



TECHNICAL BRIEF · BASED ON GAO-25-108211 · DOW

GAO WANTS DOW TO CHECK WHAT LEADERS KNOW BEFORE RISK DECISIONS

2 reports

RECURRING REPORTS THAT KEPT DOW SENIOR LEADERS UPDATED ON ONE CYBER HYGIENE PLAN WHEN GAO REVIEWED IT, WITH NOTHING REGULAR ON THE OTHER INITIATIVES OR ON PRACTICES

GAO told DoW (formerly DoD) to assess whether senior leaders have complete information for cyber risk decisions and to revise its recurring reports. The recommendation is open, and DoW's scorecard still omitted two topics in its April 2024 version.

THE FINDING

GAO's May 2025 letter, [Chief Information Officer Open Recommendations: Department of Defense](#) (GAO-25-108211), lists 54 open recommendations to DoW (formerly DoD), seven of them aimed at component-level CIOs. One asks DoW to find out whether its senior leaders have enough cybersecurity information to make risk-based decisions.

The recommendation comes from [Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene](#) (GAO-20-241, April 2020). GAO found that two recurring reports kept senior leaders updated on the Cyber Discipline Implementation Plan. Leaders did not regularly receive information on the other cyber hygiene initiatives, or on whether hygiene practices were actually in place.

Recommendation 7 told the Secretary of Defense to ensure the DoW CIO assesses the extent to which senior leaders have more complete information to make risk-based decisions, and then revises the recurring reports or develops a new one.

WHY IT KEEPS HAPPENING

The reporting followed the plan, not the risk. GAO reviewed three cyber hygiene initiatives: the 2015 Cybersecurity Culture and Compliance Initiative, the 2015 Cyber Discipline Implementation Plan, and the Cyber Awareness Challenge training. Only the Cyber Discipline plan had recurring reports behind it.

The data gap sat further down. GAO found some components could not say how many users had finished Cyber Awareness training or how many had lost network access for skipping it. DoW had identified the adversary

techniques it sees most often and the practices that counter them, but it did not know how widely those practices were applied, partly because no component monitored them.

DoW later folded its reporting requirements into the Cybersecurity Hardening Scorecard, which tracks tiered and prioritized initiatives for cyber maintenance and operations. GAO's status note says DoW has taken some action.

The note also says the April 2024 version left out two things: the cybersecurity practices in DoW's hygiene initiatives, and the hygiene practices that protect networks from key cyberattack techniques. GAO's 2020 findings point to the same two gaps at the source. A scorecard cannot report what nobody measures.

WHY IT MATTERS TO YOUR BID

The recommendation goes to the DoW CIO, not to contractors, and it creates no contract clause. It still shapes what evaluators want to see. Cybersecurity operations, continuous monitoring, and RMF support task orders at DoW components all end in a report that someone above the program office reads, and GAO has told the department that its own version of that report was incomplete.

An offeror that treats reporting as a dashboard screenshot invites the same gap. A technical volume that names each measure, its data source, how often it refreshes, and who acts on it reads as understanding of the requirement. Two weak patterns stand out to an evaluator: measures built on tool counts instead of on whether a practice is in place, and a report with no stated reader and no escalation path.

Recompetes add a transition angle. An incoming contractor inherits the incumbent's data feeds and definitions. If those were never documented, the first months go to finding out what the numbers meant.

TECHNICAL APPROACH

The method below comes from Avalon's [NIST RMF Implementation service](#), with coverage mapping and dashboard work from its Enterprise Monitoring service. It is scoped at the assessment and design level, one component at a time, for unclassified environments. It supports the CIO's assessment; it does not perform it.

1. **Trace the reports to their sources.** Collect every recurring report and scorecard that reaches senior leaders, interview the ISSM, ISSO, and operations staff who produce them, and map each field to its source system and owner. Mark which fields speak to the two topics GAO named. The output is a report-to-source map and a gap list.
2. **Map coverage against the authoritative asset inventory.** For each practice a leader should see, record which assets and enclaves feed it and where telemetry is silent. Silent gaps become findings, because a measure that covers only part of the enterprise should say how much.
3. **Write the monitoring metrics under NIST SP 800-137.** For each practice, name the NIST SP 800-53 Rev. 5 control it evidences (CA-7, SI-4, RA-5, or CM-6 as applicable), the metric, the monitoring frequency, the data feed, the owner, and the reporting cadence to the Authorizing Official. Where a practice is a hardening setting, tie the metric to the DISA STIG or CIS benchmark check that tests it, so the figure comes from configuration scans and not from a survey.
4. **Build the leadership view.** Construct dashboards for defined audiences (system owners, operations, executives) from the feeds, with alert thresholds, owners, and escalation paths. Each executive measure shows its coverage figure from step 2 beside the result.
5. **Record it and hand it over.** Structure the results in the governance platform of record (eMASS for DoW), write runbooks for refreshing each feed, and train the agency staff who will run it. The transition tapers Avalon's involvement.

Avalon designs the metrics and builds the reporting. It does not make the CIO's assessment, decide what leaders do with the data, assess controls, or make or promise an authorization decision, which stays with the Authorizing Official.

WHAT "FIXED" LOOKS LIKE

GAO has not published closure evidence for this recommendation. Its status note describes the bar: the CIO assesses the extent to which senior leaders have information on the two missing topics, then revises the recurring reports or develops a new one.

Practical targets, written as targets:

- A documented CIO assessment that names the decisions leaders make and the information each needs.
- A scorecard version that carries both topics: practices from the hygiene initiatives, and practices against key attack techniques.
- Each measure traceable to a named data feed and owner, with its coverage stated beside it.

STATUS CHECK

OPEN GAO's product page for GAO-20-241 shows recommendation 7 as open and partially addressed, and its latest dated reference is the April 2024 scorecard version. No separate update date appears. The May 2025 CIO letter, GAO-25-108211, still lists the recommendation among DoW's open items.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Report-to-source inventory, telemetry coverage map, continuous monitoring metrics and reporting cadence, and a leadership view built from the feeds, under the prime's cybersecurity operations or RMF support task order, in unclassified environments
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 cybersecurity operations, continuous monitoring, or RMF support at a DoW component is in your capture plan, Avalon teams as the sub that maps what leadership reports are built from, writes the metrics behind them, and builds the view leaders read.

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.