



TECHNICAL BRIEF · BASED ON GAO-19-384 · CIVILIAN AGENCIES, VA, HHS, GSA, SBA, DOT

HOW AGENCIES CLOSED 55 OF 58 GAO CYBER RISK RECOMMENDATIONS

55 of 58

GAO-19-384 CYBERSECURITY RISK MANAGEMENT RECOMMENDATIONS CLOSED AS IMPLEMENTED

In 2019, GAO found 11 civilian agencies had no full process for assessing cyber risk across the whole agency. All 11 have since closed that recommendation, the last in April 2026, and GAO's notes show exactly what it accepted: aggregated system-level risk, scored and reported to leadership.

THE FINDING

In July 2019, GAO reviewed cybersecurity risk management at 23 civilian agencies in [Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges](#) (GAO-19-384). DoW (formerly DoD) was not part of the review. GAO made 58 recommendations: 57 to the agencies and one to OMB.

One of the gaps was basic. Eleven agencies had not fully established a process for assessing agency-wide cybersecurity risk based on an aggregation of system-level risks. Each received the same recommendation: establish a process for conducting an organization-wide cybersecurity risk assessment.

Seven years on, all 11 are closed. EPA closed the last one in April 2026. Across the whole report, 55 of the 58 recommendations are closed as implemented, and GAO's status notes record what each agency showed to close them.

WHY IT KEEPS HAPPENING

Risk at an agency is measured one system at a time. Each system has its own authorization, its own POA&M, and its own scan results, often kept by a different contractor. An agency-wide view needs those records gathered, scored the same way, and reported upward, and that only works if the system-level data is current.

Speed varied widely. NRC and USAID closed the recommendation in December 2019. VA closed it in March 2022, OPM in June 2024, and EPA in April 2026.

Two of the three open recommendations show where it stalls. DOT agreed to update its policies to require an organization-wide risk assessment but, as of March 2024, had not provided them or a completion date. DOT's risk

management strategy recommendation is also open; in February 2025, DOT told GAO it was assessing needs and resources. The third, to OMB, asked for a way to share successful approaches across agencies, and GAO had received no information on it as of March 2024.

WHY IT MATTERS TO YOUR BID

GAO's closure notes show what an agency-wide risk process runs on: system-level indicators, vulnerability scan results, and risk data collected from bureaus and offices. Contractors produce most of that data. A prime running O&M or cyber support on a set of systems is maintaining the records the CISO's dashboard reads.

Evaluators who know this report will look for that connection in the technical volume. A response that treats POA&M upkeep and monitoring as paperwork misses it. One that explains how the contract's systems will report risk in a consistent, scoreable form, on a set cadence, shows understanding of how the agency manages risk above the system level.

It also matters at transition. An incoming contractor inherits stale POA&Ms and authorization records, and those feed the agency's enterprise numbers from day one. Cleaning them up early protects the agency's risk picture and the new contractor's reputation.

TECHNICAL APPROACH

The method below comes from Avalon's [NIST RMF Integration service](#) and its POA&M service. It works at the system and program level, producing the data an agency-wide assessment aggregates. It describes how the work is done, at the methodology level.

- 1. Assess the authorization posture.** For each system in scope, inventory package age, ATO status and expiration, governance record health in CSAM, eMASS, or Xacta, evidence currency, open POA&M items, and prior findings. The output shows which systems can report reliable risk data today.
- 2. Baseline and rationalize the POA&M ledger.** Measure counts, aging, data-quality defects, and duplicate rate, then dedupe, re-score severity against CVSS, the CISA KEV catalog, and agency risk criteria, and re-baseline milestones against real resources. Flag items that belong in a formal risk acceptance decision instead of slipping indefinitely.
- 3. Rank the risk the same way every time.** Build a risk-ranked remediation priority matrix sortable by severity, KEV status, effort, and ATO impact, so every system in the portfolio reports on one scale.
- 4. Design the monitoring feed.** Write the continuous monitoring strategy under NIST SP 800-137: frequency per control, the metric that shows it is working, the data feed behind it, and the reporting cadence to the authorizing official.
- 5. Hand over the cadence.** Leave a POA&M management SOP, a cadence calendar, and a monthly status brief in CIO-metric language the government team keeps running.

The agency-wide risk assessment, and every decision to accept risk, stays with the agency. Avalon drafts risk acceptance memos for the government to decide on, and it does not assess controls it implemented.

WHAT "FIXED" LOOKS LIKE

GAO accepted different tools that do the same thing:

AGENCY	CLOSURE EVIDENCE GAO ACCEPTED	DATE
Treasury	A consolidated enterprise risk register and a system that aggregates, scores, ranks, and prioritizes risks	March 2021
HHS	A methodology that collects cyber risk data across the department and scores it	January 2022
VA	A quantitative enterprise risk analysis, architecture reviews, and enterprise scan results fed into department reporting	March 2022
SBA	Risks aggregated from internal and external sources, scored, and reported to leadership with remediation actions	January 2021
GSA	System-level risks aggregated and reported to officials, including the Administrator	October 2020
NASA	An agency-wide scorecard of key cyber risk indicators	February 2022
EPA	A risk dashboard whose source data staff validate monthly	April 2026

The common thread is system-level data, scored on one method, reported upward on a schedule.

STATUS CHECK

MIXED As of GAO's last updates, three recommendations remain open: OMB's (no information as of March 2024) and DOT's two (last DOT update February 2025). All 11 organization-wide risk assessment recommendations are closed.

TEAMING FIT

NAICS	541512, 541611
AVALON'S SUB ROLE	Authorization posture assessment, POA&M rationalization and risk-ranked reporting, and continuous monitoring reporting design for the systems under the prime's cyber support or O&M task order
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 civilian agency cyber support or O&M work is in your capture plan, Avalon teams as the sub that keeps your systems' POA&Ms, authorization records, and monitoring data current enough for the agency's enterprise risk picture to trust.

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.