State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.03.02	Vulnerability Management	A	9/01/2021	1 of 3

1.0 PURPOSE

This standard establishes the minimum requirements for vulnerability management on technology assets, including both Operating System (OS) and non-OS software, as required to implement the CIS Controls v7.1.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100
Software Inventory and Control, S.6.02.01
Software Patch Management, S.6.03.01

6.0 STANDARD

6.1 Run automated vulnerability scanning tool

A. Agencies must adopt and implement a Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool in their environment. Agencies should use the state's enterprise vulnerability management tool, as it meets SCAP requirements and supports compliance with other CIS Controls requirements.

B. Agencies must have a documented procedure in place for automatically scanning all devices on their network, both managed and unmanaged, on at least a weekly basis.

C. Vulnerability scans must document a list of all identified potential vulnerabilities on the agency's systems.

6.2 Perform authenticated vulnerability scanning

A. Agencies must implement local scanning agents on each of their devices or configure remote scanners to perform authenticated vulnerability scans of every system on their network. All scans must be performed with the required credentials and elevated privileges to perform authenticated scans.

6.3 Protect dedicated assessment accounts

A. Agencies must designate at least one service account as an authorized vulnerability scanning account and provide the account(s) with elevated privileges required on every system they scan.

B. Agencies must not use authorized vulnerability scanning accounts for any purpose other than official vulnerability scans.

6.4 Compare back-to-back vulnerability scans

A. The SCAP compliant vulnerability scanning tool agencies utilize must allow for comparing consecutive months' vulnerability scan results to show timely remediation of identified vulnerabilities.

B. Agencies should maintain vulnerability scan results for at least three months to facilitate this comparison.

6.5 Utilize a risk-rating process

A. Agencies must adopt a standard, industry-recognized risk-rating methodology, such as the Common Vulnerability Scoring System (CVSS) or similar system, and use it to assign a criticality to each identified vulnerability.

B. Agencies must prioritize the remediation of identified vulnerabilities based on the criticality assigned by their risk-rating methodology.

C. Agencies must have a documented process in place detailing their selected risk-rating and prioritization methodologies for vulnerability management.

7.0 DEFINITIONS

Patch or **Update**: An improvement to software, including security patches, software updates to firmware, cumulative software patches, and other software features.

Technology Assets: As defined in CIS Controls v7.1, the term "Technology Assets" (also referred to therein as "Hardware Technology Assets" or "Hardware Assets") collectively refers to equipment and devices that have the potential to store or process information, whether connected to the network or not.

8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls Guide v7.1

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

State of Nevada

Information Security Committee

Standard

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	8/26/2021
State Chief Information Security Officer (CISO)	Signature on File	8/30/2021
State Chief Information Officer (CIO)	Signature on File	9/01/2021

Document History

Revision	Effective Date	Change
A	9/01/2021	Initial release for alignment with CIS Controls v7.1, Control 3 Continuous Vulnerability Management