



TECHNICAL BRIEF · BASED ON GAO-26-108443 · VA, STATE, SBA

ONLY 3 OF 8 CLOUD SYSTEMS FULLY MONITORED

3 of 8

SELECTED AGENCY CLOUD SYSTEMS WHERE GAO FOUND CONTINUOUS MONITORING FULLY PERFORMED

GAO reviewed eight agency cloud systems at State, DOT, VA, and SBA and found continuous monitoring fully performed on three. Five open recommendations ask for reviewed provider deliverables, collected audit logs, and documented tools: work that sits on the agency side of every cloud task order.

THE FINDING

On June 25, 2026, GAO published [Cybersecurity: Selected Agencies Need to Better Protect Cloud Data](#) (GAO-26-108443). It looked at two cloud systems, one PaaS and one SaaS, at each of four agencies: State, DOT, VA, and SBA.

Continuous monitoring was the weakest practice. GAO found that agencies fully performed it for three of the eight systems. It scored four activities: a monitoring plan, review of the provider's continuous monitoring deliverables, documented use of vulnerability management tools, and collection and review of audit logs.

AGENCY	REC	SYSTEM	WHAT GAO ASKED FOR
State	1	PaaS	Review the provider's continuous monitoring deliverables
VA	3	PaaS	Collect and review audit logs
VA	4	SaaS	Collect and review audit logs
SBA	8	PaaS	Implement the plan, review deliverables, document vulnerability tools, collect and review audit logs
SBA	9	SaaS	Document the use of vulnerability management tools

SBA's PaaS system carries the broadest gap. Its SaaS recommendation covers tool documentation only. DOT fully implemented all three practices GAO reviewed for both of its systems and got no recommendations.

WHY IT KEEPS HAPPENING

GAO's report gives the agencies' own explanations. Most point to ownership and follow-through rather than missing tools.

State told GAO it does not hold monthly continuous monitoring meetings with its PaaS provider. Officials said the system sat in a department continuous assessment program and promised more information, then reported that the responsible cyber teams had moved in a reorganization. VA had documented policies requiring audit log collection but gave GAO no evidence it collected or reviewed the provider's logs for either system; officials said VA was in the early stages of migrating the applications to a new monitoring system. SBA officials said they would provide a signed monitoring plan and did not.

A provider produces monitoring data on its own schedule; someone on the agency side has to read it and record that they did. When a team moves or a platform changes, that duty drops out first.

VA agreed with its five recommendations; State neither agreed nor disagreed, and SBA did not comment.

WHY IT MATTERS TO YOUR BID

Cloud hosting, migration, and O&M task orders put a contractor in the middle of this relationship. The prime often runs the workload, manages the provider account, and sits closest to the logs. An evaluator who has read GAO-26-108443 will look for whether the offeror's plan names who receives provider deliverables and where audit logs go.

In a proposal, the technical volume needs a monitoring design that covers PaaS and SaaS sources, not only the virtual machines the contractor builds. The transition plan needs to keep log collection running while a monitoring platform changes, which is the exact moment VA described. Management volumes that promise monthly reporting should say what the ISSO receives and in what form.

FedRAMP adds a December date. Under its [Vulnerability Evaluation and Reporting rules](#), a non-GAO source, certified providers must give a human-readable report at least monthly once the rules take effect on December 7, 2026. More provider reporting only helps if the agency side reads it.

TECHNICAL APPROACH

This method comes from Avalon's [Enterprise Monitoring service](#), with boundary and evidence work from Cloud Architecture & Engineering. It is described at the methodology level.

- 1. Map provider log coverage per system.** Inventory the monitoring and logging tools touching each cloud system (licensed, deployed, and shelfware) and map telemetry coverage against the asset inventory. For PaaS and SaaS, list which audit log sources the provider exposes and which ones actually reach the agency's platform. Record inherited versus agency-implemented controls so the gap is assigned, not assumed.
- 2. Onboard the missing audit logs.** Build a log source onboarding matrix for each system and route provider logs through a pipeline that normalizes, centralizes, and retains them. Set retention and searchability to the agency's logging plan under OMB M-26-14, a non-GAO memo whose scope includes systems operated by third parties on the agency's behalf. During a platform migration, onboard in phases, pilot enclave first, so no source drops at cutover.
- 3. Give provider deliverables an owner.** Treat the provider's continuous monitoring package as an inbound source; GAO's criteria include FedRAMP's continuous monitoring documentation. Each deliverable gets an

owner, a review step, and an escalation path, built as the dashboards and alert definitions the ISSO can use. The review record is the evidence GAO said State could not show.

4. **Write the monitoring plan into the SSP.** Produce NIST SP 800-53 Rev 5 implementation notes for AU-6, CA-7, and SI-4 that the ISSO can reuse, and lay out the data collection and reporting mechanics of the NIST SP 800-137 continuous monitoring program. The coverage map documents which tools run against each system, which is the gap in SBA's SaaS recommendation.

This work produces capability and evidence. It does not assess controls, author the SSP, or make an authorization decision, and analyzing security events in the collected logs is separate work.

WHAT "FIXED" LOOKS LIKE

GAO's own example is DOT. For both of its systems, DOT developed a continuous monitoring plan, reviewed the provider's deliverables, documented its use of vulnerability management tools, and collected and reviewed audit logs.

For the open recommendations, these are targets:

- Every provider audit log source for the system listed, with its onboarding status.
- A dated review record for each provider deliverable, with the reviewer named.
- A signed monitoring plan matched by SSP language for CA-7 and AU-6.

STATUS CHECK

OPEN All five continuous monitoring recommendations (State 1, VA 3 and 4, SBA 8 and 9) were open as of GAO's last update, June 2026, with no agency action confirmed yet. The report's other seven recommendations, on incident response, recovery, and service level agreements, were also open.

TEAMING FIT

NAICS	541519, 541512
AVALON'S SUB ROLE	Provider-log coverage map, log source onboarding, and a continuous monitoring evidence workflow for agency cloud systems under the prime's cloud hosting or O&M task order
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 518210C Cloud Computing and Cloud Related IT Professional Services); GSA MAS (SIN 54151S IT Professional Services); GSA Alliant 3

If VA, State, or SBA cloud hosting work is in your capture plan, Avalon teams as the sub that gets the provider's audit logs into the agency's platform and gives every monitoring deliverable an owner and a dated review record.

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.