WINTER 2023

GovCIO
MEDIA & RESEARCH

DeepDives

ZERO TRUST at the Pentagon

INSIDE:

SPONSORED BY

leidos

GovCIO
MEDIA & RESEARCH

From the writer's desk

Kate Macri, Deputy Editor

The Long-Awaited Zero Trust Strategy

The Defense Department released its long-awaited zero trust strategy right before Thanksgiving, outlining benchmarks and recommendations for the military services and Fourth Estate to cultivate different approaches to zero trust.

Many DOD components have been working toward zero trust for some time, but this new strategy elevates zero trust as a policy goal and the dawn of a new era for DOD cybersecurity. This supplements efforts such as the Joint Warfighting Cloud Capability (JWCC) and Joint All-Domain Command-and-Control (JADC2).

Still, scaleability and interoperability between diverse zero trust solutions across DOD remain a challenge. The new strategy aims to close those gaps.

With the stroke of a pen, DOD CIO John Sherman transformed zero trust from a much-hyped buzzword into an operational imperative. Stay tuned for zero trust developments in the defense community over the next four years as DOD races to the first zero trust deadline at the close of fiscal year 2027.

Table of Contents

Anastasia Obis,
Staff Writer

GovCIO MEDIA & RESEARCH

Inside the Pentagon's Roadmap to Zero Trust

First of its kind strategy will guide the agency in achieving a more robust cybersecurity framework that will reduce risk and improve user experience.

BY ANASTASIA OBIS

Photo credit: Marv Lynchard / DVIDS DOD CIO John Sherman

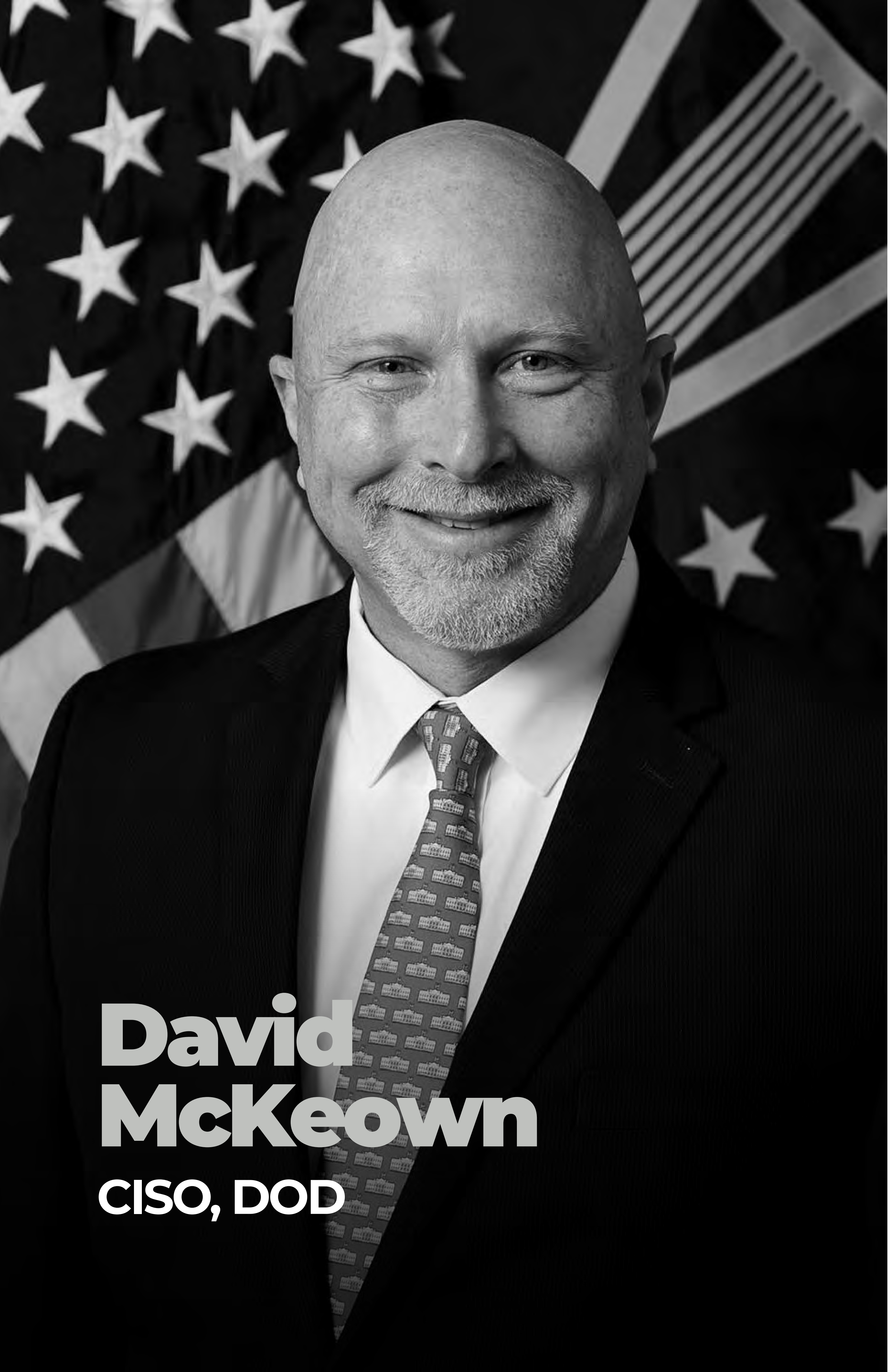
The Defense Department's new zero trust strategy, part of a family of strategies living under the National Defense Strategy (NDS), establishes its zero trust vision to improve security, user experience and overall mission performance while achieving information dominance.

The strategy will be critical to implementing DOD's Joint All Domain Command-and-Control (JADC2) plan, which aims to connect the joint forces through secure, seamless communication for improved response times in theater.

The long-anticipated strategy provides guidance for advancing the zero trust concept, which includes gap analysis, requirements, development and investment in zero trust capabilities that will have the significant cybersecurity impact necessary within the department to protect against malicious actors.

"We're taking an aggressive stance. Our funding is in alignment with this — that we want to be at targeted zero trust for the department by the end of fiscal year 2027," DOD Deputy CIO for Cybersecurity David McKeown said at the Billington Cybersecurity Summit in September. "It is very comprehensive. It's our North Star."

The zero trust strategy is nested under the department's Digital Modernization Strategy and aligns with President Joe Biden's Executive Order



David McKeown

CISO, DOD

on Improving the Nation's Cybersecurity from 2021, the Federal Zero Trust Architecture Strategy the Office of Management and Budget (OMB) released in January 2022, the National Defense Authorization Act for Fiscal Year 2022 and other Executive-level memorandums that guide the department toward implementing zero trust architecture across the board.

The DOD Office of the Chief Information Officer (OCIO) also established a Zero Trust Portfolio Management Office (PfMO) in January, which is responsible for coordinating DOD-wide zero trust execution.

"Defending DOD networks with high-powered and ever-more sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our information enterprise that spans geographic borders, interfaces with external partners and support to millions of authorized users, many of which now require access to DOD networks outside traditional boundaries, such as work from home," DOD CIO John Sherman wrote in a foreword to the new strategy.

The Strategy sets four goals to achieve DOD's vision for zero trust.

1. Zero trust cultural adaptation, where all DOD employees understand, are trained and committed to a zero trust mindset and culture.

   "This urgency means that our colleagues, our warfighters, and every member of DOD must adopt a zero trust mindset, regardless of whether they work in technology or cybersecurity or the human resource departments," Sherman wrote. "This 'never trust, always verify' mindset requires us to take responsibility for the security of our devices, applications, assets and services; users are granted access to only the data they need and when needed."

2. DOD information systems are secured and defended,

where a zero trust framework is applied to all new and legacy information systems.

To accomplish the “information systems secured and defended” goal, DOD and its components need to achieve 45 capabilities organized around seven pillars, including user, device, application and workload, data, network and environment, automation and orchestration, and visibility and analytics. DOD aims to publish the component-level execution plan by September 2023, which will guide how zero trust should be applied across its networks. Components must achieve target-level outcomes of zero trust capabilities by the end of fiscal year 2027.

3. Technology acceleration, where zero trust-based technologies are deployed at a pace exceeding industry advancements and stay ahead of the ever-changing threat environment.

4. Zero trust enablement, where the zero trust framework is “cemented” across the DOD information enterprise (IE), which will require processes, policies and funding.

“This goal identifies the ‘tail’ to the [zero trust] ‘tooth,’ the latter being unable to achieve its mission without the former, and requires the whole of the [zero trust] ecosystem’s attention and effort and cannot be addressed ‘at a later time,’” according to the strategy.

The strategy breaks down zero trust into two levels of implementation: the target level and advanced level. The target level is the minimum set of zero trust activities necessary to protect and manage known threats and is planned to be achieved “as soon as possible.” The new zero trust management office will monitor and guide this progress.

(ctd.)

Photo Credit: thinkhubstudio/Shutterstock

As for resourcing and acquisition, the strategy does not mandate a specific technology or solution that must be applied to achieve zero trust. As long as the components reach the target zero trust level through the described capabilities and move on to the advanced level, they can design their own solutions.

"The components are free to select their own solutions and solution architectures, as long as they deliver the specified [zero trust] capability outcomes needed to reach the target or advanced-level zero trust and are able to show that proof," the strategy reads.

In addition, DOD released the Zero Trust Capability Execution Roadmap providing recommendations and timelines to zero trust.

JADC2 Impact

DOD IT and cyber leaders have long emphasized the importance of rapidly developing new capabilities for JADC2, but over-classification and the lack of secure data exchange remain some of the main hurdles to the successful implementation of those capabilities.

Special Operations Command (SOCOM) repeatedly reported over-classification is an obstacle to meeting mission-critical needs. Air Force leaders said secure communication networking remains a hindrance to JADC2 implementation.

Air Force Chief Data and AI Officer Maj. Gen. John Olson believes zero trust is "essential" to JADC2 implementation.

"We've been talking about zero trust for a long time with Thunderdome. We need to get real implemented data- and user- level zero trust," Olson said at the National Defense Industry Association's JADC2 Symposium in July.

Programs such as the Defense Information Systems Agency's (DISA) Thunderdome zero trust prototype are designed to enable DOD employees and service members to securely access the resources they need "without having to traverse the DODIN." DISA expects the Thunderdome prototype for DOD's

Photo Credit:
Tommy Lee Walker/Shutterstock

classified and unclassified networks (NIPRNet and SIPRNet) to be completed by early 2023, according to a recent interview with GovCIO Media & Research.

While prototypes like these won't solve all the problems when moving toward JADC2 implementation, it will allow its users to access critical information securely to complete their missions.

"For JADC2, zero trust is essential. When dealing with peer competitors, we have to assume things are compromised. That particular policy or set of policies is essential to the way forward," Stuart Whitehead, DOD Cyber and Command, Control, Communications and Computers (C4) deputy commander, said during an event at the Potomac Officers Club event.

DOD Cloud and Armed Services

Zero trust underpins all DOD services' and components' modernization efforts as they move to a cloud environment. DOD plans to rely on commercial cloud service providers (CSPs) to help deliver zero trust solutions compatible with DOD cloud, according to the DOD Zero Trust Capability Execution Roadmap released with the zero trust strategy. Key to successful implementation will be standardization of zero trust tools across the enterprise and maintaining DOD's "target" zero trust maturity level.

The Army's updated cloud plans align with DOD's various IT modernization initiatives and rely upon a zero trust approach to cybersecurity. So far, the Army has moved about 100 applications to the cloud and awarded a $1 billion contract called the Enterprise Application Migration and Modernization (EAMM) to help achieve those long-term goals. A zero trust approach to security is one of the primary pillars facilitating the many cloud projects in the Army's pipeline.

"Globally, we've been fielding systems and accrediting those systems and construct the kind of a network perimeter security model, and this pivot into zero trust really changes the way not only our infrastructure is delivered, our

Photo Credit: Metamorworks/Shutterstock

enterprise services are delivered, but then also how our applications and services and, most importantly, our data is structured to leverage a zero trust architecture," Paul Puckett, former director of the Army's Enterprise Cloud Management Agency (ECMA), told GovCIO Media & Research.

At the Navy, Principal Cyber Advisor Chris Cleary and CTO Jane Rathbun consider identity management the first step and cornerstone of a robust zero trust strategy, which they're pursuing aggressively via the department's Cybersecurity Superiority Vision released October 2022.

> **"We're taking an aggressive stance. Our funding is in alignment with this — that we want to be at targeted zero trust for the department by the end of fiscal year 2027. It is very comprehensive. It's our North Star."**
>
> **— David McKeown, Deputy CIO for Cybersecurity, DOD**

GovCIO
MEDIA & RESEARCH

DeepDives

The Pentagon's Zero Trust Roadmap

A Timeline of the Zero Trust Journey

With no constraints on methods or tools used, the Defense Department allows services and components to adopt a zero trust approach that works for them.

1 USER SECURITY

Authentication, identity management, activity and access limits (target requirements: FY 2027, advance requirements: FY 2031)

2 DEVICE SECURITY

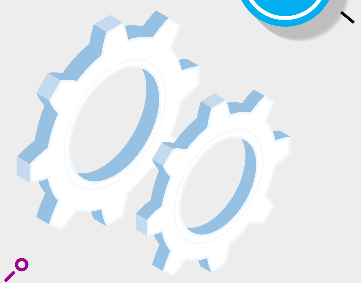
Authorization, inventory, patch (target: FY 2027, advanced: FY 2031)

3 APPLICATION & WORKLOAD SECURITY

Includes containers and virtual machines (target: FY 2027, advanced: FY 2032)

4 DATA SECURITY

Standards, visibility, tagging, end-to-end encryption (target: FY 2027, advanced: FY 2023)



5 NETWORK & WORKLOAD

Segmentation, isolation, control (target: FY 2027, advanced: FY 2032)

6 AUTOMATION

Automate manual security processes enterprise-level at speed and scale (target: FY 2026, advanced: FY 2030)

7 VISIBILITY & ORCHESTRATION

Analyze events, activities, behaviors for improved real-time decision-making (target: FY 2026, advanced: FY 2032

PARTNER INTERVIEW

leidos

Embracing a 'Fail Fast' Methodology to Secure the DOD Information Enterprise

Tips and tricks for meeting the first targets laid out in the Defense Department's five-year zero trust strategy.

Jesse Peoples, Chief Security Architect, Leidos

One of the Pentagon's zero trust strategy goals is to accelerate technology to keep pace with industry regarding zero trust advancement. What are the top three ways industry can come alongside the Defense Department to help adopt zero trust?

Peoples The goal of accelerating technology is to secure and defend the DOD information enterprise and networks quickly and effectively. This must be done by aligning architectures with zero trust principles and by leveraging the most up-to-date technologies that allow for scaling, amplifying and failing fast for innovation. These goals are not unique to the federal government. Leidos has been investing in research and development in zero trust with a fail-fast approach for more than three years. We have established a Zero Trust Proving Ground, assessment and adoption methodology, and AI/ML risk scoring across all zero trust pillars.

There are many successes and lessons here that can help propel DOD rapidly into a more mature zero trust architecture.

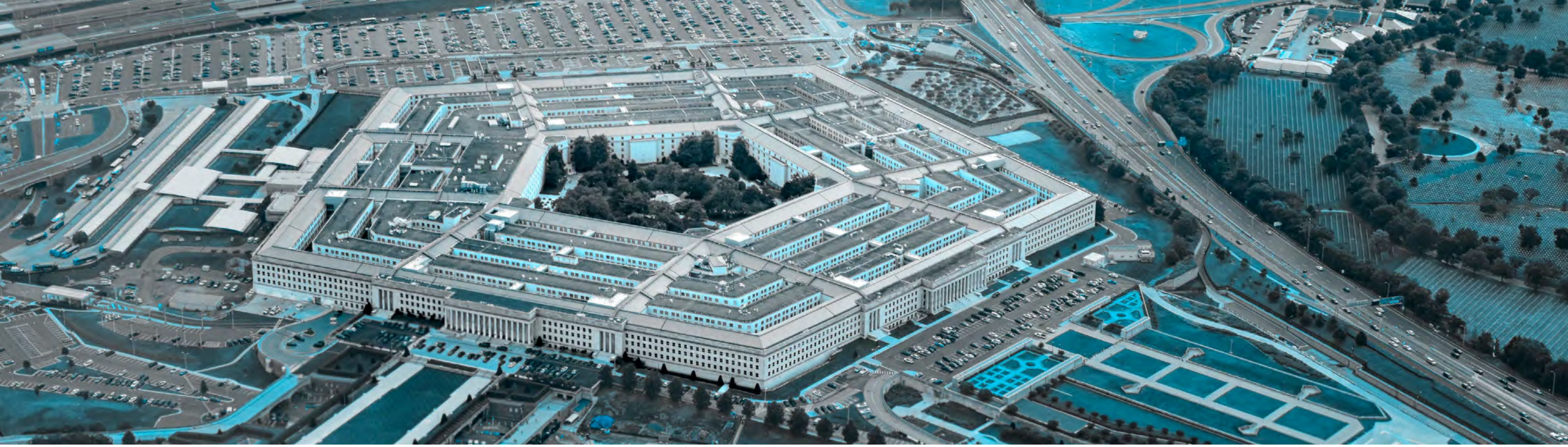
(ctd.)

The three ways industry can partner with DOD to help adopt zero trust are based on similar successes and lessons learned across industry.

1. Start with making bold changes and significant investments in the environment to adopt zero trust and stay well ahead of the evolving guidance. Industry needs to be beyond compliance and building resilient systems to operate and adapt through adverse events, and we need to share that intelligence with DOD to deliver capabilities for its critical missions. Leidos' Zero Trust Proving Ground is a catalyst to test capabilities and drive delivery of zero trust advancements in its own architecture. This proving ground provides a critical fail-fast mechanism for DOD without the full investment of technology insertion.

2. Industry needs to help DOD components assess where it stands today as an organization. We need to break the overall strategy down further and translate it into specific actions with timelines. Define a zero trust roadmap with solutions and guidance based on risk assessments and priorities. Build off the DOD's investments in zero trust in-place components to move faster and then prioritize the next areas of investment. Leidos does regular assessments of its own architecture and zero trust roadmap and is leading several agencies through this zero trust journey. These agencies can prove out vendor integrations and solutions in our lab, conduct zero trust readiness assessments in support of adoption, and unify

> **"I think the Pentagon's biggest hurdle to reach target capabilities by 2027 is adopting and integrating solutions while staying within its execution plans and budgets. Zero trust adoption and integration really requires clear direction from leadership and buy-in from the components down to the operators."**
>
> **— Jesse Peoples, Chief Security Architect, Leidos**



deployed customer technologies with Leidos' multi-context risk scoring solution called Policy Devision Point (PDP). This is the type of partnership the DOD should seek out, where both industry and DOD, together, are all in in the zero trust journey.

3. Industry needs to recognize that zero trust is more than an IT solution. Zero trust is a mindset and is heavily dependent on cultural adoption and cross-organizational integration. As an example, industry partners can play a critical role by bringing expertise across the network operations center (NOC), security operations center (SOC) and engineering areas to identify dependencies and proving out integrations across the DOD zero trust ecosystem. Leidos is using its decades of experience deploying, operating and improving NOCs, SOCS, etc. to identify both organizational and technological dependencies within each ecosystem that underpin the required cultural shift for zero trust adoption. The DOD should partner with industry to understand where its dependencies lie and what is the critical path in the cultural zero trust revolution.

The Pentagon's upcoming zero trust roadmap for commercial cloud expects to rely on commercial cloud providers to "develop zero trust compliant environments using the Greenfield approach." What is the Greenfield approach and how can it help DOD develop and customize tools for traffic logging, data mapping, and user and asset inventories?

Peoples DOD's zero trust strategy has made it really clear they're exploring innovative options to accelerate zero trust implementation. Commercial cloud is a key enabler for DOD's mission and security goals. With a Greenfield approach, a zero trust architecture could be built from scratch, and it won't depend on legacy technology or pre-existing design patterns. The Greenfield approach to modernization is important because it improves productivity by enabling future adaptation as new practices and technologies emerge. Leidos is actively working with the Army to deploy Greenfield solutions across multiple cloud service providers and cloud impact levels. (ctd.)

Photo Credit: Jeremy Christensen/Shutterstock

What do you think will be the Pentagon's biggest hurdle to reaching the "target level" of zero trust capabilities by 2027?

Peoples The Pentagon's biggest hurdle to reach target capabilities by 2027 is adopting and integrating solutions while staying within its execution plans and budgets. Zero trust adoption and integration really requires clear direction from leadership and buy-in from the components down to the operators. To obtain and keep that buy-in, DOD must understand operational needs so the implementation of these security measures enables mission performance instead of becoming a barrier for the users. The implemented zero trust solutions must enhance security, the user experience and the overall mission performance.

I believe the Zero Trust Portfolio Management Office (PfMO) is critical to the overall successful execution of the zero-trust strategy. This office will closely work with the components to define, develop and perhaps most importantly adapt the execution plans to achieve the zero trust goals and objectives. The components will have to address their funding for the zero trust execution plans through their annual budget process, which sometimes is a challenge. We have seen several federal agencies leverage the Technology Modernization Fund (TMF) for those zero trust projects to get ahead.

How can DOD address disparate cybersecurity risks across legacy IT systems and cloud environments under one zero trust approach? What is the role of cultural considerations here?

Peoples Having a unified zero trust approach at the strategic level will help make implementation achievable at the tactical level. The key here is for that one approach to include standardization of tools across the enterprise. Zero trust is not one size fits all. There are commercial solutions that will need to be customized for DOD.

The antiquated way we think of cybersecurity must evolve. Successfully implementing the DOD zero trust framework requires the entire department to understand and embrace the culture and mindset of zero trust. Preserving the culture is really important because it derives from a real mission need. In the end, the outcomes must be aligned with DOD's National Defense strategy and support enhancing the warfighter mission-critical priorities.

Recognizing and implementing zero trust, while very beneficial for defense cyber operations, is not inherently with the scope of most SOC teams. It's actually heavily dependent on network operations and engineering teams. Industry partners like Leidos who have expertise across all elements will be critical to DOD's successful zero trust implementation within their timelines.

Image Credit: Ar_TH/Shutterstock

Pentagon Zero Trust Challenges Include Scalability, Interoperability

DISA addresses remaining impediments as it moves closer to completing its zero trust prototype.

BY ANASTASIA OBIS

As the Defense Information Systems Agency (DISA) finishes up its Thunderdome zero trust prototype, remaining challenges include testing, scaling the capability from operational and technology perspectives and interoperability with other zero trust solutions.

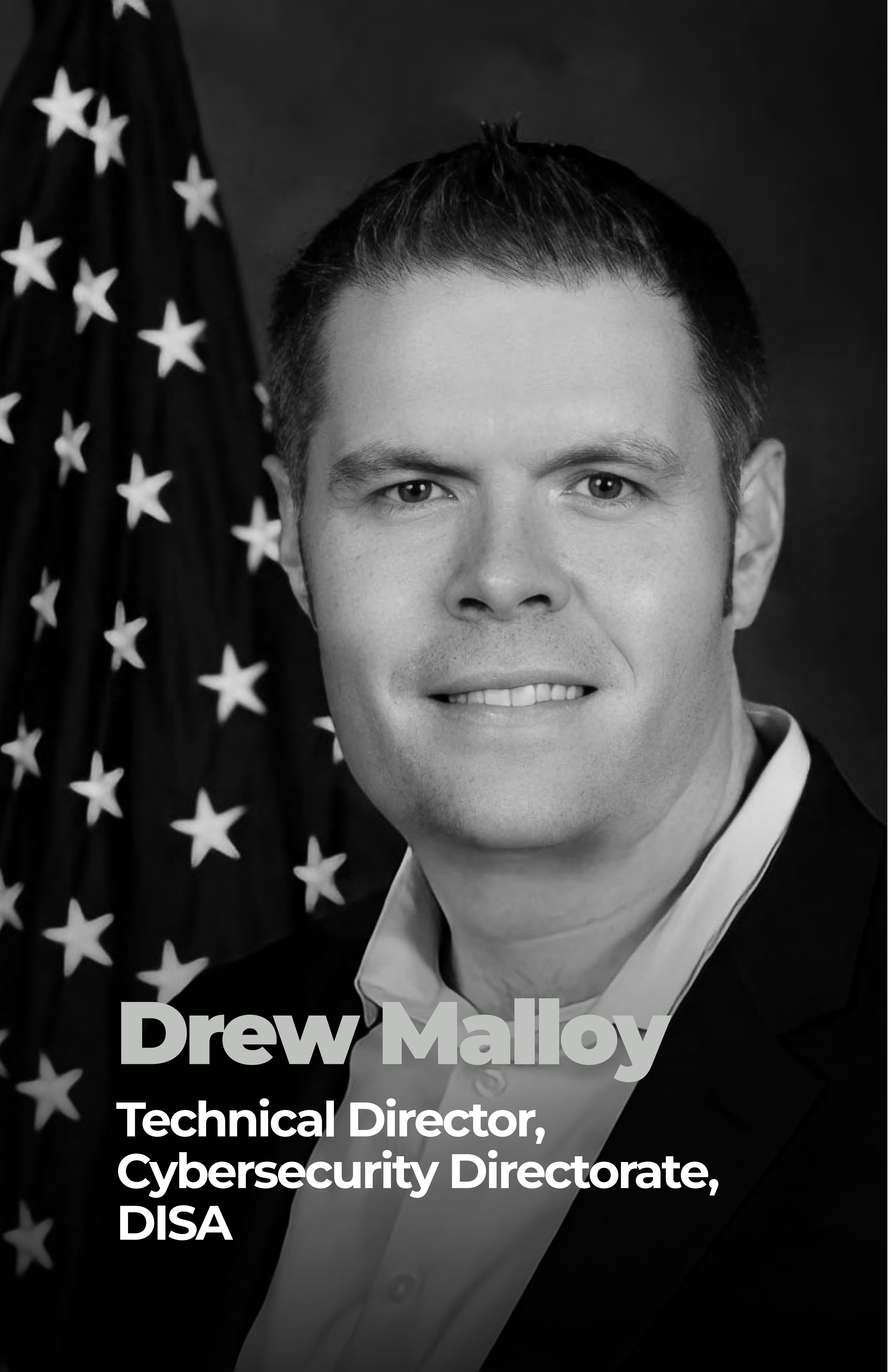
"As a department, we have a pretty consistent track record of not agreeing on what one single solution is. So we wanted to operate with that as a design constraint in mind to say, 'There are going to be other solutions out there. How do we make sure that we work well together?'" Drew Malloy, technical director for the Cyber Development Directorate at DISA, said during a Federal News Network panel. "How do we interoperate ... how do we make sure that we aren't isolating ourselves and having to stand up duplicative systems in order to achieve the same goal?"

DISA awarded the $7 million Thunderdome zero trust prototype contract to Booz Allen Hamilton in January 2022, initially setting a six-month project completion timeline. The war in Ukraine highlighted the need for the Defense Department (DOD) to develop a cybersecurity solution for a modernized classified network, which prompted DISA to extend the pilot by six more months to include a zero trust prototype for the DOD's classified network, SIPRNet.

As DISA integrates these innovative solutions, the agency hopes to address concerns such as out-of-date data standards or solutions not working well with other third-party security systems.

(ctd.)

Photo credit: Petty Officer 2nd Class Jesse Hyatt/DVIDS



Drew Malloy

Technical Director, Cybersecurity Directorate, DISA

"When you look at what we're trying to do, from an end-to-end security mindset around zero trust, you really want to have those integrations out of the box with those security tools to make sure that everything is working in a consolidated fashion," Malloy said. "And right now … we're carrying some risks around the fact that some of these solutions aren't working well together."

Thunderdome's ultimate goal is enabling military service members and civilian employees to access the services they need securely. Successful implementation includes figuring out how many sites DISA will have, how to manage them and what the provisioning or sustainment will look like.

DISA is also working on the messaging around how to engage both the user community, the security applications and data owners.

"We can put out a lot of these capabilities that … are centered around zero trust, but until folks adopt them, especially from an application perspective — talking about how do you look at what you do for access control currently and how can you take advantage of what's being given to you by this SASE solution to make better decisions based off of the different parts of your application and or the data within your application," Malloy said. "We've put a lot of enabling technologies out there, but we aren't taking as much advantage of it as we can. So that's part of our efforts as well."

“As a department, we have a pretty consistent track record of not agreeing on what one single solution is. So we wanted to operate with that as a design constraint in mind to say, ‘There are going to be other solutions out there. How do we make sure that we work well together?’”

— Drew Malloy, Technical Director, Cybersecurity Directorate, DISA