



TECHNICAL BRIEF · BASED ON GAO-24-106343 · OMB, GOVERNMENT-WIDE

OMB HAS NOT SHOWN GAO HOW IT COORDINATED EDR RESOURCING

4 of 5

GAO-24-106343 RECOMMENDATIONS OPEN IN GAO'S STATUS NOTES THROUGH NOVEMBER 2024, INCLUDING ALL THREE TO OMB

GAO told OMB to show it coordinated with agencies on resourcing for endpoint detection and response. As of GAO's November 2024 status notes, OMB had provided no documentation, and the recommendation is open.

THE FINDING

In April 2024, GAO published [Cybersecurity: Implementation of Executive Order Requirements is Essential to Address Key Actions](#) (GAO-24-106343). Executive Order 14028 contains 115 provisions, and GAO assessed the 55 leadership and oversight requirements assigned to CISA, NIST, and OMB. As of March 2024, those agencies had fully completed 49, partially completed five, and found one not applicable.

That count measures what the leadership agencies did. It does not measure whether agencies deployed endpoint detection and response (EDR) across their fleets.

GAO made five recommendations, three to OMB. One asks OMB to demonstrate that it coordinated with pertinent agencies on resourcing needs for implementing an EDR capability. GAO's status note says OMB neither agreed nor disagreed with the recommendation and had not provided documentation of actions to address it. The same notes show the other two OMB recommendations open.

WHY IT KEEPS HAPPENING

GAO's notes show a recommendation without a response, so the reasons are not in the record. The structure of the underlying directive is.

OMB [M-22-01](#), a non-GAO memo issued October 8, 2021, split the work. CISA runs a central EDR initiative. Each agency, in turn, analyzes its own EDR gaps with CISA, gives CISA access to its EDR tools for threat hunting, and works with its CFO and the OMB Resource Management Office to fund the tool for its lifespan, including updates and licensing. The memo excludes DoW (formerly DoD) and the intelligence community.

Resourcing therefore sits between an agency budget office and OMB, and GAO's recommendation asks OMB to show the OMB half. Nothing in the status notes says OMB has.

The pattern repeats. OMB's two other open recommendations also concern resourcing: cost analyses for threat-information sharing, and resourcing for logging, log retention, and log management. [B02](#) covers the logging side, so this brief stays on EDR.

WHY IT MATTERS TO YOUR BID

An unanswered government-wide question about who pays for EDR lands in the task orders that operate it. SOC support, endpoint security, and O&M recompetes each carry assumptions about coverage, licensing, and staffing that nobody upstream has confirmed for the agency.

Evaluators who read this report can test an offeror on three points. The technical volume should state a coverage figure against an authoritative inventory, not only the number of licenses owned. Price volumes should say who provides agent licenses and console access, and what happens to the schedule if the agency does not. Management volumes should show how a detection-testing result reaches the CIO's budget office in a form it can fund.

Recompetes add a transition problem, because an incoming team inherits the incumbent's EDR deployment as it stands. A transition plan that measures that baseline in the first weeks gives the contracting officer a number to hold the new contract against, instead of the vendor dashboard's.

GAO's report sets no evaluation criteria. These are the places where an unresolved funding question can surface in questions and risk ratings.

TECHNICAL APPROACH

The method below comes from Avalon's [Endpoint Detection & Response service](#). It describes how the work is done on the EDR platform an agency already licenses, at the methodology level, inside the agency's console under a signed statement of work.

1. **Reconcile the inventory to the console.** Compare the authoritative endpoint inventory (Active Directory, CDM asset data, the CMDB) against what the EDR console reports. The output is a coverage percentage and a named gap list by endpoint class: workstations, member servers, domain controllers, Linux, macOS, VDI, and cloud workloads. This is the "widest number of endpoints" test M-22-01 sets.
2. **Audit agent health and policy.** Find stale check-ins, broken sensors, version drift, and agents installed but left in passive or audit mode. Review prevention and detection policy against vendor baselines and CIS Benchmarks, and list every exclusion and allowlist entry with its justification or the lack of one.
3. **Test detection with safe emulation.** Run Atomic Red Team or MITRE Caldera test cases mapped to MITRE ATT&CK techniques on agency-provided test devices. Record what fired, what was blocked, what was missed, and how long detection took, and deliver the result as an ATT&CK Navigator layer.
4. **Confirm what the agency reports.** Check that the reporting feeds for CDM dashboards and FISMA CIO metrics match the as-built deployment, and that CISA access arrangements under M-22-01 reflect it. Map the evidence to SI-3, SI-4, and IR-4 for the SSP.
5. **Cost the gaps.** Write a prioritized, costed remediation roadmap, one gap-register row per gap with endpoint class, cause, and fix. Report four numbers at the start: coverage against inventory, agent health, median time to detect in controlled testing, and false-positive rate.

The roadmap is what a component brings to its own CFO conversation. It does not substitute for OMB's coordination, and nothing here closes GAO's recommendation.

WHAT "FIXED" LOOKS LIKE

For GAO, the recommendation closes when OMB provides documentation that it coordinated with pertinent agencies on EDR resourcing needs. That is OMB's evidence to produce, and GAO's status note says to expect an update once it verifies action.

At the agency or component level, the targets are measurable. Coverage against the authoritative inventory is a number the CISO will sign. Every endpoint class outside coverage has a documented reason or a funded plan, and agents in passive mode are counted with a dated path to blocking. A repeat of the ATT&CK-mapped test shows whether detection held after fixes.

Results depend on agency decisions and change-board timing, so these are targets, not promises.

STATUS CHECK

OPEN Open as of GAO's status notes, last dated November 2024. Four of the five recommendations are open: all three to OMB and one to DHS on the Cyber Safety Review Board. The DHS recommendation on critical software categories is closed as implemented. The 49-of-55 figure dates from March 2024 and describes leadership agencies, not agency adoption.

TEAMING FIT

NAICS	541519, 541512
AVALON'S SUB ROLE	Inventory-to-console coverage reconciliation, agent-health and policy audit, ATT&CK-mapped detection test, and a costed remediation roadmap under the prime's endpoint security or SOC support task
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151HACS Highly Adaptive Cybersecurity Services); GSA MAS (SIN 54151S IT Professional Services); GSA OASIS+

If an agency's endpoint security, SOC support, or EDR recompile is in your capture plan, Avalon teams as the sub that measures coverage against the inventory, tests what the platform catches, and hands the prime a costed gap register.

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.