AVALON

TECHNICAL BRIEF · BASED ON GAO-22-105330 · DOW

15 OF 25 DOW BUSINESS IT PROGRAMS COULD NOT SHOW SUPPLY CHAIN RISK PLANS

15 of 25

DOW MAJOR IT BUSINESS PROGRAMS THAT DID NOT DEMONSTRATE A SYSTEM SECURITY PLAN ADDRESSING ICT SUPPLY CHAIN RISK MANAGEMENT (10 OF 25 LACKED AN APPROVED CYBERSECURITY STRATEGY)

GAO reported in June 2022 that 15 of 25 DoW major IT business programs could not show a security plan that addresses ICT supply chain risk, and 10 of 25 could not show an approved cybersecurity strategy. Both recommendations were open as of GAO's January 2025 update.

THE FINDING

In June 2022, GAO published Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning (GAO-22-105330). It reviewed 25 major IT business programs at DoW (formerly DoD), which had planned about $8.8 billion for them across fiscal years 2020 through 2022.

Two counts matter here. Officials at 10 of the 25 programs did not demonstrate an approved cybersecurity strategy, which DoD requires. Officials at 15 of the 25 did not demonstrate a system security plan that addresses information and communication technology (ICT) supply chain risk management. Both counts reflect program responses as of February 2022.

GAO made three recommendations, and DoW concurred. This brief covers two of them. GAO told the Secretary of Defense to direct the Chief Information Officer to ensure that major IT business programs "develop approved cybersecurity strategies, as appropriate," and "develop plans that address information and communication technology supply chain risk management, as appropriate."

WHY IT KEEPS HAPPENING

GAO put the supply chain gap in plain terms: DoD guidance does not require programs to address ICT supply chain risk management in security plans. DoD Instruction 5200.44 directs programs to apply supply chain risk management disciplines to protect system integrity and trust. It does not make the security plan carry that content.

DoD CIO officials gave GAO two explanations. IT programs might address supply chain risk in program protection plans, and recent supply chain efforts had focused on weapons systems. A business program can therefore have the work done somewhere else and still have nothing in its security plan to show a reviewer.

DoW's later responses follow the same line. By September 2023 it said it was pursuing a strategy to make sure programs implement ICT supply chain risk management "through policy and RMF implementation," and it gave GAO an estimated completion date of December 2024. As of GAO's January 2025 notes, DoW had provided no further information.

The strategy recommendation moved more visibly. DoW's CIO reviewed and approved strategies for several programs in 2022, and as of March 2024 GAO found six programs still without an approved one.

WHY IT MATTERS TO YOUR BID

A recompete for authorization support, sustainment, or modernization of a DoW business system inherits the program's security plan and has to keep it defensible.

A technical volume that says "we will address supply chain risk" invites the obvious follow-up: where does that appear in the security plan, against which suppliers, and who approved the strategy it rests on? DoW told GAO its answer runs through RMF implementation, which makes the RMF record the place a reviewer will check.

Transition is the second exposure. GAO's counts include programs that reported having an approved strategy but could not hand it over. An incoming contractor that cannot find a program's approved documents in week one starts the base period with a records problem. An offeror that proposes a document inventory in the first 30 days prices that risk instead of discovering it.

TECHNICAL APPROACH

The method comes from Avalon's System & Application Security Plans service, working inside the NIST RMF record. It describes how the work is done, at the methodology level, for unclassified environments.

1. **Inventory the program's documents and records first.** Collect the authorization package, the GRC record in eMASS or the program's system of record, and the approved cybersecurity strategy the program points to. For each, record package age, ATO status and expiration date, record health, and whether a reviewer can retrieve the strategy and the security plan today.
2. **Validate the boundary and categorization, then fix the baseline decision.** Confirm the FIPS 199 impact levels and the SP 800-53B baseline, and document the organization-defined parameters. SR-2, the supply chain risk management plan control, is selected in NIST's Rev. 5 Moderate baseline, and its first parameter names the systems, components, or services the plan covers. That parameter is where the program writes its scope down.
3. **Write SR-family implementation statements against a real supplier list.** Reconcile the component inventory (CM-8) and the external services and inherited controls (SA-9, AC-20) so each statement names actual suppliers, who acts, what mechanism enforces it, and where evidence lives. Verify inherited controls against the providing system's package and customer responsibility matrix. Record the true status, including "planned."
4. **Place the plan where the program's process reads it.** NIST SP 800-18 Rev. 2 (final June 30, 2026) groups security, privacy, and cybersecurity supply chain risk management plans as "system plans." Where a program office adopts that structure, the security plan and the supply chain plan cross-reference each other. Either way, the SR-family statements live in the program's GRC record and point to any program protection plan that holds related content.

5. **Log the gaps and set the maintenance routine.** Programs with no plan, or only a plan to write one, go into a gap log formatted for POA&M intake. A short maintenance procedure keeps the statements current under continuous monitoring.

Strategy approval stays with DoW. This work keeps each program's record pointing at the approved strategy and shows whether the plan matches the system. Avalon writes and validates the documents; it does not issue authorizations or certify supply chain compliance.

WHAT "FIXED" LOOKS LIKE

GAO's January 2025 notes set the test. On the strategy recommendation, DoW "has not demonstrated" that it addressed it. On the supply chain recommendation, DoW had provided no additional information. Closure therefore rests on DoW showing evidence, not on a policy memo alone.

Program-level targets:

- Every program in the set can produce its approved cybersecurity strategy on request.
- Every security plan carries SR-family statements with a defined scope, named suppliers, and an honest implementation status.
- Gaps appear in the POA&M with owners and dates.
- The count of programs that cannot show both documents falls from GAO's baseline of 10 and 15.

STATUS CHECK

OPEN Both recommendations were open as of GAO's January 2025 update. GAO found six programs without an approved strategy in March 2024, and DoW had given an estimated completion date of December 2024 for the supply chain recommendation. The third recommendation, on IT Dashboard reporting, is outside this brief. The program counts in the report date to February 2022.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Program document inventory, SR-family control implementation statements against a reconciled supplier list, plan structure in the program's GRC record, and a gap log and maintenance procedure under the prime's A&A or IT support task order, in unclassified environments
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 DoW business-system support is in your capture plan, Avalon teams as the sub that inventories each program's strategy and security plan records, then writes the supply chain control statements, gap log, and maintenance procedure so the prime can put both documents in front of an evaluator.

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.