



TECHNICAL BRIEF · BASED ON DODIG-2025-090 · DOW

ZERO TRUST AT DOW: WHERE THE COMPONENT PLANS FELL SHORT

7 of 11

DOW COMPONENT ZERO TRUST IMPLEMENTATION PLANS THE DOD OIG REVIEWED THAT INCLUDED ALL REQUIRED ELEMENTS

The DoD Inspector General reviewed 11 of 45 DoW component zero trust implementation plans and found 7 complete. Three components submitted incomplete plans and one submitted none, against a strategy that requires target-level zero trust by the end of FY 2027.

THE FINDING

In April 2025, the DoD Office of Inspector General, a non-GAO source, published [Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust](#) (DODIG-2025-090). It checked whether DoW (formerly DoD) met Section 1528 of the FY 2022 NDAA, which required a zero trust strategy, architecture, and implementation plans.

At the department level, the OIG found DoD generally complied. Component plans were uneven. Of 45 component-level implementation plans, the OIG reviewed 11, and 7 of those included all the required elements. The Defense Finance and Accounting Service, the Defense Media Activity, and the National Guard Bureau submitted incomplete plans, and the Defense Legal Services Agency had not submitted one.

Each of the four received recommendations. At publication, five were resolved but open and one was unresolved.

WHY IT KEEPS HAPPENING

Section 1528's required elements are concrete, which makes gaps easy to see. A plan has to cover acquisitions, implementations, instrumentation, and operational workflows; a schedule with target milestones; interim and final metrics, including a phased migration plan; and the funding, authorities, and policies still needed.

The OIG's notes show three different failure points:

- **Missing pieces.** DFAS's plan lacked specific acquisitions and a detailed schedule. The Defense Media Activity's lacked acquisitions, implementations, schedule, and metrics.
- **No inventory to plan from.** The OIG told the Defense Media Activity to first build a plan for identifying all its network and system assets, then update its zero trust plan.

- **Inherited capability.** The National Guard Bureau's plan included none of the required elements, and the OIG told it to coordinate with the Army and Air Force on the zero trust capabilities it inherits from them. That recommendation was unresolved at publication because the Bureau's response didn't address inheritance.

Smaller components run lean IT staffs and often depend on a larger organization's infrastructure. Writing a plan means knowing what you own, what you inherit, and what you still have to buy.

WHY IT MATTERS TO YOUR BID

The deadline is close. According to the OIG, the DoD Zero Trust Strategy requires components to reach a target level for each zero trust capability by the end of FY 2027. The target level is a set of minimum requirements; the OIG counts 91 activities to reach it.

That puts zero trust inside task orders that are not labeled as zero trust work. An IT operations or cyber support recompile at a defense agency or Guard organization will touch identity, devices, networks, and data, and the component has to show progress on each. Evaluators will look for an offeror that can tie its technical approach to the component's plan and to specific target-level activities.

Inheritance is the detail most proposals miss. A component that relies on a Service's identity or network capabilities needs to document what it inherits and what it implements itself. A prime that can map that boundary early gives the component a plan it can defend.

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. **Baseline against the DoW roadmap.** Score the component against the DoD Zero Trust Capability Execution Roadmap's seven pillars and target-level activities, using document review, architecture walkthroughs, and verification of which tools are actually configured rather than merely owned.
2. **Reconcile the asset inventory first.** Build or reconcile the authoritative inventory of network and system assets, because segmentation, device posture, and every later pillar depend on it. This is the step the OIG asked the Defense Media Activity to plan for.
3. **Map what is inherited.** For each target-level activity, record whether the component implements it, inherits it from a Service or enterprise provider, or shares it, and confirm the inherited pieces with the provider.
4. **Design the target architecture.** Under NIST SP 800-207, define where policy decision and enforcement points sit, how identity and device signals feed access decisions, the segmentation model, and the access pattern for legacy applications.
5. **Sequence the roadmap and the evidence.** Phase the work by budget cycle with dependency ordering (identity before device-conditioned access, inventory before segmentation, logging before analytics), and keep a traceability matrix from each completed activity to its evidence. The roadmap doubles as the component's input to implementation-plan reporting.

Avalon designs and documents; it does not certify zero trust maturity, guarantee target level by FY 2027, or issue authorizations.

WHAT "FIXED" LOOKS LIKE

The OIG's own closed recommendation shows the bar. A.1, to the DoD CIO, asked for a plan with milestones to accelerate zero trust policies for operational technology, infrastructure, and weapon systems; it closed when the acting CIO provided an implementation plan.

For the component recommendations, closure means a submitted plan with every required element. Practical targets:

- A current asset inventory the plan is built on.
- An inheritance map agreed with the Service or provider.
- A schedule, metrics, and funding needs tied to the target-level activities.

STATUS CHECK

OPEN As of the OIG's April 2025 report, recommendations to DFAS, the Defense Media Activity, the National Guard Bureau, and the Defense Legal Services Agency were resolved but open, except NGB's inheritance recommendation, which was unresolved.

TEAMING FIT

NAICS	541512
AVALON'S SUB ROLE	Zero trust maturity baseline against the DoW target-level activities, target architecture, and an implementation roadmap and evidence matrix for the component 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 IT or cyber support work at a DoW component is in your capture plan, Avalon teams as the sub that baselines the component against the target-level activities and turns its inventory and inheritance into a zero trust plan it can submit.

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.