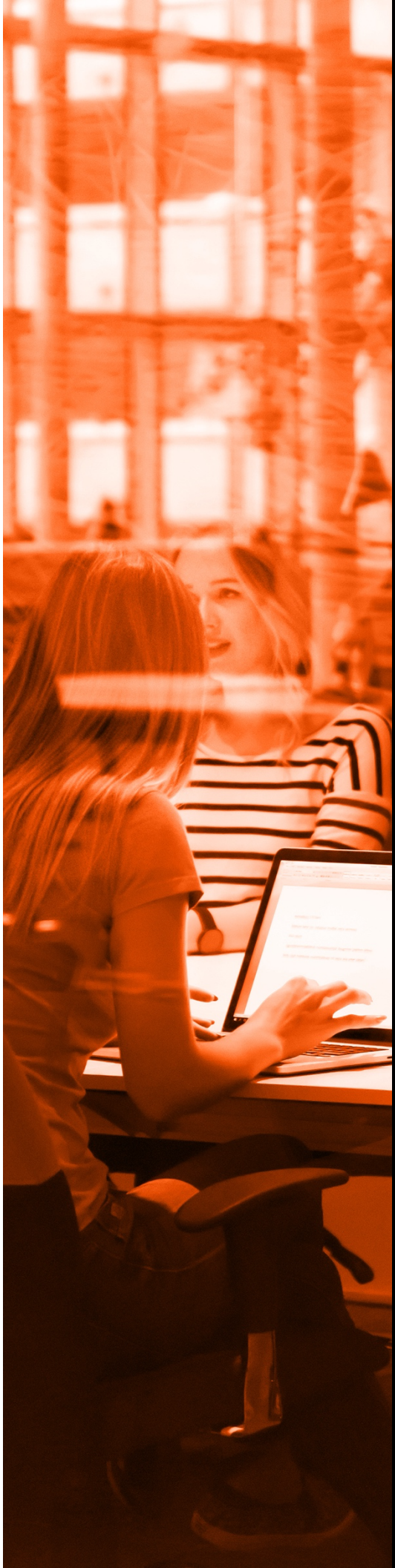
AXONIUS
FEDERAL SYSTEMS LLC

M-21-31 compliance: meeting the federal mandate for logging.

How Axonius helps agencies comply with Section 8 of Executive Order 14028.



THE CHALLENGE: TACKLING M-21-31 OF EXECUTIVE ORDER 14028

Executive Order 14028, *Improving the Nation's Cybersecurity*, directs decisive action to improve the Federal Government's investigative and remediation capabilities. Section 8 of the Executive Order, also known as M-21-32, is a clear directive for Federal agencies ("agencies") to advance logging capabilities, including log retention and management, *"with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency."*

WHAT MUST AGENCIES DO?

Agencies are mandated to address the availability and accuracy of their logs, including:

- Identifying all deployed log management technology (e.g., Splunk)
- Visibility into gaps in log coverage (e.g., missing sensors, malfunctioning sensors, API misconfigurations that prevent accurate reporting)
- Assurance that (known) log management tools are deployed correctly and are free from misconfigurations, overly permissive administrative access, and system vulnerabilities

Further, agencies must acquire and maintain comprehensive and ongoing knowledge of all assets (devices, users, networks) to properly manage them and ensure an audit trail of their security state as a means to "*accelerate incident response efforts and to enable more effective defense of Federal information and executive breach department and agencies*."

HOW CAN M-21-31 BE ACHIEVED?

Axonius Cybersecurity Asset Management: Allowing agencies to meet requirements

The Axonius Cybersecurity Asset Management (CAM) platform allows agencies to meet logging requirements defined in M-21-31. Axonius:

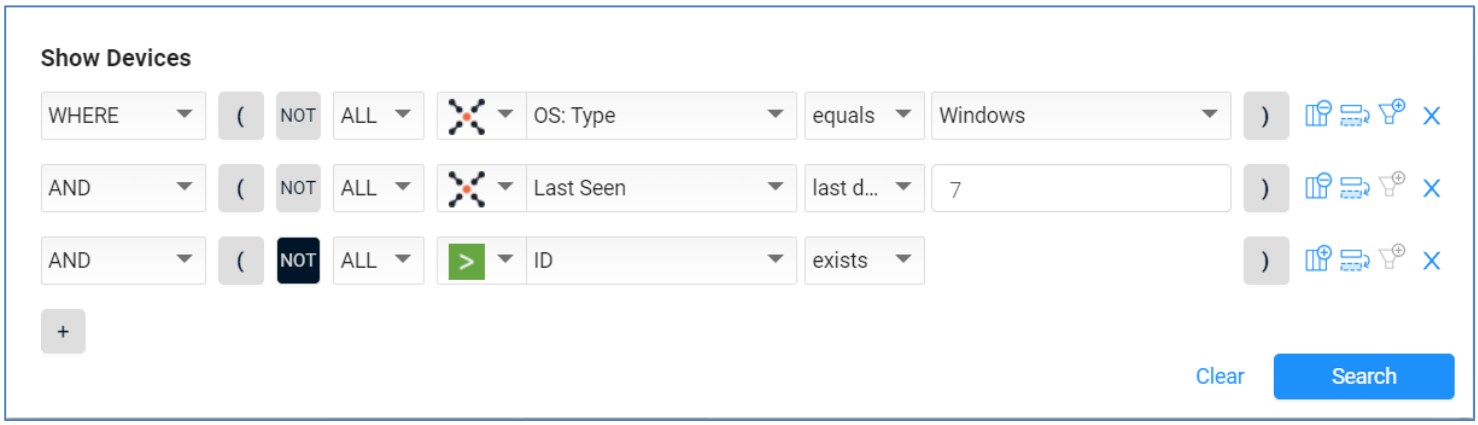
1. Assures agencies have full accounting of ALL enterprise assets including log sensors.
2. Assures continuous verification that all logging tools and sensors are in deployed, deployed correctly, and are functioning properly.
3. Provides historical auditing of the daily state of all logs, associated sensors, and users' interactions with the tools. Reporting is available on a 24x7x365 basis and can be achieved

in-platform, via log management tooling, or via an export (e.g., downloadable CSV, JSON, Axonius API, etc.).

4. Provides notification capability for when an asset or a sensor falls out of operational or security policy (e.g., gap of installation, loss of connection, failure of functionality).
5. Provides an operational platform for initiating and facilitating incident response actions.

Axonius is uniquely positioned to provide agencies with:

- **A complete asset inventory**: Ensures that agencies have a complete understanding of their IT/security ecosystem (on-prem, cloud, virtual), with visibility into every tool deployed and every user accessing systems.
- **Asset data consolidation and analysis**: Axonius aggregates, correlates, normalizes, and deduplicates asset data from every IT/security tool deployed in agencies' ecosystems, including those from log management tools. The data are provided in a consolidated dashboard so that administrators have a centralized view of their environment, leading to greater accuracy, collaboration, reporting, and ongoing cybersecurity management.
- **Accurate security gap assessments**: Identifies when tools, systems, and users (including those related to log management) are misconfigured or do not conform to policies. This gives agencies the ability to quickly detect and investigate potential security problems before they turn into incidents.
- **Remediation capabilities**: Allows agencies to remediate cyber threats by providing in-system and push system enforcement actions such as alerting, tagging, ticket creation, patch management, etc.



Screenshot of Axonius Cybersecurity Asset Management Query Surfacing all Windows Devices where Splunk Log Data Does Not Exist in the Customer Environment.

WHY AXONIUS FOR M-21-31

Axonius **enhances your log management capabilities**, tying together every asset in your agency's environment and providing a view into what's there AND what's missing—a fundamental capability that will help agencies comply with M-21-31. Unlike a standalone technology or technology with limited integration:

- Axonius can identify every location your agency is NOT logging.
- Axonius will find all agency assets missing log coverage.
- Axonius reveals inconsistencies of tool coverage and tool functionality.

Axonius gives you the assurance that your log coverage is **complete** and **actionable**. The platform provides log data **correlation** and **centralized visibility** into assets and their operational state.

But Axonius goes beyond basic: Uniquely, Axonius **detects** and **reports** on security gaps—where logs are missing or incomplete, and when sensors are misconfigured or malfunctioning.

In short, Axonius tells you what other tools can't find and provides a consolidated view of your entire asset environment for the highest level of security preparedness and defense.