



TECHNICAL BRIEF · BASED ON GAO-26-108596 · DOW

SIX OF 18 DOW IT PROGRAMS HAD NO ZERO TRUST PLAN FOR 2027

6 of 18

DOW IT BUSINESS PROGRAMS GAO REPORTED HAD NOT DEVELOPED PLANS TO IMPLEMENT ZERO TRUST BY DOD'S 2027 DEADLINE

In September 2026, GAO reported that 6 of 18 DoW IT business programs had not developed zero trust plans for DOD's 2027 deadline. GAO's count was 4 of 24 a year earlier. No new recommendation covers the gap, so primes face it as a bid question.

THE FINDING

On September 28, 2026, GAO published [IT Systems Annual Assessment: DOD Should Improve IT Fraud Risk Management Practices](#) (GAO-26-108596), its yearly review of DoW (formerly DoD) IT business programs. Twelve of the 18 programs reported implementing zero trust architecture as part of their security framework. Six had not developed plans to implement zero trust in their cybersecurity frameworks by DOD's 2027 deadline.

A year earlier, [GAO-25-107649](#) put the same gap at 4 of 24 programs, with 20 of 24 reporting implementation. GAO reviewed 24 programs then and 18 now, so the two counts are not a trend line.

Neither report makes a new recommendation on zero trust. In June 2025 GAO said it would continue to monitor the department's progress in developing zero trust plans. The 2026 report's one new recommendation covers fraud risk training, and GAO reiterated six earlier recommendations that remain unimplemented.

WHY IT KEEPS HAPPENING

GAO's text does not say why programs lack plans, and this brief won't guess. The record does show how the requirement is stacked.

As GAO describes it, a May 2021 executive order told agencies, DoW included, to develop a zero trust plan. The FY 2022 NDAA then [directed DOD to produce a strategy, a model architecture, and implementation plans](#). According to the DoD Office of Inspector General (DODIG-2025-090), a non-GAO source, the [DoD Zero Trust Strategy](#) sets a target level for each capability by the end of FY 2027, and that review of component plans is the subject of [a separate Avalon brief](#).

The units differ. The OIG reviewed component-level plans, 11 of 45. GAO's questionnaire went to individual business programs, such as financial management, logistics, health care, and contracting systems, which sit inside those components. Whether a component's plan covers a given program's boundary is a question GAO's count doesn't answer.

The counts also come from program offices' own answers. "Reported implementing" and "has a plan" are different measures, and neither shows what a system enforces today.

WHY IT MATTERS TO YOUR BID

Program-level IT work at DoW, whether sustainment, modernization, or a cyber support task order for a business system, now carries a deadline that GAO counts program by program. FY 2027 ends September 30, 2027, so a task order awarded early in the year has months, not years, to show progress.

Expect a technical volume on this work to be read for three things. A stated boundary comes first: which system, which enclave, and which outside capabilities it relies on. Next is a plan tied to named target-level activities, with dates. Last, evaluators want to see how the offeror will show enforcement rather than ownership.

A prime that offers only "we will implement zero trust" gives the evaluator nothing to score. A prime that brings a dated plan for the program's boundary answers the exact question GAO keeps asking.

TECHNICAL APPROACH

The method below comes from Avalon's [Zero Trust Architecture Implementation service](#), in its assessment and roadmap shape. It describes how the work is done, at the methodology level, for unclassified environments.

- 1. Fix the boundary, then baseline.** Use the system security plan, architecture walkthroughs, and interviews to define the program's boundary. Score it against the DoD Zero Trust Capability Execution Roadmap's seven pillars and target-level activities, and verify which tools are configured and enforcing rather than licensed.
- 2. Run discovery before planning.** Structure the sequence on the NSA's Zero Trust Implementation Guidelines, a non-GAO source: a Discovery phase, then [Phase One with 36 activities and Phase Two with 41](#), so the plan follows a structure DoW's oversight chain recognizes.
- 3. Design the target architecture.** Under NIST SP 800-207, place policy decision and enforcement points, define how identity and device signals feed access decisions, and set the segmentation model. Where an application cannot be modernized, the design puts an identity-aware proxy in front of it.
- 4. Write the dated roadmap.** Phase the work by budget cycle and dependency: identity before device-conditioned access, asset inventory before segmentation, logging before analytics. Each phase lists the target-level activities it completes, so the document is both the program's plan and its budget justification.
- 5. Build the evidence matrix.** Trace each planned change to NIST SP 800-53 controls and to the roadmap activity it completes, with allowed and denied access test cases the assessor can rerun.

Avalon designs and documents. It does not validate target-level achievement, certify zero trust maturity, or issue authorizations. Those belong to the Department's own assessment process.

WHAT "FIXED" LOOKS LIKE

GAO has not defined closure for zero trust plans because it made no new recommendation on them. These are targets, not GAO criteria.

- Every program in a prime's portfolio has a written zero trust plan covering its own boundary.
- Each plan names the target-level activities it will complete, with dates before the end of FY 2027.

- The plan separates what the program implements from what it relies on elsewhere.
- Evidence ties each completed activity to controls and test results.

A later GAO count showing no program without a plan would be the visible sign.

STATUS CHECK

OPEN GAO made no new recommendation on zero trust plans and said in June 2025 it would keep monitoring. As of GAO's last update, September 2026, the new recommendation in GAO-26-108596, on fraud risk training, is open. Six earlier recommendations are reiterated as not yet implemented.

TEAMING FIT

NAICS	541512
AVALON'S SUB ROLE	Program-level zero trust baseline against the DoW target-level activities, NIST SP 800-207 target architecture, and a dated implementation roadmap with an activity-to-evidence matrix under the prime's IT or cyber 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 work is in your capture plan, Avalon teams as the sub that baselines the program's boundary against the target-level activities and turns it into a dated zero trust plan the evaluator can score.

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.