OKLAHOMA
Office of Management
& Enterprise Services

Vulnerability Management Standard

Introduction

OMES is committed to ensuring the security of State of Oklahoma systems and protecting sensitive information from unauthorized disclosure. This standard provides vulnerability management practices for vulnerability scanning, patch management and reporting an observed vulnerability or cyber security weakness threatening State of Oklahoma security systems.

Purpose

This document establishes the vulnerability and patch management standard for the State of Oklahoma. By applying security-related software or firmware updates (patches) to applicable IT systems, the expected result is reduced time and money spent dealing with exploits by reducing or eliminating the related vulnerability. This standard also provides guidelines for reporting security vulnerabilities to the OMES Cyber Command within 24 hours of discovery.

Definitions

State systems and assets include, but are not limited to:

- CVE – Common vulnerabilities and exposures; a list of publicly disclosed computer security flaws.
- Hosted servers or SaaS solutions must provide a vulnerability management solution at least as comprehensive as described in this document and a reporting mechanism back to Oklahoma Cyber Command no less than monthly.
- Servers, such as database servers, web servers, virtual servers, etc., internal to the state network. This excludes hosted servers or services that lie outside of the internal network.
- Workstations, such as laptops, desktops, tablets, etc., that are managed by OMES.

Standard

Vulnerability scans will be conducted monthly on all agency-connected devices and servers for software application and hardware vulnerabilities:

- Vulnerabilities for software or applications, such as CVE's, exploits or other vulnerabilities.
- Vulnerabilities for hardware, such as drivers, components, etc.
- All currently open ports on the system.
- Missing patches pertaining to software installed on the system being scanned.
- Missing patches for the current OS running on the system being scanned.
- Vulnerability definitions are continuously updated by defensive security tools and automatically distributed to the platform via cloud-based administration.

Vulnerability scan reports are produced automatically from the monthly scans and made available to agency auditing or compliance staff, OMES IS tower leadership (i.e., server team) and select Cyber Command Defense engineers and technicians, as requested. Reports can be downloaded for viewing in several formats. Vendor access to reports must be reviewed and approved on a case-by-case basis.

Reports from past vulnerability scans are archived and available on demand. Available features, upon request include:

- Dashboards to track scan history.
- Scanning for remediation, either on demand or during subsequent scans.

Patch management must be addressed as follows:

- All nonconsolidated agencies must assign a business owner responsible for patch management. OMES is responsible for patch management for all consolidated agencies.
- If patch management is outsourced, service level agreements must be in place addressing the requirements of this standard and outlining responsibilities for patching. If patching is the responsibility of the third party, agencies must verify the patches have been applied.
- Patching must include all application software. This includes enterprise applications, custom applications, commercial off-the-shelf applications, legacy applications and all related software such as operating systems, virtualization, database, etc.
- A process must be in place to manage patches. This process must include:
  - Monitoring security sources for vulnerabilities, patch and non-patch remediation and emerging threats. Examples of security sources are vendor website or notification lists, vulnerability scanners, penetration tests and the National Vulnerability Database.
  - Overseeing patch distribution, including verifying a change control procedure is followed.
  - Testing for stability and deploying patches.
  - Using an automated centralized patch management distribution tool whenever technically feasible. The tool should maintain a database of patches, deploy patches to endpoints and verify the installation of patches.
- Appropriate separation of duties must exist so that the individual(s) verifying patch distribution is not the same individual(s) distributing the patches.
- As per the Information Security Policy, Procedures and Guidelines policy, all agencies must maintain an inventory of hardware and software assets. Patch management must incorporate all installed IT assets.
- Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System and CISA directives. A CVSS score of 7-10 is considered a high-impact vulnerability, while 4-6.9 is considered a moderate-impact vulnerability and 0-3.9 is considered a low-impact vulnerability. A CISA directive is considered a critical-impact vulnerability.
- The patching process must follow the timeline shown here:

Impact/Severity	**Patch Initiated**	**Patch Completed**
Critical	Within **24 hours** of patch release.	Within **1 week** of patch release.
High	Within **24-72 hours** of patch detected in vulnerability management software.	Within **2 weeks** of patch detection.
Medium	Within **1 week** of patch release detected in vulnerability management software.	Within **1 month** of patch detection.

Low	Within **1 month** of patch release detected in vulnerability management software.	Within **365 days** during normal maintenance cycles unless ISO determines this an insignificant risk to environment.

- If patching cannot be completed in the specified timeframe, an extension must be requested from the chief information officer and the chief information security officer. The extension request must include:
  - Detailed explanation of why the patching cannot be completed in the timeframe listed.
  - List of compensating controls put in place.
  - Remediation plan for getting the system(s) compliant with specified timeframe(s). Note: Any system that is noncompliant for more than two periods annually is subject to decommissioning.
- If a patch requires a reboot for installation, the reboot must occur within the specified timeframe.

Vulnerability reporting.
The State of Oklahoma requires vulnerability reporters to notify Oklahoma Cyber Command within 24 hours of discovery of a real or potential security vulnerability, unless specified otherwise contractually.

Vulnerability reports are submitted by emailing cybercommand@omes.ok.gov and should:

- Make every effort to avoid privacy violations, degradation for user experience, disruption to production systems and destruction or manipulation of data.
- Include the location where the vulnerability was discovered and the potential impact of exploitation.
- Include a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).

Submitting an illegitimate vulnerability report exhibits the following characteristics that may be subject to criminal prosecution under the Oklahoma Computer Crimes Act.

- Uses an exploit to compromise or exfiltrate data, establish command line access and/or persistence or use the exploit to pivot to other systems.
- Performs network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Participates in physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- National Institute of Standards and Technology Special Publications: NIST 800-40.
- Common Vulnerability Scoring System.
- State of Oklahoma Security Policy, Procedures, Guidelines.
- CISA Coordinated Vulnerability Disclosure (CVD) Process.
- Oklahoma Computer Crimes Act.
- Internal – IS 2.06.01 Change Management Process.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/30/2025	**Review cycle:** Annual
Last revised: 06/30/2025	**Last reviewed:** 06/30/2025
Approved by: Dan Cronin, Chief Information Officer	