

4.1. For OIT-hosted information assets, OIT Information Security executes the vulnerability (see Definitions) scans.

4.2. For externally hosted information assets (see Definitions), OIT Information Security either executes the vulnerability scans or collects vulnerability scans from vendors or other third-party auditors.

4.3. OIT Information Security distributes the scan results, on a need-to-know basis, to the downstream partners and works with them to filter out the false-positives and false-negatives, thereby identifying the legitimate vulnerabilities (see Definitions). The downstream partners and information asset owners include:

4.3.1. OIT Client Technologies;

4.3.2. OIT Network Services;

4.3.3. OIT Computing Infrastructure and Services;

4.3.4. OIT Data Services; and

4.3.5. OIT Application Divisions.

4.4. The downstream partners listed above remediate all legitimate vulnerabilities within their span of control (see Definitions), within the prescribed remediation schedule. They also collaborate with OIT Information Security in exploring compensating controls (see Definitions) should outright remediation turn out to be elusive.

4.5. OIT Information Security also liaises with horizontal industry partners (see Definitions), on a need-to-know basis, to help contain similar vulnerabilities in the

wild. These include the Multi-State Information Sharing & Analysis Center (MS-ISAC)[1] and the Maine Information and Analysis Center (MIAC),[2] (which interfaces with State, local, and Federal law-enforcement partners).

4.6. DAFS IT Procurement, in collaboration with agency business partners and OIT information asset owners, holds all vendors and partners for externally hosted information assets accountable to this procedure, within the vendor's or partner's span of control.

4.7. OIT Account Managers owns the agency business customer interface related to this Procedure.

4.8. By default, vulnerability scanners (see Definitions) classify vulnerabilities into three risk tiers: low, medium, and high. Even if a vulnerability scanner uses a different taxonomy in its output, OIT Information Security will translate that output into the standard low-medium-high tier structure, according to the following meanings:
- 4.8.1. Low: No direct compromise of cybersecurity.
- 4.8.2. Medium: Measurable, but limited, compromise of cybersecurity.
- 4.8.3. High: Severe compromise of cybersecurity.

4.9. The default OIT vulnerability remediation schedule is as follows:
- 4.9.1. For *new* information assets:
  - 4.9.1.1. High-risk vulnerabilities must be remediated *prior to production deployment.*
  - 4.9.1.2. Medium-risk vulnerabilities must be remediated *prior to production deployment.*
  - 4.9.1.3. Low-risk vulnerabilities must be remediated in alignment with the natural product lifecycle (version and release upgrades, patch lifecycle, and so on).
- 4.9.2. For *established* information assets:
  - 4.9.2.1. High-risk vulnerabilities must be remediated within 30 calendar days of identification of the vulnerabilities.
  - 4.9.2.2. Medium-risk vulnerabilities must be remediated within 90 calendar days of identification of the vulnerabilities.
  - 4.9.2.3. Low-risk vulnerabilities must be remediated in alignment with the natural product lifecycle (version and release upgrades, patch lifecycle, and so on).

4.10. Irrespective of the default risk classification and the default remediation schedule, specified above, for any specific vulnerability, the Chief Information Security Officer (CISO) may impose a different classification, or a different a remediation schedule, or both.

[1] https://www.cisecurity.org/ms-isac/
[2] https://memiac.org/

4.11. Typically, vulnerabilities are remediated by applying vendor-supplied patches, or updating custom code. However, under certain circumstances, compensating controls may be used as an alternative until the next maintenance/patching schedule. The CISO remains the final arbiter of whether a compensating control does qualify as remediation, and the timeframe thereof.

4.12. The vulnerability scanners are updated in real time as released by the vendor. **(RA-5(1), RA-5(2))**

4.13. The vulnerability scanners utilized by OIT are industry-leading products, and, at a minimum, they are configured for **(RA-5(3), RA-5(4))**:

4.13.1. The CIS Benchmarks for Configurations[3];

4.13.2. Missing original vendor patches;

4.13.3. Missing third-party, commodity application (such as from Adobe, Oracle-Java, and others) patches;

4.13.4. Misconfigurations in third-party commodity applications (such as from Adobe, Oracle-Java, and others), as recommended by the product vendors or industry partners;

4.13.5. Functions, services, ports, and protocols that should be disabled or restricted, as recommended by the product vendors or industry partners;

4.13.6. Higher sensitivity toward information assets that are discoverable from the internet;

4.13.7. Higher sensitivity toward the potential for privilege escalation;

4.13.8. Higher sensitivity toward the potential for information leakage;

4.13.9. Industry-standard output, in terms of the Common Vulnerabilities and Exposures (CVE),[4] the Open Vulnerability and Assessment Language (OVAL),[5] the Common Weakness Enumeration (CWE),[6] the National Vulnerability Database (NVD),[7] the Common Vulnerability Scoring System (CVSS),[8] and others;

[3] https://www.cisecurity.org/cis-benchmarks/
[4] https://cve.mitre.org/
[5] https://oval.mitre.org/
[6] https://cwe.mitre.org/
[7] https://nvd.nist.gov/
[8] https://www.first.org/cvss/

4.13.10. For web-based applications, vulnerability standards include the Open Web Application Security Project (OWASP),[9] SAFECode,[10] Building Security in Maturity Model (BSIMM),[11] the Cloud Security Alliance,[12] and so on.

4.14. At a minimum, the vulnerability scans are authenticated (white-box) scans using administrative/privileged access. **(RA-5(5))**

4.15. Scanning Frequency:

4.15.1. OIT-hosted infrastructure is scanned at Infrastructure Deployment Certification,[13] when new vulnerabilities potentially affecting such information assets are reported by industry partners, and whenever a major upgrade to such an information asset is performed. Additionally:

4.15.1.1. Servers (including server-based backup components) and databases are scanned at least once per month.

4.15.1.2. Perimeter firewalls are scanned routinely by the U.S. Department of Homeland Security, which also provides weekly reports of these scans.

4.15.1.3. Endpoint workstations undergo local vulnerability scans once every six hours.

4.15.1.3.1. Ad Hoc reviews of Microsoft Defender reports are compared to vulnerability scans for comparison purposes.

4.15.1.4. Endpoint mobile devices are managed via a mobile endpoint security application.

4.15.2. OIT-hosted applications are scanned at Application Deployment Certification[14] and as requested.

4.15.3. Externally hosted information assets are scanned at the relevant Deployment Certification (infrastructure or application) and once every calendar year subsequently. They are also scanned at every major upgrade, and when new vulnerabilities potentially affecting such information assets are reported by industry partners. Depending on the contractual terms, OIT Information Security may do the scanning, a scan may be provided by the vendor, or a third-party auditor may provide the scan.

4.16. Any vulnerability remediation (including instituting compensating controls) on any information asset involves testing, and it potentially impacts agency business partners. OIT must coordinate all agency business partners' liaison through the

[9] https://www.owasp.org/
[10] https://safecode.org/
[11] https://www.bsimm.com/
[12] https://cloudsecurityalliance.org/
[13] https://www.maine.gov/oit/policies/Infrastructure-Deployment-Certification.pdf
[14] https://www.maine.gov/oit/policies/Application-Deployment-Certification.pdf

Account Managers. Agencies cooperate with OIT on User Acceptance Testing for the remediation of legitimate vulnerabilities.

4.17. Any necessary configuration change must be managed as outlined in the Change Management Policy.[15]

4.18. OIT employs an industry-leading security information and event management (SIEM) system, to: **(RA-5(6), RA-5(8), RA-5(10))**

4.18.1. Compare the results of vulnerability scans over time to determine trends in information system vulnerabilities;

4.18.2. Review historic audit logs to determine whether a vulnerability identified in the information system has been previously exploited; and

4.18.3. Correlate the output from vulnerability scanning tools to determine whether multi-vulnerability or multi-hop attack vectors are present.

4.19. Should there occur a high-risk legitimate vulnerability in an information asset that is not amenable to timely remediation or a compensating control, the CISO may instruct the cessation-of-operation of information asset until the risk is mitigated to the satisfaction of the CISO.

5.0. Document Details

5.1. Initial Issue Date: March 6, 2020
5.2. Latest Revision Date: June 30, 2021
5.3. Point of Contact: Enterprise.Architect@Maine.Gov
5.4. Approved By: Chief Information Officer, OIT
5.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[16]
5.6. Waiver Process: Waiver Policy[17]
5.7. Distribution: Internet[18]

6.0. Review

This document is reviewed annually and when substantive changes are made to policies, procedures, or other authoritative regulations affecting this document.

7.0. Records Management

OIT security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures* and *Internal Control Policies and Directives* records management categories. They will be retained for 3 years and then destroyed, in accordance with guidance provided by Maine State Archives. Retention of these

[15] https://www.maine.gov/oit/policies/ChangeManagementPolicy.pdf
[16] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[17] https://www.maine.gov/oit/policies/waiver.pdf
[18] https://www.maine.gov/oit/policies-standards

documents will be subject to future State Archives General Schedule revisions that cover these categories.

8.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA), certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as to security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the Maine State Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the State.

9.0. Definitions

9.1. Compensating control: An alternative mechanism instituted to mitigate a legitimate vulnerability when the mechanism to properly remediate the vulnerability is deemed impractical in the present time. If utilized, compensating controls must provide the same, or greater, level of defense as would be attained through the proper remediation. Compensating controls may be used until full remediation can be undertaken.

9.2. Externally hosted information asset: An information technology product consumed from the public cloud, includes the full spectrum of Software as a Service, Platform as a Service, and Infrastructure as a Service.

9.3. Industry partner: An external party that apprises the information security division of the cybersecurity vulnerability landscape. These can be open-channel partners, such as product vendors, trade magazines, security research organizations, and so on; or they can be closed-channel partners, such as the MS-ISAC, or the MIAC.

9.4. Information assets: The full spectrum of all information technology products, including business applications, system software, development tools, utilities, appliances, and so forth.

9.5. Legitimate vulnerability: Neither a false positive nor a false negative, but a true weakness that has been verified by a human analyst in addition to being flagged by an automated scan.

9.6. Span of control: The area of activity and number of functions, people, or things for which an individual or organization is responsible.

9.7. Vulnerability: Weakness in an information asset that could be exploited by a threat source.

9.8. Vulnerability scanner: A specialized application custom-built to detect, and report out, vulnerabilities. Examples include Tenable Nessus, HCL/IBM AppScan, etc.

9.0 Abbreviations

9.1 BSIMM: Building Security in Maturity Model
9.2 CISO: Chief Information Security Officer
9.3 CVE: Common Vulnerabilities and Exposures
9.4 CVSS: Common Vulnerability Scoring System
9.5 CWE: Common Weakness Enumeration
9.6 CE: Control Enhancement
9.7 FOAA: (Maine) Freedom of Access Act
9.8 MIAC: Maine Information and Analysis Center
9.9 MS-ISAC: Multi-State Information Sharing & Analysis Center
9.10 NIST: National Institute of Standards and Technology
9.11 NVD: National Vulnerability Database
9.12 OIT: Office of Information Technology
9.13 OVAL: Open Vulnerability and Assessment Language
9.14 OWASP: Open Web Application Security Project