



CISA BOD 26-04

Risk-Based Remediation Needs Superintelligent ZTHA

From Asset Visibility to AI-Powered
Hardware Truth, Risk Intelligence,
and Zero Trust Hardware Access

Executive Summary

CISA Binding Operational Directive 26-04, issued June 10, 2026, moves federal vulnerability remediation toward a risk-based model. Remediation deadlines are determined by asset exposure, known exploitation, exploit automation, and technical impact. Agencies must also continuously identify and tag relevant assets and report through established federal processes.

Yet there is a fundamental challenge: remediation decisions are only as reliable as the underlying asset intelligence.

Hidden hardware, identity spoofing, and unmanaged devices can create critical visibility gaps even in mature vulnerability management programs.

Sepio combines trafficless physical-layer discovery, verified Hardware AssetDNA, and AI-powered Superintelligent ZTHA to turn large volumes of hardware intelligence into actionable insights, contextualized risk assessments, and policy-driven decisions.

Sepio strengthens the foundation of BOD 26-04 implementation by improving hardware visibility and identity confidence while complementing vulnerability scanners, CISA KEV intelligence, exposure assessment platforms, and remediation systems.

1 From BOD 23-01 Visibility to BOD 26-04 Action

CISA BOD 23-01 established the importance of recurring asset discovery and vulnerability enumeration across federal networks.

BOD 26-04 advances the discussion: agencies must not only identify vulnerable assets but also determine which require urgent remediation.

This progression introduces a crucial question:

How can an agency prioritize the risk of hardware it cannot see, or whose identity it cannot verify?

Sepio's AI-powered Superintelligent ZTHA supports a four-stage approach:



DISCOVER

Identify managed, unmanaged, hidden, and rogue hardware.



VERIFY

Establish hardware identity using physical-layer AssetDNA.



ANALYZE

Apply AI-powered intelligence to identify anomalies and contextualize hardware risk.



ACT

Translate verified identity and risk intelligence into policy-driven mitigation through supported integrations.

This turns hardware discovery into actionable intelligence, supporting the risk-based principles behind BOD 26-04.

2 Understanding BOD 26-04

BOD 26-04 replaces BOD 19-02 and BOD 22-01 and applies to covered Federal Civilian Executive Branch information systems.

Its remediation framework considers four primary variables:

Variable	Central question
ASSET EXPOSURE	Is the affected asset publicly exposed?
KNOWN EXPLOITATION	Is the CVE listed in CISA's Known Exploited Vulnerabilities catalog?
EXPLOIT AUTOMATION	Can the full exploitation sequence be automated?
TECHNICAL IMPACT	Would successful exploitation provide partial or total control?

Depending on these factors, required remediation may range from three calendar days to longer timelines or the next system upgrade. Certain high-risk combinations additionally require forensic triage.

The directive also introduces requirements involving asset identification, tagging, address information, and reporting.

Importantly, proprietary hardware risk scores do not replace the official criteria used to determine remediation deadlines.

3 The Hardware Visibility Gap

Traditional vulnerability management depends heavily on network discovery, authenticated scanning, software inventories, and known asset records.

However, many organizations operate with hardware that remains unidentified, misclassified, or improperly trusted.

Examples include unmanaged network switches, unauthorized endpoints, transparent inline devices, rogue peripherals, dormant devices, and hardware impersonating approved assets.

These devices can introduce multiple problems:

VULNERABLE HARDWARE

may remain
outside the
scanning scope

ASSET RECORDS

may contain
incorrect
identities or
classifications

SECURITY TEAMS

may investigate
the wrong
devices

ROGUE HARDWARE

may introduce
risks that
cannot be
captured
through CVE
data alone

BOD 26-04 makes accurate asset intelligence even more important because remediation priorities depend on knowing which actual systems are affected and how they are exposed.

You cannot accurately assess the risk of an asset whose physical identity has not been established.

4 Sepio: Applying AI-Powered Superintelligent ZTHA

Discover Hardware Beyond Conventional Visibility

Sepio's trafficless discovery technology utilizes network infrastructure metadata and physical-layer characteristics without requiring packet capture, SPAN ports, or deep packet inspection.

This approach enables organizations to discover managed and unmanaged hardware, including certain hidden and transparent devices that conventional IP-based discovery may overlook.

For agencies implementing BOD 26-04, Sepio helps expand the visibility foundation supporting asset inventory and vulnerability assessment.

Verify Hardware Identity with AssetDNA

Hardware AssetDNA analyzes physical-layer characteristics to help establish what a connected device actually is, rather than relying exclusively on identifiers it reports.

This provides an independent signal for detecting spoofing, masquerading, unexpected network connections, and anomalous hardware characteristics.

For vulnerability management, verified identity can improve confidence that assessment results are associated with the correct physical assets.

Transform Hardware Data into Intelligence with AI/SI

Large organizations generate extensive amounts of hardware-related metadata. Identifying important anomalies manually can be difficult.

Sepio's AI-powered Superintelligent ZTHA helps translate physical-layer signals and device characteristics into actionable risk intelligence.

Through Asset Risk Factor and Risk Indicators, Sepio can highlight conditions such as:

- ✓ Hardware AssetDNA anomalies.
- ✓ Unexpected network port characteristics.
- ✓ Unusual or rare devices.
- ✓ Unsupervised network infrastructure.
- ✓ Suspicious or inconsistent hardware identities.

These additional signals enable security teams to investigate hardware risks that may not be apparent from CVE severity alone.

They enrich enterprise risk decisions without replacing the directive's mandated prioritization variables.

Turn Intelligence into Risk Mitigation

Discovering and classifying hardware risk is valuable only when organizations can respond.

Sepio's Zero Trust Hardware Access approach translates verified hardware identity and risk intelligence into policy decisions and security workflows.

Through supported integrations, organizations can pursue actions such as network restrictions, isolation, escalation, and additional investigation.

This is particularly valuable where immediate patching may be difficult, including legacy infrastructure, sensitive operational environments, and critical systems.

However, compensating controls or isolation do not automatically satisfy all directive remediation requirements. Agencies must establish and document the actual change in exposure and fulfill their applicable obligations.

Enrich Federal Inventory and Reporting Processes

Sepio provides hardware intelligence, topology context, anomalies, and asset records to established security and IT management systems.

Integration with CMDB, SIEM, and vulnerability management workflows can help agencies reconcile discovered hardware against existing inventories.

Specific CDM reporting integrations, field mappings, data completeness, and reporting schemas must be validated for each deployment.

5 The AI/SI Difference: From Physical Signals to Intelligent Action

Sepio's Hardware Superintelligence positioning addresses the gap between collecting hardware signals and extracting actionable meaning.

DISCOVER → **VERIFY** → **ANALYZE** → **ACT**

This sequence supports BOD 26-04 implementation in several ways.



Discovery helps reduce overlooked hardware assets.



Identity verification strengthens the reliability of asset inventories.



AI/SI highlights hardware anomalies and suspicious device characteristics that may warrant additional investigation.



Integration-based response enables validated hardware context to inform containment and remediation workflows.

The operational result is a more trustworthy hardware intelligence foundation for existing vulnerability management processes.

Formal CVE assessment, KEV matching, public exposure validation, remediation timetable calculation, and required reporting remain the responsibility of the organization's established cybersecurity tools and procedures.

6 Mapping BOD 26-04 to Sepio

BOD 26-04 activity

Sepio contribution

**IDENTIFY AND
CLASSIFY ASSETS**

Trafficless hardware discovery and
AssetDNA verification

**IMPROVE ASSET
RECORDS**

Hardware type, identity, network
connection, and topology context

**SUPPORT VULNERABILITY
PRIORITIZATION**

AI-powered hardware risk intelligence
and anomalies

**SUPPORT REMEDIATION
WORKFLOWS**

Integration-enabled policy enforcement
and escalation

**IMPROVE INVENTORY
REPORTING**

Asset intelligence exports and
integration with management systems

SUPPORT INVESTIGATION

Hardware anomalies, asset relationships,
and physical identity evidence

Sepio complements the vulnerability and reporting platforms responsible for satisfying the directive's detailed technical requirements.

7 Illustrative Federal Use Case

Consider a federal agency operating a sensitive network environment.

Its vulnerability management solution identifies a newly exploited vulnerability affecting a specific class of network appliances.

The agency searches its inventory for potentially affected devices.

However, Sepio identifies an unexpected hardware signature on a switch port associated with an approved network asset.

Further investigation suggests that the connected hardware may be improperly classified or potentially unauthorized.

Sepio's AssetDNA and AI-powered anomaly intelligence provide additional evidence that prompts the security team to reassess the asset.

Investigators then correlate this physical hardware intelligence with existing CMDB, vulnerability, KEV, and external exposure data.

If the asset is confirmed vulnerable, the agency applies BOD 26-04's formal remediation requirements while using available policy enforcement and incident response capabilities.

The result is a more reliable workflow grounded in verified hardware identity rather than unquestioned logical identifiers.



8 Implementation Blueprint

A practical implementation can follow five stages:



BASELINE

Use Sepio to identify managed, unmanaged, and unexpected hardware connected to supported infrastructure.



RECONCILE

Compare discovered assets against CMDB, inventory, topology, and ownership records.



ENRICH

Correlate verified hardware assets with vulnerability scanner findings, KEV intelligence, and exposure information.



RESPOND

Apply authorized remediation and enforcement workflows, using supported integrations where appropriate.



DOCUMENT

Validate the resulting remediation status and ensure the required information is reflected in established CISA/CDM reporting processes.

Why Sepio Matters

BOD 26-04 represents an important development in federal cybersecurity: vulnerability remediation must increasingly reflect actionable risk, rather than severity scores alone.

But actionable risk management requires trustworthy asset intelligence.

Sepio addresses this challenge through a distinctive combination of trafficless hardware discovery, physical-layer verification, AI-powered Hardware Superintelligence, and Zero Trust Hardware Access.

Rather than replacing vulnerability management technologies, Sepio enriches their underlying understanding of the connected hardware environment.

Sepio's AI-powered Superintelligent ZTHA helps agencies base risk-based action on verified hardware truth.

Discover what
connects.
Verify what
it really is.
Understand
hardware risk.

**Turn intelligence
into Zero Trust
action.**