Standard DE.CM: Cyber Hygiene

February 10, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.10 19:04:11 -05'00'

_____ _____

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
1.0	7/26/2019	Initial draft
1.0	12/20/2019	Underwent annual policy review for accuracy and timeliness and to incorporate updates to NIST SP 800-53 Rev. 4. & DHS BOD 19-02 reporting procedures.
1.1	1/17/2020	Revision to Section 2.3 to include 30-day analysis period for remediation of internally facing vulnerabilities.
1.2	1/25/2021	Underwent annual policy review for accuracy and timeliness. Standardized Risk Acceptance and Policy Exceptions verbiage. Updated references in Appendix A.

Table of Contents

1. INTRODUCTION 1

1.1. Purpose 1

1.2. Background 1

1.3. Scope 1

2. STANDARD 1

2.1. Overview 1

2.2. ED Coordination with NCATS 1

2.3. Remediation Deadlines for Vulnerabilities 2

2.4. Deadline Noncompliance 2

2.5. Notification of IP Inventory Changes 2

2.6. Removal of IPs Blocks 3

2.7. Configuration of SIEM Sensors 3

2.8. NCATS Reporting 3

2.9. Binding Operational Directive 19-02 4

3. RISK ACCEPTANCE/POLICY EXCEPTIONS 4

APPENDIX A: RESOURCES AND REFERENCES 4

1. INTRODUCTION

1.1. Purpose

This document establishes the Department standard for remediating information system vulnerabilities identified by Department of Homeland Security (DHS) Cyber Hygiene scanning. It supersedes any prior documentation establishing such a standard.

1.2. Background

DHS Binding Operational Directive (BOD) 19-02 (*Vulnerability Mitigation Requirements for Internet-Accessible Systems* (April 29, 2019) supersedes and revokes BOD 15-01, *Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (May 21, 2015). In doing so it sets a shorter timeframe for the remediation of system vulnerabilities identified by National Cybersecurity Assessments and Technical Services (NCATS) "Cyber Hygiene" scans.

1.3. Scope

The standard established in this document applies to all employees, contractors, and users authorized to access ED information systems, systems operated or maintained on behalf of ED, or ED information.

2. STANDARD

2.1. Overview

National Cybersecurity Assessments and Technical Services (NCATS) conducts regular Cyber Hygiene scans on the Department's Internet-facing systems to find and report vulnerabilities and configuration weaknesses. The scope of scans includes all static, public IP addresses. Once initiated, scans are automated and require little direct interaction from Department personnel.

2.2. ED Coordination with NCATS

All ED Cyber Hygiene related activities must be coordinated through Information Assurance Services (IAS) at OCIO_IAS@ed.gov. **All Cyber Hygiene related communications with IAS must be noted as such in the subject line.** Upon request from IAS, system stakeholders must submit updated Cyber Hygiene agreements to OCIO_IAS@ed.gov.

2.3. Remediation Deadlines for Vulnerabilities

Information System owners (ISO), Information System Security Officers (ISSOs), and/or other relevant system stakeholders must remediate vulnerabilities detected on externally facing systems (including High Value Assets [HVAs] and systems or assets with FIPS 199 High categorization) as follows:

- **Critical vulnerabilities** must be remediated within **15** calendar days of initial detection.
- **High vulnerabilities** must be remediated within **30** calendar days of initial detection.
- **Moderate vulnerabilities** must be remediated within **90** calendar days of initial detection.
- **Low vulnerabilities** must be remediated within **180** calendar days of initial detection.

No later than three (3) calendar days after the deadline, system stakeholders must notify IAS of any remediation actions taken, and IAS in turn will notify NCATS.

Note: For **internally facing systems only**, system stakeholders are allowed a 30-day analysis period prior to the initiation of the timeframes listed above.

2.4. Deadline Noncompliance

- If critical and high vulnerabilities are not remediated within the above specified timeframes, NCATS will provide a partially populated remediation plan to ED DHS points of contact for validation and population. IAS DHS POCs will disseminate the POA&M template to the respective Information System Owners (ISOs). ISOs for the associated system will need to validate and populate for their associated system. IAS working with the Department POCs shall return the completed remediation plan ***within three working days*** of receipt to DHS through CyberScope.
- NCATS and IAS will use Cyber Hygiene scanning to track and validate the remediation of identified vulnerabilities and will engage senior Department leadership as necessary and appropriate to ensure compliance.

2.5. Notification of IP Inventory Changes

Relevant system stakeholders must notify IAS (OCIO_IAS@ed.gov) of any changes to the Internet-facing IP inventory **within three (3) days of a change**. This includes any newly acquired public, static IPv4 addresses or any addresses recently returned to the Internet

Service Provider (ISP). Cyber Hygiene is unable to scan domains, dynamic IPs, or IPv6 addresses. IAS in turn will notify NCATS of this change directly.

2.6. Removal of IPs Blocks

Cyber Hygiene scanning is focused on quickly exposing vulnerabilities prior to their exploitation and makes no attempt at stealth. Consequently, Cyber Hygiene scans may trigger Intrusion Prevention System (IPS) capabilities. If an IPS capability prevents Cyber Hygiene access, system stakeholders must promptly remove the relevant block and notify OCIO_IAS@ed.gov. In turn, IAS will notify NCATS at NCATS@hq.dhs.gov so the scan can be repeated if necessary. To distinguish Cyber Hygiene scans from other system penetration attempts, NCATS publishes its scanning addresses at https://rules.ncats.cyber.dhs.gov.

2.7. Configuration of SIEM Sensors

To reduce alerts and conserve analyst resources, security information and event management (SIEM) sensors can be configured to not generate alerts on traffic from NCATS published addresses, however addresses may change without notice, so regular monitoring is necessary. There is no need to whitelist Cyber Hygiene or to open any ports or services beyond what is normally available for Department systems.

2.8. NCATS Reporting

To further ensure compliance with this Standard, NCATS will:

- Provide to the Department regular reports on Cyber Hygiene scanning results and current status, and to Department leadership a Federal Enterprise "scorecard"
- Provide standard remediation plan templates for the Department to populate if remediation efforts exceed required timeframes
- Engage Department POCs to discuss remediation status and provide technical expertise for the remediation of specific vulnerabilities, as requested and appropriate
- Engage Agency Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other relevant personnel throughout the escalation process, if necessary
- Provide monthly Cyber Hygiene reports to Office of Management and Budget (OMB) to identify cross-agency trends and persistent challenges, and to facilitate policy and/or budget-related actions and remedies.

2.9. Binding Operational Directive 19-02

DHS Binding Operational Directive 19-02 (*Vulnerability Remediation Requirements for Internet-Accessible Systems*, April 29, 2019) supersedes and revokes BOD 15-01, *Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (May 21, 2015). To view the full text and further information on how to apply this Directive, go to https://cyber.dhs.gov/bod/19-02/ .

3. RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: RESOURCES AND REFERENCES

- Department of Homeland Security: *Cybersecurity and Infrastructure Security Agency - Binding Operational Directive 19-02* (BOD 19-02), 2019