



TECHNICAL BRIEF · BASED ON GAO-19-384 · CIVILIAN AGENCIES, STATE, SBA

8 AGENCIES HAD TO TIE POA&M PRIORITY TO RISK. ALL 8 RECS ARE CLOSED

8 of 8

GAO-19-384 POA&M PRIORITIZATION RECOMMENDATIONS CLOSED AS IMPLEMENTED

GAO told eight civilian agencies to require that risk assessments drive how they rank POA&M items. All eight recommendations are closed, and GAO's notes show the written rules it accepted, which is the standard a recompetitiveness evaluator will hold a contractor's ledger to.

THE FINDING

In July 2019, GAO reported in [Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges](#) (GAO-19-384) that 17 of the 23 civilian agencies it reviewed had not fully established agency- and system-level policies for assessing, responding to, and monitoring risk. DoW (formerly DoD) was not part of the review.

Eight of those policy recommendations had a specific ask: require that risk assessments inform how the agency prioritizes its plans of action and milestones (POA&Ms). They went to USDA, Commerce, HUD, Labor, State, NASA, NRC, and SBA. All eight are now closed as implemented.

GAO's status notes date the closures from March 2020 (HUD and SBA) to September 2025 (Labor), a spread of more than five years. The report overall has 55 of 58 recommendations closed, and none of the three still open concerns POA&Ms.

WHY IT KEEPS HAPPENING

A POA&M is the ledger of known weaknesses, and prioritization is the step where judgment enters. NIST SP 800-53 Rev. 5 control [PM-4](#) asks agencies to review their POA&Ms for consistency with the organizational risk management strategy and organization-wide priorities for risk response. An agency that has no written rule linking the two can leave each system owner to rank items alone.

The fix GAO accepted was a document. HUD updated its POA&M procedures, and SBA revised its risk management framework implementation procedures. NASA revised its IT Security Handbook, while Commerce updated its Security and Privacy Assessment and Authorization Handbook.

Commerce did not state whether it concurred; HUD, Labor, State, NASA, NRC, and SBA did. Labor provided updated policies in September 2025, six years after the report, and Commerce its handbook in February 2024. The notes describe policy text. They do not say how closely daily ranking follows it, which is where a contractor's work either matches the rule or doesn't.

WHY IT MATTERS TO YOUR BID

A recompile for A&A or ISSO support will often hand the contractor a ledger that already exists. The evaluator wants to see how you will rank what is in it, and "highest severity first" is a weak answer when the agency's own handbook says risk, not scanner score, sets the order.

Name the agency's rule in the technical volume. Show the sort keys, who signs a re-ranking, and how a ranked item connects to a milestone and a resourced owner. Evaluators who know GAO-19-384 will read that as understanding of the requirement.

Timing adds pressure. CISA's BOD 26-04, a non-GAO directive for civilian agencies, sets remediation windows of 3, 14, or 60 days from December 7, 2026, as covered in [our BOD 26-04 brief](#). Items on the Known Exploited Vulnerabilities (KEV) list can no longer wait for a quarterly re-sort.

TECHNICAL APPROACH

The method below comes from Avalon's POA&M service. It works inside the agency's own system of record and describes how the work is done, at the methodology level.

- 1. Build complete entries.** Turn findings from assessment reports, ACAS, Nessus, or Qualys scans, STIG checks, and pen tests into entries with a weakness description, source, severity, affected assets, responsible party, required resources, interim milestones, and a scheduled completion date. That is the content NIST SP 800-53 CA-5 asks the plan to document.
- 2. Rationalize the backlog.** Remove duplicates and re-score severity against CVSS, CISA KEV presence, and the agency's own risk criteria. Flag items that belong in a formal risk acceptance or deviation decision rather than a rolled date.
- 3. Rank by one rule.** Produce a risk-ranked remediation priority matrix, sortable by severity, KEV status, effort, and ATO impact. Weights come from the agency's risk management strategy, the same reference PM-4 points to.
- 4. Package closure evidence.** For each item ready to close, assemble the configuration artifact, before-and-after scan delta, change record, and sign-off in the format the agency's security control assessor expects. The assessor validates; Avalon does not.
- 5. Hand over the cadence.** Leave a POA&M management SOP, a calendar for working sessions, and a monthly one-page status brief in CIO-metric language. Draft risk acceptance memos for the authorizing official to decide.

Avalon does not accept risk, validate closure, or make authorization decisions. Technical fixes sit with the system owner or a remediation task.

WHAT "FIXED" LOOKS LIKE

GAO closed each recommendation on a written rule in a controlling document.

AGENCY	EVIDENCE GAO'S NOTES RECORD	CLOSED
HUD	Updated POA&M procedures requiring risk to inform prioritization	March 2020
SBA	Updated risk management framework implementation procedures	March 2020
NRC	Updated policies that prioritize POA&Ms on its organization-wide risk assessment	January 2021
USDA	Updated policies and procedures using risk assessments for POA&M prioritization	October 2021
NASA	Revised IT Security Handbook requiring risk in POA&M prioritization	January 2022
State	Updated documentation with risk-based POA&M prioritization	Aug–Sep 2023
Commerce	Updated Security and Privacy Assessment and Authorization Handbook	February 2024
Labor	Updated policies tying POA&M prioritization to the risk management strategy	September 2025

On a contract, the targets are Avalon's own, not GAO's: every open item carries a risk rank traceable to the rule, an aging report cut by rank, and sampled closure packages that the assessor accepts on first review.

STATUS CHECK

CLOSED Closed, 8 of 8, as of GAO's last update on these recommendations, September 2025 (Labor). Across GAO-19-384, 55 of 58 are closed as implemented, and the three open ones (OMB rec 1, DOT recs 26 and 27) are not POA&M recommendations.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	POA&M entry development, backlog rationalization, a risk-ranked priority matrix, closure evidence packages, and a POA&M management SOP with cadence, inside the agency's own eMASS, CSAM, or Xacta, under the prime's A&A or ISSO 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 a civilian agency's A&A or ISSO support recompile is in your capture plan, Avalon teams as the sub that ranks the ledger by the agency's own risk rule and leaves the government team a cadence it can run.

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.