



TECHNICAL BRIEF · BASED ON GAO-26-107530 · GOVERNMENT-WIDE, OMB

11 OF 24 AGENCIES REPORT MULTI-VENDOR CLOUD INTEROPERABILITY PROBLEMS

11 of 24

CFO ACT AGENCIES THAT REPORTED MULTI-VENDOR CLOUD ADOPTION RAISED NEW TECHNICAL CONSIDERATIONS SUCH AS INTEROPERABILITY

In June 2026, GAO reported that 11 of 24 CFO Act agencies hit new technical issues, such as interoperability, when they adopted multiple cloud vendors. GAO asked the Federal CIO Council to collect and share leading practices, and that recommendation is open.

THE FINDING

In June 2026, GAO published [Cloud Computing: Federal Government Needs to Address Procurement Challenges](#) (GAO-26-107530). GAO reported what officials at the 24 CFO Act agencies said about the challenges of buying cloud. Six challenges made the list. Multi-vendor adoption, with new technical considerations such as interoperability, drew 11 of the 24.

GAO's summary is specific about who is affected: "Several larger agencies are using multiple cloud vendors to achieve efficiencies," but they are also running into interoperability problems. GAO says sharing multi-cloud leading practices would help other agencies learn from them.

GAO made one recommendation on this point. The Federal CIO Council, working with its chair, the Office of Management and Budget's Deputy Director for Management, should collect and share examples of leading practices in the federal government on multi-vendor cloud solutions, including containerization and testing platform interoperability. The report lists the recommendation as open and says the Council did not provide comments.

WHY IT KEEPS HAPPENING

GAO lists multi-vendor solutions among the three challenges that remain, next to conflicting software guidance and outdated acquisition regulations. The remedy GAO picked is a collection exercise: it asked the Federal CIO

Council to gather examples from the federal government, so any leading practice has to come from agencies already running more than one provider.

GAO has asked the Council for something similar before. In [GAO-24-106137](#), its 2024 review of OMB cloud procurement requirements, GAO made a similar recommendation to the CIO Council. GAO's September 2025 status note said the Council had not yet acted on it.

REPORT	RECOMMENDATION TO THE CIO COUNCIL	STATUS	AS OF
GAO-24-106137 (Sep 2024)	Collect and share agency guidance and contract language on OMB cloud requirements	Open, no action yet	GAO's September 2025 update
GAO-26-107530 (Jun 2026)	Collect and share leading practices on multi-vendor cloud solutions	Open, Council did not comment	GAO's June 2026 report

WHY IT MATTERS TO YOUR BID

A cloud hosting, migration, or modernization task order can place workloads in more than one provider's environment. With no published government practice to point to, the evaluator reads the technical volume for the offeror's own method. Your "understanding of the requirement" has to show how identity, connectivity, tagging, and security documentation work when two or more platforms are in play.

Three themes carry weight. One is whether each workload's placement has a written reason tied to data type, impact level, and cost model, so the choice survives a CIO review. Another is whether security documentation covers each platform separately, because a control inherited from one provider may sit with the program on another. Exit is the third.

An open recommendation cuts two ways. A prime that waits for government guidance may wait a long time, while one that brings a method now gives the evaluator something to score. For the consumption-billing side of the same report, see the [cost control brief](#).

TECHNICAL APPROACH

The steps below come from Avalon's [Gov-Shared Cloud Services](#) method, with landing-zone practice from its SaaS/IaaS Implementation service. They describe how the work is done, at the methodology level.

- Score each workload against each candidate environment.** Inventory workloads and data types (CUI, PII, PHI, classification level), then score every candidate shared environment on five criteria: impact-level support, inheritable controls, cost model, onboarding lead time, and exit terms. The output is a decision record per workload that explains why it sits where it sits.
- Keep identity in one place.** Federate each tenant to the agency's identity provider with CAC/PIV, so access rules do not drift across providers. Align each tenant's connectivity to the applicable TIC 3.0 use case. For cloud, that is the [TIC Cloud Use Case](#), which CISA, in this non-GAO source, says satisfies OMB M-19-26.
- Write one baseline and apply it in every tenant.** Define the account structure, guardrails, logging hookup to the agency SOC, and a tag dictionary once, then express them as infrastructure as code (Terraform or OpenTofu, using platform-provided modules where the platform supplies them). A shared tag dictionary lets cost and ownership data from different providers line up.
- Reconcile controls platform by platform.** For each environment, build a Customer Responsibility Matrix reconciliation against NIST SP 800-53 Rev 5 that states control by control what is inherited, what is shared, and what the program owns. The spreadsheet is built for import into the System Security Plan.

5. **Write exit and portability notes at the start.** For each platform, record the data and configuration the program would need to move, plus the consumption and chargeback model, so the next recompile does not begin from scratch.

This work stops at a tenant-ready state. Moving workloads, designing a cross-provider architecture, and testing interoperability between platforms are separate scopes, and the Authorize decision stays with the agency's authorizing official.

WHAT "FIXED" LOOKS LIKE

GAO has not published closure criteria. The recommendation's own wording sets the likely test: examples of multi-vendor leading practices, shared across government, that include containerization and platform interoperability testing.

For a program, these are targets Avalon proposes, not GAO's:

- A decision record for every workload that names the environment chosen and the reason.
- One identity and connectivity pattern that every tenant follows.
- A control inheritance workbook for each platform that an assessor can trace.
- Exit notes on file before the first production cutover.

STATUS CHECK

OPEN GAO-26-107530's recommendation to the Federal CIO Council was open as of GAO's last update, June 2026, and the report says the Council did not provide comments. GAO-24-106137's recommendation to the Council was open, with no action, as of GAO's September 2025 update. GAO says it will update the 2026 recommendation once it confirms actions taken.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Workload-by-environment fit scoring with a decision record, tenant landing-zone configuration and identity federation, a control inheritance workbook per platform, and exit and portability notes under the prime's cloud 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 OASIS+; GSA Alliant 3

If a multi-provider cloud task order is in your capture plan, Avalon teams as the sub that documents why each workload belongs where it is, configures each tenant to one identity and tagging baseline, and hands the assessor a control inheritance workbook for every platform.

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.