Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

BINDING OPERATIONAL DIRECTIVE 2026-03-06

Remediation of Known Exploited Vulnerabilities
(KEV)
on Public-Facing Assets

Date Issued: March 6, 2026

Table of Contents

Revision Control History

Version	Author(s)	Date	Description
1.0.0	Miheer Khona	March 6, 2026	Initial Version

Background

The Department of Information Technology (DoIT), Office of Security Management (OSM) is responsible for establishing security requirements for State information systems and information technology (IT) resources pursuant to Maryland Code, State Finance & Procurement (SF&P) § 3.5-2A-04; and is headed by the State Chief Information Security Officer (SCISO), in accordance with SF&P § 3.5-2A-03.

Pursuant to SF&P § 3.5-2A-04, OSM oversees the direction, coordination, and implementation of the overall cybersecurity strategy and policy for units of State government. OSM is also charged with developing and maintaining information technology security policy, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology (NIST).

The SCISO issues this Binding Operational Directive (BOD) in accordance with the Maryland Cybersecurity and Privacy Policy Suite.

BOD Authority

All units of State government are required to comply with this BOD. Any failure to immediately comply, is considered a violation of Maryland Cybersecurity & Privacy Policy Suite and, per SF&P Code 3.5-2a-04(b)(6), may result in the SCISO determining, directing, or taking actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.

The technical execution and enforcement of Known Exploited Vulnerability (KEV) remediation are governed by the System and Information Integrity Standard (MD-STD-319-SI-01). This Standard is a core component of the Maryland Cybersecurity and Privacy Policy Suite, intentionally designed to position all state agencies to maintain a defensible posture against active threats.

Scope & Applicability

Scope

State Government: Unless otherwise expressly exempted, all agencies or units of the Executive Branch of State government including departments, agencies, boards, and commissions.

Local Government entities, including but not limited to, counties, municipalities, and public schools, are highly encouraged to prioritize inventorying and patching public-facing assets to reduce the risk of exploitation by threat actors.

Applicable Systems

This BOD addresses KEVs impacting public-facing assets on State-owned and/or operated infrastructure (e.g., data centers, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and environments (e.g., AWS, Azure, Google Cloud)) where the State agency retains direct responsibility for operating system, network, or application-level patching.

In cases where DoIT maintains administrative control over an agency's information systems, DoIT assumes primary responsibility for the technical remediation of identified vulnerabilities.

Exemptions

Software-as-a-Service (SaaS) and fully vendor-managed or operated solutions within vendor-hosted infrastructure environments—where the State agency does not have administrative access to patch the underlying infrastructure or applications — are exempt from the scope of this BOD.

Definitions

A **BOD** is a mandatory instruction requiring specific actions to safeguard Maryland information systems (see MD-POL-100 Cybersecurity & Privacy Governance Policy). Each directive is applicable to the State units, or other State-owned network users, identified in the directive. These directives typically address internal cybersecurity practices required to mitigate operational risk; are issued to establish and maintain uniform practices in a specific area of risk; and are generally long-term and remain in effect until officially modified or revoked.

A **KEV** refers to a security flaw listed in the KEV Catalog maintained by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). This catalog is the authoritative source of vulnerabilities that have been actively exploited in the wild, meaning attackers are already using them to compromise systems.

A **public-facing** asset is any managed information system, edge device, application, service, or infrastructure component that is directly accessible from the public internet, whether hosted on-premises or in managed cloud environments (e.g., IaaS, PaaS).

Examples include (non-exhaustive):

- Internet-accessible web applications and websites (e.g., customer portals, content management systems, etc.)
- VPN gateways and remote access services
- Email gateways
- External authentication portals
- Internet-accessible infrastructure (e.g., routers, firewalls, load balancers, etc.)

Specific Actions

1. Upon receipt of a public-facing asset vulnerability report from OSM, agencies must either patch the asset, disconnect from public-access, request an extension, or accept risk as defined in Appendix A for their unpatched asset. This is to be accomplished within 7 calendar days, or the timeframe specified within the public-facing asset vulnerability report.

2. To ensure comprehensive visibility into the State's external risk posture, all agencies are required to submit an inventory of their public-facing assets within 30 days of this BOD publication to the agency Information Security Officer (ISO) using the Public-Facing Asset Data Call sheet. This data call is essential for coordinating the rapid remediation of identified vulnerabilities and maintaining a centralized registry of Maryland's public-facing infrastructure.

    a. **Required Public-Facing Asset Data Elements:** For each public-facing asset, agencies must provide, at a minimum, the IP address, website URL hosted on the asset, primary mission use, and associated hardware and software vendor (if applicable), as well as the DNS name utilizing the Public-Facing Data Call sheet provided by the agency ISO.

b. **Points of Contact (POC):** Each submission must designate a formal technical POC for receiving OSM public-facing vulnerability reports and coordinating or executing necessary patches.

c. **Submission and Inquiry:** All inventory data, along with any questions or comments related to the data call, must be reported to the assigned agency ISO via state.iso@maryland.gov.

3. Remediation is not considered complete until it is technically validated. OSM will conduct vulnerability scans to confirm the vulnerability is no longer exploitable.

Requesting Risk Acceptance or Extension

If vendor patches are unavailable or the system cannot be disconnected or decommissioned due to mission criticality, agencies must document risk acceptance with compensating controls in the KEV Non-Compliant Risk Acceptance Memo described in Appendix A within 7 calendar days or the timeframe specified in the public-facing asset vulnerability report.

Agency Head (or a designee with executive authority) must formally report any asset with a KEV that has not been remediated within the timeframes established by this BOD to OSM. This report shall be submitted by the Agency IT Lead (or designee), to the agency's assigned ISO using a Non-Compliant Risk Acceptance Memo (see Appendix A). If an extension is required, the expected completion date must be noted in the non-compliant data sheet and submitted with the Non-Compliant Risk Acceptance Memo.

The Agency Head (or a designee with executive authority) submission of a Non-Compliant Risk Acceptance Memo shall constitute formal risk acceptance (business and IT) associated with continued exposure to a KEV. This acknowledgment does not waive the obligation to remediate the vulnerability and does not preclude further direction or corrective action from the SCISO. The final acknowledgement of the agency's acceptance of the residual risk associated with this policy exception identified in this memo will be approved by the SCISO, or their designee.

Submission and Reporting

Submission:

1. All in-scope units of State government shall submit the required documents listed below by email to state.iso@maryland.gov:
    a. Agency Non-Compliant Memo (per Appendix A)
    b. Non-Compliant Data sheet
    c. Public-Facing Asset Data Call sheet
2. The agency ISO shall acknowledge receipt of submissions to the submitter.
3. Late submissions will be recorded as reporting deficiencies and will be escalated.
4. Failure to submit required reports to the agency assigned ISO or state.iso@maryland.gov in accordance with this BOD constitutes non-compliance.

Incident Reporting:

Immediately report any potential or actual cybersecurity incidents arising during the vulnerability remediation process to the Maryland Security Operations Center:

- **Email:** soc@maryland.gov
- **Phone:** 410-697-9700, option 5
- **Availability:** The MD-SOC operates 24x7

Appendix A – Agency Non-Compliant Memo

FROM: [Agency IT Lead]

TO: State Chief Information Security Officer (SCISO)

DATE: [Date]

SUBJECT: Non-Compliant Risk Acceptance Memo for Binding Operational Directive (BOD) 2026-03-06

I am writing to formally acknowledge receipt of Binding Operational Directive (BOD) 2026-03-06 regarding the remediation of Known Exploited Vulnerabilities (KEV). I have reviewed the requirements established by the Office of Security Management (OSM) under Maryland Code, SF&P § 3.5-2A-04, and I understand the mandatory actions required to safeguard our agency information systems.

I have directed my IT leadership to prioritize the patching of KEVs for public-facing assets specified in BOD 2026-03-06. All non-remediated KEVs will follow the corresponding requirements in the non-compliant data sheet. My agency will ensure that all non-remediated KEVs, patch timeline extensions, this Non-Compliant Memo, and the Non-Compliant data sheet are submitted to their Agency Information Security Officer (ISO) and copied to state.iso@maryland.gov within the established timelines.

The non-compliant data sheet constitutes the minimum required data for a well-documented report. I confirm that this information is completed in its entirety and is attached to this memo to provide the necessary technical and operational context.

I understand that my signature on this memo constitutes formal acceptance of the risk associated with continued exposure. Furthermore, I acknowledge the SCISO's authority to direct the disconnection of any system to protect the State's infrastructure should our security posture be deemed insufficient.

Our agency [ ] has [ ] has not enrolled in DoIT Vulnerability Scanning, Assessment and Testing Services.

By signing below, the Agency Head and Authorizing Official accept the residual risk associated with this policy exception.

Authorizing Official

Print: ____________________________________ Date: __________

Signature: ____________________________________ Date: __________

Agency Head

Print: ____________________________________ Date: __________

Signature: ____________________________________ Date: __________

SCISO Acknowledgement: I [ ] do [ ] do not approve the agency’s acceptance of the residual risk associated with this policy exception identified in this memo.

______________________________________ ____________________

James Saunders Date

State Chief Information Security Officer (SCISO)

Department of Information Technology

Appendix B – Frequently Asked Questions FAQs

This FAQ provides additional clarity on the boundaries of responsibility within BOD 2026-03-06.

1. How should we handle systems that are vendor-managed or vendor-operated?

While Software-as-a-Service (SaaS) and fully vendor-managed or vendor-hosted solutions are not currently in the scope of this BOD. It is recommended for agencies to remind their contractors or vendors of their cybersecurity responsibilities within their contract.

2. Does this Directive apply to local government and public schools?

Local government entities, including, but not limited to, counties, municipalities, and public schools, are highly encouraged to prioritize inventorying and patching public-facing assets to reduce the risk of exploitation by threat actors. Maintaining a secure and resilient environment is a collective effort, and following this directive ensures that all entities connected to the state’s digital ecosystem are hardened against active threats. State minimum cybersecurity requirements still apply.

3. Who is responsible for patching systems where DoIT provides administrative support?

In cases where DoIT maintains administrative control over an agency’s information systems, DoIT assumes primary responsibility for the technical remediation and patching of identified vulnerabilities. There are cases where DoIT is responsible for the underlying operating system (OS) and agencies are responsible for hosted applications. In these instances, under the "Team Maryland" approach, DoIT and the respective agency will coordinate and collaborate to ensure technical and security requirements are met per this BOD and the System and Information Integrity Standard (MD-STD-319-SI-01) to minimize mission disruption.

4. What about internal (non-public facing) patching?

While the immediate priority of this BOD is to patch (i.e., secure) the State's public-facing assets, the Maryland Cybersecurity and Privacy Policy and System and Information Integrity Standard (MD-STD-319-SI-01) applies to all state assets.

5. Will OSM document agency vulnerabilities?

OSM will provide agencies with public-facing vulnerability reports aligned with the scope of this BOD shortly after its publication. Subsequent public-facing vulnerability reports will be shared with impacted agency POCs as they become available whenever new vulnerabilities are detected. Any non-impacted agency will not be contacted immediately, provided no vulnerable instances have been identified within their public-facing assets. OSM will continue to refine vulnerability management processes, including the identification, communication, and tracking of vulnerabilities, through methods such as automated notifications.