Axonius

AXONIUS FEDERAL

CISA BOD 26-04: How the New Directive Changes Your Approach to *Risk Management*

Evolving cybersecurity threats require a fundamental shift in how federal agencies approach vulnerability management. Rather than treating all vulnerabilities equally, agencies must focus on the vulnerabilities that are actively exploited and most likely to impact mission-critical systems.

To address these challenges, the Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive (BOD) 26-04: Prioritizing Security Updates Based on Risk. The directive establishes a modern, risk-based framework for vulnerability remediation that emphasizes continuous visibility, contextual risk analysis, and measurable operational processes.

Why BOD 26-04 Matters

BOD 26-04 requires agencies to adopt repeatable, evidence-based processes for managing internet-facing assets and prioritizing remediation according to real-world risk. Rather than relying primarily on CVSS scores or the presence of a vulnerability in the Known Exploited Vulnerabilities (KEV) Catalog, the directive evaluates multiple operational factors. You must also maintain an accurate understanding of everything within your external attack surface, continuously track agency-owned public IP addresses, and quickly identify and recover compromised internet-facing assets.

Risk prioritization is based on four primary factors:

Public exposure – Is the affected asset reachable from the Internet?

Known exploitation – Has the vulnerability been observed being exploited in the wild?

Automated exploitation – Can attackers automate exploitation?

Technical impact – Would exploitation result in partial or complete compromise?

Depending on these factors, agencies may have as little as three days to remediate the highest-risk vulnerabilities:

3 days: Highest-risk vulnerabilities

14 days: High-risk vulnerabilities

60 days: Moderate-risk vulnerabilities

Next scheduled system upgrade: Lower-risk vulnerabilities

Axonius

BOD 26-04: What You Should Do Now

To comply with BOD 26-04, you should immediately:

- Establish vulnerability management policies.
- Identify, inventory, and continuously track all public-facing IP addresses and internet-facing assets.
- Ensure complete visibility into your external attack surface—including unmanaged or previously unknown assets.
- Continuously monitor the CISA KEV Catalog
- Implement automated asset discovery, remediation tracking and workflows.
- Establish processes to rapidly identify compromised external assets and remove remediated systems from industry blocklists to restore trusted operations.

Longer-term milestones include transitioning to risk-based prioritization within 60 days and achieving complete asset visibility while eliminating unsupported edge devices within 180 days.

The Operational Capabilities You Need

Successfully implementing BOD 26-04 requires six foundational capabilities:

- Continuous asset visibility
- Dynamic risk prioritization
- Continuous exposure monitoring
- Ownership and accountability
- Automated response and workflow orchestration
- Evidence-based compliance reporting

Building these capabilities with disconnected point solutions is difficult. Agencies need a way to unify asset intelligence, vulnerability context, ownership information, public IP intelligence, and operational workflows into a single operational picture. You must be able to continuously understand everything in your perimeter, monitor changes in internet exposure, and rapidly respond when assets become vulnerable or compromised.

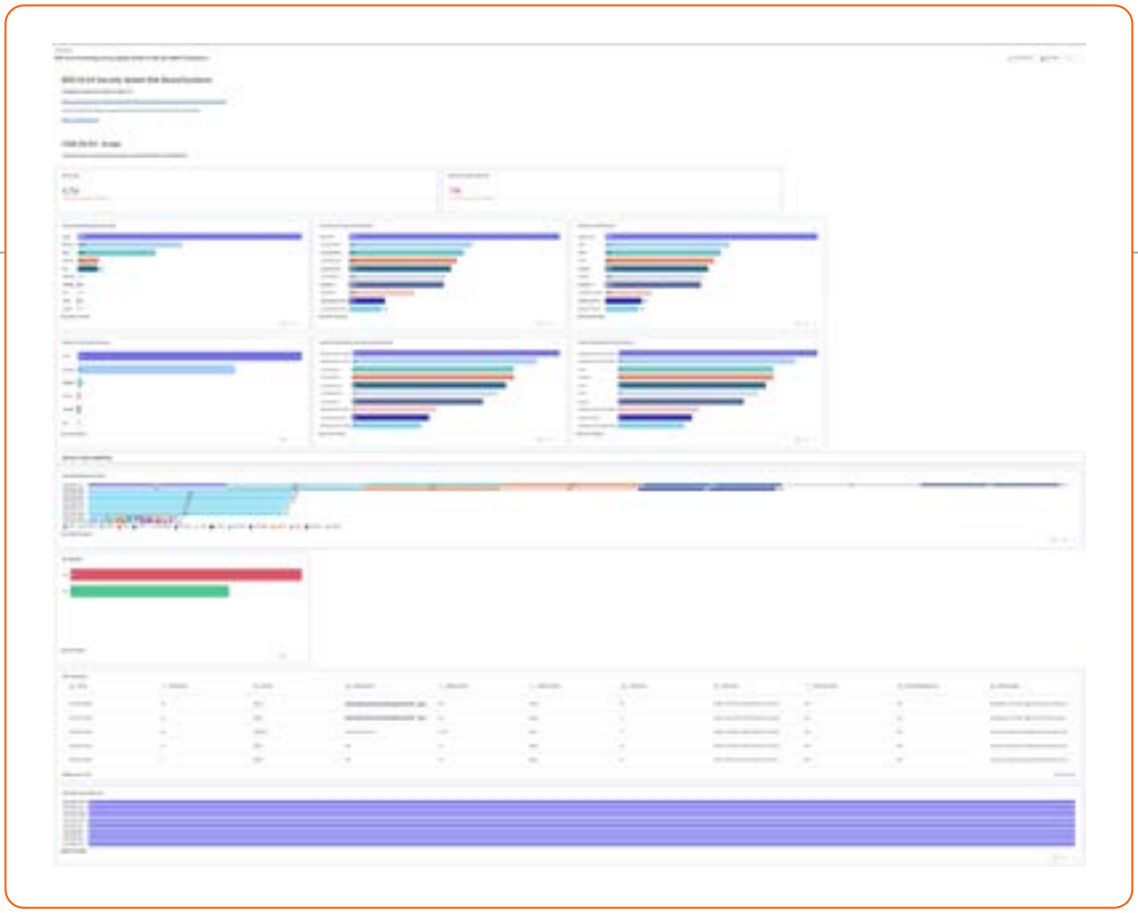
Axonius can help.

Axonius

How Axonius Operationalizes BOD 26-04

Modern, Complete Asset Visibility

Axonius aggregates and correlates data from security, IT, cloud, and infrastructure platforms to create a unified inventory of managed and unmanaged assets. Agencies can identify internet-facing systems, unmanaged devices, missing controls, and coverage gaps to better understand operational risk. Axonius also enables agencies to maintain continuous visibility into their external attack surface, including agency-owned public IP addresses and exposed assets that may otherwise go unmanaged.



Axonius customers are protected today with custom dashboards and complete visibility into vulnerabilities

Axonius

Continuous Monitoring of CISA KEV and Exposure

Axonius continuously enriches vulnerability findings with CISA KEV intelligence while monitoring changes in internet exposure. Newly elevated risks are identified quickly so teams can respond before compliance deadlines are missed. Agencies can also continuously monitor external IP space, detect newly exposed assets, and quickly determine when internet-facing systems require immediate action.

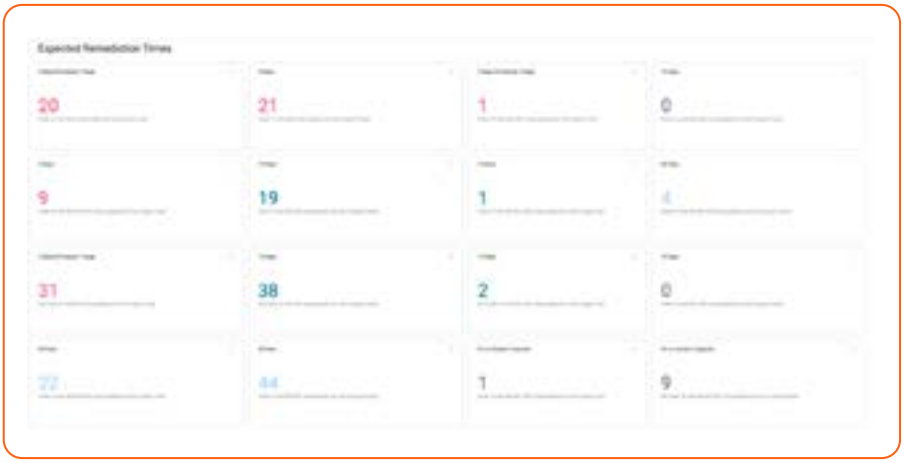
Risk-Based Prioritization

By correlating asset exposure, KEV status, exploitability, ownership, and technical impact, Axonius enables agencies to focus remediation efforts on the vulnerabilities that present the greatest operational risk.

Axonius identifies and prioritizes risk and vulnerabilities

Ownership and Accountability

Axonius correlates assets with authoritative ownership data, helping organizations assign remediation tasks, track progress, and maintain accountability across teams.



Axonius remediation activity tracking

Axonius

Investigation and Forensic Triage Support

Axonius provides a centralized view of affected assets, associated systems, security controls, and ownership information. Security and incident response teams can quickly scope investigations, identify potentially impacted systems, coordinate response activities across multiple teams, and track remediated external assets through recovery—including removing recovered systems from industry blocklists more efficiently.

Managing Data Overload

Axonius aggregates, normalizes, and correlates data from across the technology stack into a single operational dataset. Analysts can then understand assets, vulnerabilities, ownership, and risk without manually reconciling information across multiple systems.

Operational Response and Workflow Automation

Axonius supports automated workflows that initiate remediation, assign tasks, integrate with ITSM and security platforms, and accelerate investigation and incident response using a centralized operational view.

Expected Outcomes

With Axonius, you can

- Maintain continuous visibility across hybrid environments and your entire external attack surface.
- Continuously track agency-owned public IP addresses and internet-facing assets.
- Prioritize remediation using the criteria defined by BOD 26-04.
- Respond faster to KEV-driven threats.
- Automate remediation workflows, improve accountability, and accelerate recovery of compromised systems.
- Remove remediated external assets from industry blocklists more quickly.
- Generate dashboards and evidence for compliance reporting.
- Reduce operational risk while strengthening overall cyber resilience.

Axonius

Axonius: Your Trusted Partner

BOD 26-04 represents a significant evolution in federal vulnerability management. Success depends on maintaining continuous visibility into the attack surface, accurately prioritizing risk, and automating operational processes. You must know everything within your organization's perimeter, continuously monitor external IP space, and rapidly identify, remediate, and restore exposed systems as threat conditions evolve.

Axonius helps you operationalize these requirements by transforming fragmented asset, vulnerability, exposure, and ownership data into a single, actionable operational picture. The result is faster remediation, stronger compliance, and greater confidence in protecting mission-critical systems.

Learn more at

Axonius.com/federal-systems →

or

Request a Demo →

Axonius Federal Systems — Continuous Visibility for Superior Security.