Axonius

AXONIUS FEDERAL

Meeting *OMB M-26-14 Objectives* with Axonius

Threat actors are evolving the way they attack critical systems, increasingly leveraging automation and artificial intelligence to rapidly gain unauthorized access, move laterally across environments, and maintain persistent access while avoiding detection.

On May 22, 2026, OMB issued M-26-14, replacing M-21-31 with a risk-based approach to federal logging and network visibility. The memo prioritizes Continuous Event Monitoring (CEM) and Threat Hunting, Investigation, Response, and Forensics (THIRF) to help agencies defend against increasingly automated and AI-enabled threats. With Basic maturity required within 120 days of CISA's forthcoming Logging Reference Architecture and Advanced maturity within 320 days, agencies need complete asset-level visibility to identify coverage gaps, prioritize risk, and prove progress.

The Axonius Asset Cloud provides the visibility and evidence needed to meet each maturity milestone.

M-26-14 centers on two primary objectives:

- Continuous Event Monitoring (CEM): Logs, log management, and logging infrastructure that enable agencies to monitor network activity in real time, identify anomalous behavior, and respond to potential threats quickly and effectively.
- Threat Hunting, Investigation, Response, and Forensics (THIRF): Logs, log management, and logging infrastructure that enable agencies to investigate known or suspected compromises, conduct forensic analysis, and support mitigation, remediation, and recovery efforts.

Within 90 days of the memorandum's release, CISA will publish a Logging Reference Architecture (LRA) to provide agencies with implementation guidance for achieving CEM and THIRF objectives. The LRA is intended to build upon agencies' progress under M-21-31 while providing greater flexibility to address varying mission requirements and risk profiles.

Axonius

What Agencies Need to Do

Following publication of the Logging Reference Architecture, agencies must submit an Agency Logging Plan to OMB and CISA within 90 days.

Agency Logging Plans must:

- Describe the operational steps required to deploy and maintain effective CEM and THIRF capabilities.
- Document how the agency will meet M-26-14 minimum baseline requirements and any additional logging activ ities necessary to support mission needs and risk management objectives. As the architecture is revealed in 90 days this will become a continuous process, both in action and in documentation/proof evidence.

Timeline

Within 90 days	Within 120 days	Within 180 days	Within 320 days
Complete the initial Agency Logging Plan	Achieve Basic (Level 1) maturity across all model elements	Achieve Intermediate (Level 2) maturity across all model elements	Achieve Advanced (Level 3) maturity across all model elements

The Hidden Challenge of M-26-14: Asset Visibility

While M-26-14 focuses on logging, monitoring, threat hunting, and forensic capabilities, agencies face a more fundamental challenge that underpins every objective in the memorandum: visibility.

CEM and THIRF are only as effective as the data available to support them. Agencies cannot monitor, investigate, or respond to activity on systems they do not know exist.

Many organizations assume their SIEM or log management platform provides complete visibility into their environment. In reality, these platforms can only analyze data from sys- tems already configured to send telemetry. They cannot identify assets that are entirely absent from the logging ecosystem.

As a result, agencies often have blind spots. Critical servers, cloud workloads, endpoints, operational technology (OT), Internet of Things (IoT) devices, and other assets may exist outside of monitoring programs without security teams realizing it.

This creates a fundamental challenge for M-26-14 compliance. Agencies cannot vali- date logging coverage without first validating inventory coverage, a move towards modern cybersecurity asset management is required.

Axonius

How Axonius Helps Agencies Meet M-26-14 Objectives

Fortunately, M-26-14 does not require a complete overhaul of existing logging and security operations investments. Agencies already possess much of the technology necessary to achieve the CEM and THIRF objectives. The challenge is ensuring those technologies have complete, accurate, and actionable data.

This is where Axonius comes in.

Axonius provides a comprehensive asset inventory by aggregating data from hundreds of security, IT, cloud, identity, and operational systems. By establishing a complete inventory across traditional IT assets, cloud resources, OT, and IoT environments, agencies gain the visibility necessary to determine where logging exists, where it does not, and where gaps must be addressed to satisfy CEM and THIRF requirements.

For existing customers	For new customers
The combination of Axonius and their current logging and SIEM platforms—whether Splunk, Elastic, or another solution—provides the foundation needed to address the objectives outlined in M-26-14.	Axonius enhances the tools agencies already own by providing the visibility, context, and automation needed to maximize the effectiveness of those investments.

Ensuring Complete Log Coverage

One of the most significant challenges agencies face is iden-tifying systems that are not sending logs to their SIEM or log management platform.

Through integrations with Splunk and Elastic, Axonius continuously compares known assets against logging sources to identify coverage gaps. Agencies can quickly determine:

- Which critical assets are not generating logs.
- Which assets are generating incomplete telemetry.
- Which newly discovered assets have not been onboarded into logging workflows.
- Which high-value systems are not being monitored consistently.

This allows security teams to move beyond assumptions and establish measurable, defensible logging coverage aligned with M-26-14 requirements.

With more than 1,500 adapters, Axonius serves as the connective layer between security and IT systems, helping agencies maximize the effectiveness of existing tools rather than introducing additional complexity.

The result is better data quality, more actionable alerts, stronger investigations, and improved operational efficiency across the security stack.

Axonius

Quantifiable Metrics for *Compliance and Executive Reporting*

Many agencies have invested significant time and resources building custom processes and homegrown reporting capabilities. Yet despite these efforts, organizations often struggle to understand their actual coverage gaps until they undergo assessments or reviews.

Axonius provides quantifiable metrics and executive-level reporting that allow agencies to continuously measure progress against M-26-14 objectives. Security and leadership teams can quickly answer critical questions such as:

- What percentage of agency assets are covered by logging?
- Which systems are missing required telemetry?
- Which asset classes present the highest risk due to visibility gaps?
- How is logging maturity improving over time?

These insights enable agencies to demonstrate measurable progress toward the maturity requirements established in M-26-14 while supporting planning, budgeting, and risk management decisions.

Supporting Continuous Monitoring and Threat Response

The ultimate goal of M-26-14 is not simply collecting more logs, it is enabling agencies to make faster, more informed security decisions.

By combining complete asset visibility with existing SIEM and log management platforms, Axonius helps agencies ensure that security alerts a e generated from the right systems, investigations have the necessary context, and threat hunters have access to the information required to identify suspicious activity.

When agencies know what assets exist, where logs are being collected, and where coverage gaps remain, they can significantly improve their ability to achieve both CEM and THIRF objectives.

Axonius

Accelerating Compliance While Reducing Operational Burden

As agencies work toward the maturity milestones established by M-26-14, maintaining visibility and logging coverage manually becomes increasingly difficult.

Axonius automates asset discovery, coverage validation, gap identification, reporting, and remediation workflows, making compliance easier to achieve and easier to sustain over time.

Rather than requiring agencies to build new processes from scratch, Axonius helps organizations continuously validate that the systems they own are the systems they are monitoring. This reduces operational overhead, strengthens security outcomes, and provides a practical, scalable path toward meeting M-26-14 requirements while maximizing the value of existing security investments.

For federal civilian agencies,

Axonius may also be available through the Continuous Diagnostics and Mitigation (CDM) Program, providing an opportunity to strengthen asset visibility and logging effectiveness while leveraging existing government funding mechanisms.

Learn more at

www.axonius.com/federal-systems or Request a demo

Axonius Federal Systems — Continuous Visibility for Superior Security.