Standard DE.CM: OCIO Vulnerability Management

July 9, 2021

U.S. Department of Education

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.07.09 18:09:56 -04'00'

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
0.1	12/11/2020	Initial Draft
1.0	1/27/2021	Final Version
1.1	4/29/2021	Updated Version

Table of Contents

1 Contents

1 INTRODUCTION

According to the National Institute of Standards and Technology (NIST), Vulnerability Management (VM) is the process in which information technology (IT) weaknesses are identified and the risks associated with these vulnerabilities are evaluated. Vulnerability scanning identifies security weaknesses within systems and allows the Department to prioritize their resources to the most critical areas. Timely remediation of vulnerabilities is critical to maintaining the availability, confidentiality, and integrity of IT systems.

The Vulnerability Management Support procedures apply to Department of Education (the Department) owned information systems and is conducted in accordance with NIST 800-53, vulnerability monitoring and scanning and the Department Baseline Standard, OCIO-STND-01. Vulnerability management includes the following key activities:

- Monitoring and scanning for vulnerabilities regularly and when new vulnerabilities are identified and reported.
- Utilizing vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.
- Analyzing vulnerability scan reports results.
- Supporting the Information System Owner (ISO)/ Information System Security Officer (ISSO) with tracking and remediating legitimate vulnerabilities. Facilitate the tracking and remediation of legitimate vulnerabilities in accordance with Department risk tolerance as defined in Standard ID.RM: Cybersecurity Risk Management Framework (CRMF).
- Sharing information obtained from the vulnerability scanning processing analysis to help eliminate similar vulnerabilities in other Department systems (i.e., system weaknesses or overall deficiencies).

1.1 PURPOSE

This document establishes the Department standard for OCIO Vulnerability Management support. This document describes how the Department will address relevant vulnerability management security control requirements. Subsequent detailed configuration and implementation requirements must be contained within operational procedure and guideline documentation.

This standard defines how the OCIO VM Team will facilitate the management of vulnerabilities that have the potential to disrupt the Department's mission and processes consequently compromising the confidentiality, integrity, and availability (CIA) of the Department's data and overall reputation. This standard also defines the Department's strategy and approach to routine vulnerability management.

2 SCOPE

This standard focuses on technical vulnerabilities. Non-technical vulnerabilities are addressed via the Assessment and Authorization (A&A) activities performed by the A&A Support Team. This standard covers all servers and infrastructure components that provide or support the Department IT services hosted inside the Department's network.

2.1 Related Processes

Related processes include:

- Change Management
- Patch Management
- Incident Response Management
- Assessment and Authorization
- Plan of Action and Milestones (POA&M)

3 OBJECTIVE

The objective of this standard is to ensure there is a consistent, repeatable, and auditable approach for conducting OCIO vulnerability management services within Department environments regardless of the source of the threat or the platform in which vulnerability is identified or detected.

4 ROLES AND RESPONSBILITIES

Role	Responsibilities
VM Program Manager (PM):	Responsible for coordinating the overall vulnerability management program.
Vulnerability Management Analyst:	Responsible for the monitoring, investigating, and analyzing detected vulnerabilities; and providing risk mitigation strategies in collaboration with Information System Owners (ISOs).
IT System Engineer:	Responsible for implementing remediation actions as a result of detected vulnerabilities for the Department networks and assets.
OCIO VM Team:	Supports various stakeholders including, but not limited to the CISO, IV&V Team, and ISOs/ISSOs to implement the VM procedures set forth in this document. In addition, VM Team processes requests for scans; generates, reviews, and analyzes vulnerability scan reports and uploads scan results to the Vulnerability Scan SharePoint site. • Operates and maintains the VM process • Conducts vulnerability scans • Reviews scans to reduce false positives • Analyzes scan content • Delivers scans and analysis to appropriate stakeholders
Chief Information Security Officer (CISO):	Reviews, approves, and implements the VM procedures set forth in this document such as identifying overall risk exposure to the Department.
Information System Owner (ISO):	Responsible for the IT assets that are scanned during the vulnerability management process. This role decides whether identified vulnerabilities are mitigated or accepted.
Information System Security Officer (ISSO):	Supports various stakeholders including, but not limited to the CISO, IV&V Team, ISOs, and OCIO VM Team to update and implement the standards set forth in this document.
Independent	Supports with various stakeholders including, but not limited to the CISO, ISSOs, ISOs,

Verification and Validation (IV & V) Team:	and OCIO VM Team to implement the procedures set forth in this document such as creating and managing POA&Ms in the Cyber Security Assessment and Management (CSAM) tool.
Software Development and IT Operations (DevOps) Engineer:	Responsible for implementing remediations for detected vulnerabilities for hosted production environments.

5 VULNERABILITY MANAGEMENT STANDARD

Vulnerability scanning identifies security weaknesses within systems and allows the Department to prioritize their resources to the most critical areas. Timely remediation of vulnerabilities is critical to maintaining the availability, confidentiality, and integrity of information technology (IT) systems.

5.1 DISCOVERY

During the discovery phase of the Vulnerability Management (VM) cycle, the OCIO VM Team will conduct scheduled scans, ad-hoc scan and on-demand scans as requested.

The OCIO VM Team will:

- Inventory all assets (hardware, software and systems and version numbers for all operating systems, software systems) across the network and identify host details including operating system and open services to identify vulnerabilities.
- Scan Department infrastructure environments at least monthly
- Add systems discovered during scanning to the asset inventory to ensure that all systems are identified and patched accordingly.
- Conduct Dynamic Application Security Testing (DAST) web application scanning, database scanning and source code composition for the assets hosted on a reoccurring basis.
- Identify security vulnerabilities on a regular automated schedule.

5.2 ANALYSIS

During the analysis phase the OCIO VM Team will assess and analyze the vulnerability information detailed in the final scan reports

The OCIO VM Team will:

- Analyze all scan results and provide quality remediation plans that explain to the ISOs and ISSOs the needed actions/ remediation plans to secure their systems. The OCIO VM Team has five (5) business days to complete a scan analysis. Ad-hoc scan requests should be submitted to the OCIO_VM@ed.gov mailbox no less than five (5) business days prior to the requested scan date.
- Communicate the results with the stakeholders in the Department approved format. PDF scan reports are provided, with detailed listing of scan findings in the form of a Cyber Security Assessment and Management (CSAM) POA&M Creation template.
- Provide the capability to cover quarterly Tabletop Exercises for testing the contingency plan and incident response plan to the Department's systems.

5.2.1 Vulnerability Scanning

The vulnerability scanning process is designed to test and analyze systems and services for known vulnerabilities. According to NIST, the Department can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage. NIST SP 800-53A provides additional information on the breadth and depth of vulnerability scanning coverage.

The OCIO VM Team will:

- Conduct DAST web application scanning and database scanning for the assets whether hosted on premise or in the cloud on a reoccurring basis.
- Ensure that vulnerabilities that were exploited and resulted in incidents were remediated e.g., vulnerability scanning reports.
- Prioritize the vulnerabilities by criticality and resulting actions per the Department existing policies and procedures.
- Establish a vulnerability discovery capability to be used to scan and detect vulnerabilities findings on a regular basis.

5.2.2 False Positives

The OCIO VM Team will:

- Establish a mechanism to track false positive vulnerabilities.
- When possible, the findings will be validated; if a finding is a false positive, it will be notated within the CSAM template.
- Identify, analyze, and track false positives on vulnerability reports, when feasible.

5.2.3 Risk Assessments

Risk assessments identify the recognized threats, threat actors and the probability that these factors will result in an exposure or loss.

The OCIO VM Team will:

- Express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention
- Utilize the Common Vulnerability Scoring System (CVSS) v3, or similar approach, to communicate the characteristics and severity of vulnerabilities. Metrics include defining the severity thresholds of vulnerabilities in accordance with the Department's risk tolerance, such as requiring no known vulnerabilities in the delivered system with a Common Vulnerability Scoring System (CVSS) severity of medium or high.

  The OCIO VM team uses the Vulnerability Priority Rating (VPR) to help improve the remediation efficiency and effectiveness of its customers by rating identified vulnerabilities based on severity level determined by the following components: threat intelligence, risk exposure and technical impact. The OCIO VM Team will continue to evaluate other scoring systems as they emerge and adopt them based on suitability and Department need.
- Prioritize the vulnerabilities and resulting actions per the Department's existing policies and procedures.
- Provide remediation plans that explain to the ISOs and ISSOs the needed actions/ remediation plans to secure their systems.
- Provide monthly web and database scans performed to assess the Department security posture using approved Department provided tools.

- Perform internal and external vulnerability testing to include Federal Risk and Authorization Management Program (FedRAMP) certified Cloud service providers.

5.3 REMEDIATION

The objective of the Remediation Phase is to eliminate/fix the vulnerability or mitigate the system or its operating environment. The Department OCIO VM Team will identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities as derived from scanning.

5.3.1 Remediation Actions

The OCIO VM Team will analyze, prioritize, and identify vulnerabilities according to the critically of the finding and business risk. This allows ISOs to establish controls and track progress.

5.3.2 Remediation Timelines

Once the analysis period concludes, ISOs are required to remediate findings based on the risk designation below to close the finding. The ISO must provide the OCIO VM Team with remediation evidence within the designated remediation periods.

The OCIO VM Team will:

- Communicate that Plans of Action and Milestones (POA&Ms) should be injected into the Department's system of record for vulnerabilities that have exceeded the remediation timeline as documented in the latest Plan of Action and Milestones (POA&M) Standard Operating Procedures (SOP)

  It remains the ISO's responsibility to ensure that vulnerabilities are remediated within the Department OCIO timeframes based on criticality ratings as documented in the Department's policies, procedures, standards, etc.

  - Zero Day: **24-48 hours** of the discovery date
  - Critical: **15 calendar days** of the discovery date
  - High: **30 calendar days** of the discovery date
  - Moderate: **90 calendar days** of the discovery date
  - Low: **180 business calendar days** of the discovery date

    NOTE: Internal systems shall have an additional 30 days for analysis per OCIO STND-01

5.4 VERIFICATION

After a vulnerability is remediated the OCIO VM Team can verify that remediation was successful with subsequent scans.

5.4.1 Rescans

Per NIST requirements the vulnerabilities to be scanned should be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities are identified and addressed as quickly as possible.

The OCIO VM Team will:

- Provide a template to ISOs, ISSOs and other related stakeholders to track vulnerabilities, remediation, false positives etc. until they are no longer present, or the associated risk are remediated.
- Re-scan to ensure the vulnerabilities are remediated and not showing on the current report.

5.4.2 Reporting

Reports identify compliance to ongoing VM activities as defined in this standard.

The OCIO VM Team will:

- Provide Web and database scan results documented in individual systems/applications reports.
- Communicate the results with the stakeholders in the Department approved format.
- Communicate results and needed actions with stakeholders in a timely manner.
- Provide weekly, monthly, and ad-hoc reports identifying compliance to ongoing VM activities defined in this standard.
- Provide monthly analysis reports of security configuration management to the VM Program Manager following the common vulnerability reporting framework.
- Communicate the results/ outcome/ Action Report after conducting the conducting the quarterly Tabletop Exercises.

5.5 DISPOSITION

In the disposition phase of the vulnerability management process the OCIO VM Team is responsible for ensuring some designated continuous monitoring activities.

5.5.1 Continuous Monitoring

Threats to the Department's information systems are dynamic and persistent. This standard identifies one of the most critical components of vulnerability management, continuous monitoring.

The OCIO VM Team will:

- Periodically review critical system resources for ensuring the applicable hardening is reported to the OCIO VM Team Program Manager.
- Review ninety (90) password expirations for the credentials used for OCIO VM Team scanning tools.
- Periodically review Department network architecture and topology in coordination with other teams to ensure a layered, defense-in-depth approach is being utilized.
- Provide continued vulnerability scanning and analysis.
- Follow Continuous Diagnostics and Mitigation (CDM) and Information Security Continuous Monitoring (ISCM) requirements gathering guidelines from a vulnerability reporting and tracking dashboard standpoint to include, but not limited to the following tools: Tenable Nessus, CDM dashboard & eco system, Cyber Data Lake, DbProtect, WebInspect, and Qualys.

6 APPENDIX A: ACRONYMS

A&A	Assessment and Authorization
BOD	Binding Operational Directive
CDM	Continuous Diagnostics & Mitigation
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DAST	Dynamic Application Security Testing
EDSOC	Department of Education Security Operations Center
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IAS	Information Assurance Services
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
IV&V	Independent Verification & Validation
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
PDF	Portable Document Format
POA&M	Plan of Action and Milestones
PM	Program Manager
RMF	Risk Management Framework
SOP	Standard Operating Procedure
VM	Vulnerability Management

7 APPENDIX B: TOOLS

The following table summarizes the tools used during the VM process. These tools support the requirement to remediate discovered vulnerabilities within the Department set timelines based on the risk rating as documented in the Department Baseline Standard (OCIO-STND-01).

VULNERABILITY TOOL	SCAN TARGET	FREQUENCY	OWNERSHIP
WebInspect	Web Application Servers	Monthly	OCIO VM
DbProtect	Database Servers	Monthly	OCIO VM
Tenable SC	Infrastructure	Twice per week	PIVOT H
Tenable IO	Infrastructure, Web Apps	Weekly	PIVOT I
PSHTT	Web Apps	Monthly	OCIO VM

8 APPENDIX C: GLOSSARY

Term	Definition	Source
Remediation	Correction of the vulnerability or elimination of the threat. Examples of remediation efforts include installation of a software patch, adjustment of a configuration setting, or removal of affected software.	NIST Dictionary https://csrc.nist.gov/glossary/term/Dictionary
Vulnerability	Software flaw or misconfiguration that causes a weakness in the security of a system. Vulnerabilities can be exploited by a malicious entity to violate policies—for example, to gain greater access or permission than is authorized on a computer.	NIST Dictionary https://csrc.nist.gov/glossary/term/Dictionary

Term	Definition	Source
Vulnerability Management	An ISCM capability that identifies vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.	NISTIR 8011 Vol. 1 under Capability, Vulnerability Management
Vulnerability Scan	Scan to identify hosts/host attributes and associated vulnerabilities.[1] Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm	NIST Dictionary https://csrc.nist.gov/glossary/term/Dictionary

9 APPENDIX D: AUTHORIZING REFERENCES

- Department policies, standards and procedures related to the vulnerability management area
- Department's Cybersecurity Risk Management Framework standard
- Department's Information Security Continuous Monitoring (ISCM) Roadmap
- DHS Binding Operational Directive (BOD 20-01), "Develop and Publish a Vulnerability Disclosure Policy."
- DHS BOD 18-02 - Securing High Value Assets
- Executive Order (EO) 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.
- Federal and Department PII Breach Response policies (such as OMB-M-17-12), the Department's Breach Response Plan
- Federal Information Security Modernization Act (FISMA) of 2014
- FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST - Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-40 Rev. 3 Guide to Enterprise Patch Management Technologies
- NIST SP 800-53r4 - Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- OCIO: 03-112, "Cyber-Security Policy," and its subsequent child standard documents on the CRMF, "Identify," "Protect," "Detect," "Respond," and "Recover."
- OMB Circular A130
- OMB M-11-33, FAQ 15
- OMB M-19-02 - Year 2018-2019 Guidance on Federal Information Security and Privacy
- OMB M-19-03
- OMB M-20-32 - Improving Vulnerability Identification, Management, and Remediation