Business Software Alliance

Static Logs in a Dynamic World Leave US Agencies Vulnerable

Using Continuous, Standardized, Backed Up, and Integrated Logging to Improve Cybersecurity

In 2021, Office of Management and Budget (OMB) issued Memorandum 21-31 (M-21-31), a critical step in strengthening US Government agencies' cybersecurity by establishing baseline requirements for event logging, retention, and data management. These baselines improved agencies' ability to detect and respond to cyber threats.

But the technology landscape has evolved significantly since 2021 and to keep pace with evolving threats, OMB must modernize M-21-31 by moving beyond static audits to audits that are continuous, standardized, backed up, and integrated across environments.

This modernization would transform logging from a compliance exercise to a strategic capability that enables better cybersecurity.

Technology Has Evolved

Since 2021, the technology landscape has changed. Agencies have accelerated their move to the cloud, implemented zero-trust architectures, and begun adopting artificial intelligence (AI)—which cyber defenders are leveraging today. On the horizon, we can see agentic AI reshaping how systems operate and interact.

The same technologies that are changing the technology landscape are advancing how organizations can log, retain, analyze, and use data. Modern tools like scalable cloud storage and machine learning analytics now make it possible to collect, analyze, and act on security data continuously and automatically.

M-21-31 Has Not Evolved With Technology

Malicious actors have embraced new capabilities to enhance their attacks. Agencies working under M-21-31's static approach no longer achieve the cybersecurity risk management outcomes they once enjoyed. Point-in-time compliance doesn't reflect real-time risk, intermittent logging leaves blind spots, and siloed logs make detection and response slower and less effective.

In short, M-21-31's static model no longer matches the dynamic environment it was meant to secure, even though the technologies now exist to make its goals achievable.

By updating M-21-31, OMB can ensure agencies are prepared to defend against dynamic threats and turn logging from a compliance obligation into a cybersecurity advantage.

Modern Logs Deliver Modern Cybersecurity

Today's threats, including malicious actors backed by adversarial nations, are evolving rapidly. Modern logging enables real-time visibility to detect and respond to threats as they occur; automated compliance through consistent, structured data; interoperability across systems, vendors, and environments; stronger execution of zero trust principles through adaptive, data-driven access controls; and resilience with reliable, recoverable log backups.

To keep pace with today's threats, OMB should update its logging guidance to ensure agencies' logs are continuous, standardized, backed up, and integrated across environments.

- Continuous logs provide real-time visibility into system activity, allowing agencies to detect and respond to threats as they happen, not after the fact.
- Standardized logs, built on internationally recognized standards, use consistent, structured formats that make it possible to automate compliance, correlate data across systems, and enable shared situational awareness.
- Backed-up, resilient logs ensure that critical data remains protected and recoverable even in the event of system compromise, tampering, or ransomware.
- Integrated logs connect data across environments, from endpoint to cloud, so security tools can work together, strengthening detection, prevention, and response.

By updating M-21-31, OMB can ensure agencies are prepared to defend against dynamic threats and turn logging from a compliance obligation into a cybersecurity advantage.

Modernizing Logging Is a Strategic Imperative

Technology and cyber threats have evolved faster than OMB policy has adapted. By updating M-21-31 to reflect modern logging capabilities, OMB can set agencies up for success and deliver better cybersecurity.