



TECHNICAL BRIEF · BASED ON GAO-24-105658 · VA, HHS, DHS, GSA

EVENT LOGGING: ONE OPEN RECOMMENDATION, FOUR DEPARTMENTS

17 of 23

CFO ACT AGENCIES AT THE LOWEST EVENT LOGGING TIER, EL0, AS OF AUGUST 2023

GAO told VA, HHS, DHS, and GSA to fully implement federal event logging requirements, and none had closed the recommendation as of GAO's last updates. OMB has since replaced the rules, and the new logging plans are due November 18, 2026.

THE FINDING

In December 2023, GAO reported on how the 23 civilian CFO Act agencies were meeting federal incident response requirements. The report, [Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements](#) (GAO-24-105658), measured each agency against the event logging tiers in OMB's 2021 memo M-21-31.

The results were lopsided. As of August 2023, the month agencies were due to reach the top tier, three of the 23 agencies were at tier 3. Of the remaining 20, three were at the basic tier 1 level and 17 were at tier 0, which the memo defines as not effective.

GAO made 20 recommendations to 19 agencies, chiefly to fully implement event logging requirements as directed by OMB guidance. VA, HHS, DHS, and GSA each received one. In its June 2025 status notes, GAO said none of the four had provided sufficient evidence to close it, and the same recommendation appears again in the [VA CIO open recommendations letter](#) of January 2026.

WHY IT KEEPS HAPPENING

Agencies gave GAO three obstacles: a lack of staff, event logging technical challenges, and limits on cyber threat information sharing. None of them is quick to fix inside one budget year.

The old rules also made the target expensive. M-21-31 required agencies to keep logs at every criticality level for 12 months in active storage and another 18 months in cold storage. For a department with hundreds of systems, that is a large ingest and storage bill sized before anyone decided which logs mattered most.

Then the target moved. On May 22, 2026, OMB issued [M-26-14](#), a non-GAO directive that rescinds M-21-31 effective immediately.

The EL0 to EL3 tiers are gone. In their place is a five-level maturity model scored across five elements: inventory visibility, collection coverage, collection operations, data retention, and log management. Retention now follows two objectives instead of one rule: logs must stay searchable for six months to support continuous event monitoring and retrievable for a year to support threat hunting, investigation, response, and forensics.

GAO's status notes for these four departments predate the new memo. The underlying gap does not. Our [roadmap for logging under M-26-14](#) covers the memo's requirements for CISOs and ISSMs in more depth.

WHY IT MATTERS TO YOUR BID

M-26-14 starts new clocks, and they run through the next round of task orders. CISA published its Logging Reference Architecture in August 2026, and agencies must submit an [Agency Logging Plan to OMB and CISA by November 18](#). From the architecture's release, the memo gives agencies 120 days to reach at least Level 1 across all five elements, 180 days for Level 2, and 320 days for Level 3.

That puts logging next to almost any operations, cloud hosting, or monitoring buy at VA, HHS, DHS, or GSA, because every workload a contractor runs produces log sources the department has to inventory, collect, and retain. Evaluators know the open list. A generic O&M approach reads as a gap. A technical volume that explains how the work will onboard sources, meet the six-month searchable baseline, and hand the CISO maturity evidence reads as understanding of the requirement.

Transition plans are the other pressure point. Cloud migrations often finish without monitoring parity, and the operations team that understood the data center may not see the new environment at all. A prime that brings a defined method for that gap has something specific to put in front of the board.

TECHNICAL APPROACH

The method below comes from Avalon's [Enterprise Monitoring service](#). It describes how the work is done, at the methodology level.

- 1. Inventory the tools and what they actually see.** List every monitoring and logging tool in the environment, licensed, deployed, or sitting on the shelf, and map real telemetry coverage against the authoritative asset inventory. If the department has no current asset inventory, that becomes the first finding. This step produces the evidence for the inventory visibility and collection coverage elements.
- 2. Baseline against M-26-14, not the old tiers.** Measure collection, retention, and searchability against the new baseline and score each of the five maturity elements. Where the department documented an EL-tier posture under M-21-31, crosswalk it so earlier work carries forward instead of starting over.
- 3. Design retention around the two objectives.** Build the target architecture: which platforms stay and which retire, the agent and collector strategy, a measured ingest baseline with a growth model, and hot and cold tiers sized to the six-month searchable and one-year retrievable split. A retention cost table goes with the design, because over-retention sized to the old rule is often where the money is.
- 4. Onboard by source matrix, pilot first.** Agree a locked log-source onboarding matrix, deploy to a pilot enclave, then roll out in phases through the change board, with the ISSO approving agents and collectors inside the authorization boundary.
- 5. Hand over the evidence.** Deliver a retention compliance map, a maturity gap matrix, and NIST SP 800-53 AU, CA-7, and SI-4 implementation notes written so the system owner can reuse them in the SSP.

The department's logging plan submission and maturity self-reporting stay with its CISO. Analyzing the logs for threats, and investigating a suspected compromise, are separate security work. This work builds capability and evidence; it does not certify compliance.

WHAT "FIXED" LOOKS LIKE

GAO has not yet published closure evidence for any of these four recommendations, so the measures below are targets, taken from the current memo:

- An Agency Logging Plan submitted to OMB and CISA by November 18, 2026.
- At least Level 1 across inventory visibility, collection coverage, collection operations, data retention, and log management within 120 days of the architecture's release, then Level 2 and Level 3 on the memo's schedule.
- Logs searchable for six months and retrievable for a year, with the coverage map showing which sources meet that bar.

Whether GAO will close its recommendation against the new memo, or ask for something more, is GAO's call.

STATUS CHECK

OPEN The recommendation was open at all four departments as of GAO's June 2025 status update.

DEPARTMENT	WHERE GAO LISTS IT	STATUS	AS OF
VA	GAO-24-105658; VA CIO letter GAO-26-108706	Open	January 2026
HHS	GAO-24-105658	Open	June 2025
DHS	GAO-24-105658; DHS CIO letter GAO-25-108460	Open	July 2025
GSA	GAO-24-105658; GSA CIO letter GAO-25-108537	Open	July 2025

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Log-source inventory, M-26-14 maturity gap analysis, and retention architecture under the prime's IT operations or monitoring task order
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151S IT Professional Services); GSA Alliant 3; VA T4NG2

If operations, cloud, or monitoring work at VA, HHS, DHS, or GSA is in your capture plan, Avalon teams as the sub that inventories the log sources, scores them against M-26-14, and designs the retention architecture behind the department's logging plan.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.