



TECHNICAL BRIEF · BASED ON GAO-23-105482 · DHS

THE FEDRAMP AUTHORIZATION RECOMMENDATION ON DHS'S OPEN LIST

2 of 3

DHS FEDRAMP AUTHORIZATION RECOMMENDATIONS CLOSED; THE SAAS SYSTEM'S
AGENCY AUTHORIZATION IS STILL OPEN

In 2023, GAO told DHS to issue its own authorization for a cloud service one of its systems relied on. DHS pointed to the Joint Authorization Board's work. As of July 2026, GAO still had no agency authorization on file, and the JAB no longer authorizes anything.

THE FINDING

In May 2023, GAO reviewed how four agencies secured 15 cloud systems. The report, [Cloud Security: Selected Agencies Need to Fully Implement Key Practices](#) (GAO-23-105482), covered Agriculture, DHS, Labor, and Treasury, and found they had partially implemented, or not implemented, several of six key practices for some of their systems.

For DHS, GAO made three recommendations about FedRAMP authorizations, one for each type of cloud service it examined. Two are closed: DHS showed GAO it had authorized the selected infrastructure service in September 2023 and the platform service in January 2025. The third is not. GAO asked DHS to fully implement the FedRAMP requirements for its "selected SaaS system 2, to include issuing an authorization for the cloud service."

That recommendation still appears in GAO's [DHS CIO open recommendations letter](#) (GAO-25-108460). In its latest status note, GAO wrote that as of July 13, 2026, DHS said it was still working on the documentation needed to close it.

WHY IT KEEPS HAPPENING

DHS's answer to GAO explains the gap. The department said that through its role on the FedRAMP Joint Authorization Board (JAB) it ensures the provider meets the program's requirements. DHS officials also told GAO that components using a board-authorized service must perform a risk assessment and issue an agency authorization. GAO had not seen evidence that the component did so for this service.

That is a common confusion. A FedRAMP authorization covers the provider's controls. The agency's use of the service still carries controls the agency owns: who gets accounts, how data is configured, what the agency monitors. Someone has to document those and an authorizing official has to accept the risk.

OMB's [M-24-15](#), a non-GAO memo issued in July 2024, made the point explicit. Agencies must presume a FedRAMP package is adequate for their own authorization decision at or below its impact level, and "appropriate agency authorizing officials must issue an authorization when reusing artifacts." The presumption saves the agency from re-assessing the provider. It does not replace the agency's own decision.

The JAB itself is gone as an authorization body. FedRAMP said in December 2024 that it had worked with providers to transition away from the JAB, and M-24-15 directed that existing JAB authorizations be re-designated. The reason DHS gave GAO in 2023 now describes a body that no longer issues authorizations.

WHY IT MATTERS TO YOUR BID

DHS components buy SaaS for mission and business applications, and FedRAMP authorization is a baseline requirement for those services. A technical volume that says "the service is FedRAMP authorized" answers half the question. Evaluators who know this recommendation will look for the other half: the agency-side package, who writes it, and how long it takes.

The gap also shows up after award. A system that goes live on a cloud service without an agency authorization becomes the operations contractor's problem at the next audit or FISMA review. GAO's companion recommendation to DHS, still open, asks that cloud service level agreements define performance metrics and how they are enforced. Both land on whoever runs the system.

Transition planning is where a prime can get ahead of it. A plan that inventories every cloud service in the boundary, confirms which have agency authorizations on file, and schedules the missing ones turns an open GAO finding into a dated deliverable.

TECHNICAL APPROACH

The method below comes from Avalon's [ATO Process Facilitation service](#), following the NIST SP 800-37 Rev. 2 steps. It describes how the work is done, at the methodology level.

- 1. Draw the boundary around what the system actually uses.** Inventory existing artifacts, then define the authorization boundary with network and data-flow diagrams that show every cloud service in it. Record the FIPS 199 categorization with its rationale and run the privacy threshold analysis. A SaaS service that sits outside the drawn boundary is how a recommendation like this one starts.
- 2. Reuse the provider package, then map inheritance.** Start from the provider's FedRAMP package, which M-24-15 says the agency must presume adequate at its impact level. Use the customer responsibility matrix to split controls into inherited, shared, and customer-owned, and write down the tailoring decisions.
- 3. Write the customer side from evidence.** Draft implementation statements for the customer-owned and shared controls by interviewing the engineers and reviewing configurations, so each statement traces to something an assessor can check. Configuration, account management, and data handling inside the service are usually where these statements are thin.
- 4. Run a readiness review, then support the assessment.** Hold a mock assessment against NIST SP 800-53A procedures, close documentation gaps, and assemble the evidence library before the agency's assessor arrives. The independent assessment stays with the agency's assessor.
- 5. Package the decision and the monitoring.** Build the POA&M with realistic milestones, the residual-risk narrative, and the briefing for the authorizing official. Hand over a continuous monitoring strategy under NIST

SP 800-137 that includes reviewing the provider's monitoring deliverables, the practice GAO's other DHS recommendations in this report addressed.

The authorizing official makes the decision. Avalon does not grant authorizations, is not a FedRAMP third-party assessment organization, and does not serve as the independent assessor on a package it helped prepare.

WHAT "FIXED" LOOKS LIKE

GAO's closed DHS recommendations show what it accepts. The infrastructure recommendation closed when DHS issued the authorization and sent an authorization letter to the FedRAMP program office. The platform one closed in January 2025. On continuous monitoring, GAO closed recommendations once DHS documented its reviews of the provider's deliverables.

Applied to the open SaaS recommendation, those closures point to clear targets:

- A signed agency authorization for the cloud service, at or below its FedRAMP impact level.
- A customer responsibility matrix with every customer-owned control documented and traced to evidence.
- A monitoring record showing the provider's deliverables are reviewed on a set cycle.

STATUS CHECK

OPEN The SaaS authorization recommendation was open as of GAO's last update, July 2026, as was the recommendation on cloud service level agreement metrics. GAO closed the infrastructure and platform authorization recommendations in 2023 and 2025.

TEAMING FIT

NAICS	541512, 541690
AVALON'S SUB ROLE	Customer-side authorization package for FedRAMP-authorized cloud services: boundary, inheritance mapping, customer control implementation statements, readiness review, and ConMon handoff under the prime's DHS 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 a DHS SaaS deployment or cloud operations task is in your capture plan, Avalon teams as the sub that builds the agency-side authorization package a FedRAMP stamp leaves undone.

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.