Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Risk Management Office

Vulnerability Management Standard

Document Name: Vulnerability Management	Effective Date: October 15th, 2018
Document ID: IS.016	Last Revised Date: November 22, 2023

Table of contents

1. PURPOSE

1.1. *Vulnerability Management Standard* — The purpose of this *standard* is to document the requirements to protect, detect and recover from *vulnerabilities* in the technology environment.

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of *information*, *information systems*, electronic and computing devices, *applications*, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), such as mass.gov, must agree to comply with this document as a condition of use. Commonwealth Agencies and Offices are required to implement *procedures* that ensure their *personnel* comply with the requirements herein to safeguard *information*.

4. RESPONSIBILITY

4.1 The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this *standard*.

4.2 The Enterprise Risk Management Office is responsible for monitoring compliance with this *standard* and may enlist other offices to assist in monitoring and maintaining compliance with this *standard*.

4.3 Any inquiries or comments regarding this *standard* must be submitted to the Enterprise Risk Management Office by sending an email to ERM@mass.gov.

4.4 Additional *information* regarding this *standard* may be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch including all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested online through ServiceNow, https://www.mass.gov.service-now.com A *policy exception* may be granted only if the benefits of

the *exception* outweigh the increased *risks*, as determined by the **Commonwealth CISO** or his or her designee. Any and all *exceptions* will be for a limited time and will be narrow in scope.

6. STANDARD STATEMENTS

6.1.　Vulnerability Management

Processes to identify, classify and remediate *vulnerabilities* across all technology environments and platforms to reduce the Commonwealth's exposure to cyber threats must be documented. Commonwealth Agencies and Offices will do the following:

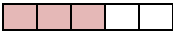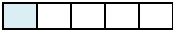6.1.1.　Establish a *vulnerability* and patch management process to:

6.1.1.1.　Ensure *information* systems are patched in a timely manner.

6.1.1.2.　Ensure that the *patch management process* and cadence is consistent with the recommendation of patch providers.

6.1.1.3.　Reduce the number of service disruptions, *incidents* and problems caused by *vulnerabilities.*

6.1.1.4.　Provide a defined, repeatable method for ensuring consistent execution of associated patch management activities and tasks.

6.1.1.5.　Provide clarity around *stakeholder*/participant roles and responsibilities.

6.1.1.6.　Enable key performance metrics to be captured for performance monitoring and improvement.

6.1.1.7.　Define roles and responsibilities associated with *vulnerability* management.

6.1.2.　Identify *vulnerabilities* within the IT environments:

6.1.2.1.　In support and consistent with *IS.004 Asset Management Standard* , perform *asset* discovery scans on the internal network, update *asset* inventories as necessary.

6.1.2.2.　Monitor security-related email alerts and/or vendor notification sites for *vulnerabilities* that may affect systems or *applications*.

6.1.2.3.　As appropriate, generate internal security alerts.

6.1.2.4.　Ensure alerts are distributed to the Commonwealth SOC and ensure that associated directives are implemented within established timeframes, or the issuing organization is notified of noncompliance.

6.1.2.5.　Perform credentialed *vulnerability* scans. Where technically feasible, include *endpoints* (i.e., desktops and laptops).

6.1.2.6.　Conduct automated *vulnerability* scans, at a minimum monthly, on internal and external networks.

6.1.2.6.1. For PCI-specific environments, perform *vulnerability* scans on externally facing IP addresses; use an Approved Scanning Vendor (ASV) and track findings through remediation.

6.1.2.6.2. Perform ad hoc *vulnerability* assessments after any significant change to the PCI environment (e.g., new system component installations, changes in network topology, firewall rule modification, major version upgrade).

6.1.2.7. Perform *vulnerability* scanning before any significant infrastructure or *application* upgrade or modification (e.g., new system component installations, changes in network topology, firewall rule modifications) is implemented into production.

6.1.2.8. Perform manual *vulnerability* assessments on a periodic basis to identify difficult to detect *vulnerabilities*.

6.1.2.9. Test for the presence of unauthorized wireless access points on Commonwealth networks on a quarterly basis.

6.1.2.10. Review public-facing web *applications* via manual or automated *application vulnerability* security assessment tools or methods at least quarterly.

6.1.2.10.1. For PCI specific environments, perform reviews on public-facing web *applications* after any change to the PCI environment, or install a web *application* firewall in front of a public-facing web *application* as a mitigating *control*.

6.1.2.11. Conduct internal and *third-party* network-layer and *application*-layer penetration testing at least annually or collect evidence to attest that the *third-party* has had a *vulnerability* assessment performed.

6.1.3. Perform timely reviews of *vulnerability information* received from internal and external sources (e.g., *software* suppliers) and report to the Enterprise Security Office. The report will include:

6.1.3.1. *Vulnerability* description

6.1.3.2. Hosts affected

6.1.3.3. Current status at the time of reporting

6.1.3.4. Recommendations for remediation

6.1.3.5. Supporting *information*

6.1.4. *Vulnerabilities* will be prioritized using a *risk*-based approach

Severity	Level	Description	Remediation timeframe
	Critical	Threat actor may gain control of the host, or there may be potential leakage of *restricted* or *confidential information*.	30 calendar days

	High	Threat actor may gain access to **sensitive data** or other **information** stored on the host, including security settings resulting in potential misuse.	60 calendar days
	Medium	Threat actor may be able to collect **sensitive data** or other **information** from the host, such as the precise version of **software** installed.	90 calendar days
	Low	Limited **risk** to host.	Best effort

6.1.5. Perform necessary actions to ensure that the likelihood and impact of threats, which can potentially exploit **vulnerabilities**, are minimized by implementing security **controls** within the established timeframes (section 6.1.4).

6.1.5.1. Remediate **vulnerabilities** by deploying patches or making configuration changes as a mitigation strategy. Appropriate testing must be conducted prior to patch deployment. Configuration changes to **information systems** must follow the *Change Management* process and obtain the required approvals. (*See Change Management in IS.004 Asset Management Standard)*

6.1.5.2. In the event that a patch or mitigation strategy is not available to remediate the **vulnerability**, a mitigating **control** will be enacted or a security **exception** from the **Commonwealth CISO** or his or her designee is required.

6.1.6. Report through the various stages of the **vulnerability** and **patch management process** using established performance metrics. Summary reports will be used to inform management of the current status and effectiveness of the **vulnerability** and patch management program.

6.1.6.1. The agencies must report **vulnerabilities** on a monthly basis to the Enterprise Security Office:

6.1.6.1.1. **Vulnerabilities** by severity and aging

6.1.6.1.2. **Vulnerabilities** with **exceptions** in place

6.1.6.1.3. Open and closed **vulnerabilities**

7. CONTROL MAPPING

Section	NIST SP800-53 Rev 5	CIS 18	NIST CSF
6.1 Vulnerability Management	RA-3	-	ID.RA-1
	RA-5	CSC 7	ID.RA-1
	SI-2	CSC 7	ID.RA-1
	SI-5	CSC 7	ID.RA-1
	CA-8	CSC 16	ID.RA-1
	SA-8	-	PR.IP-2
	SC-7	CSC 4	PR.AC-5
	SC-38	-	-
	SI-3	CSC 10	DE.CM-4
	SI-7	CSC 10	PR.DS-6

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/02/2018	Corrections
0.95	Sean Vinck	5/7/2018	Corrections and formatting.
0.97	Andrew Rudder	5/31/2018	Corrections and formatting.
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-publication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	NIST 800-53 R5 mapping and Annual Review
1.4	Thomas E. McDermott	11/22/2023	Corrections, formatting, updating and Annual Review
1.5	Anthony O'Neill	11/22/2023	Final Review

4.5 The owner of this document is the **Commonwealth CISO** (or his or her designee). It is the responsibility of the **document owner** to maintain, update and communicate the content of this document. Questions regarding this document must be submitted to the **document owner** by sending an email to ERM@mass.gov.

9.1 Annual Review

This document, the *Vulnerability Management Standard,* should be reviewed and updated by the **document owner** on an annual basis or when significant **policy** or **procedure** changes necessitate an **amendment**.