

JULY 2024



DeepDives

Meeting

# ZERO TRUST GOALS

in **Government**

## INSIDE:

- Culture Shifts in Government for Identity Management ..... 3
- New Zero Trust Overlays at Defense ..... 6
- Zero Trust as a Change Agent for Tech ..... 7
- Clearer Standards for ZT Implementation ..... 11

SPONSORED BY



# From the editor's desk



Ross Gianfortune, Managing Editor

## Zero Trust is a Needed Shift for Agencies

The government's zero-trust implementation goals require large shifts in culture, standards and systems. First outlined in the 2021 Biden administration cybersecurity executive order, the goals require agencies to adopt zero trust capabilities, technologies, solutions and processes.

Adjusting to zero trust means that big changes are in store for agencies. Livermore National Laboratory and White House officials highlighted the difficulties in making large cultural adjustments to implement zero trust in line with administration goals. Technology and people need to work in concert to hit the mile markers established by the White House, they said.

The Defense Department's 400-page overlays document outlines a

guide for the agency and its components to implement zero trust. The plan sits on seven DOD pillars to ensure a standard execution.

DOD's Zero Trust Portfolio Management Office is trying to make it easier for department components to enact zero trust. Randy Resnick, the head of the office, said that his team is clarifying standards for implementation. Resnick noted that zero trust plans need to have defined roles, with no "gaps" or "gray areas" of responsibility.

Emphasizing the importance of zero trust security in the face of ongoing cyber threats requires huge shifts at agencies. It won't be small. As Resnick has said, agencies "need to understand what they're working with, need to write policies and rules to do it correctly." 🌸

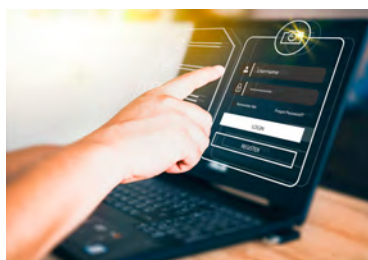
# Table of Contents



Harrison Deitz,  
Staff Writer Intern



Jordan McDonald,  
Staff Writer



ARTICLE

## **It Takes Shifting Culture to Institute Zero Trust in Government**

Federal officials say that priorities in identity management are critical to cybersecurity, but it requires a mindset shift

BY HARRISON DEITZ



INFOGRAPHIC

## **Pillars of Zero Trust Overlays at Defense**

In June, the Defense Department updated its zero trust overlays to clarify plans throughout the department. The agency's zero-trust implementation plan is partially defined by seven DOD pillars to ensure a standard execution. The pillars provide the foundational areas for the DOD's zero-trust models and architectures.



PARTNER INTERVIEW

## **Zero Trust is a Catalyst for Technology Change**

Agencies are establishing leadership in zero trust strategy and policy amid mandates and modernization plans.

**Sean Connelly, Executive Director, Global Zero Trust Strategy and Policy, Zscaler**



ARTICLE

## **DOD Zero Trust Chief: Implementation Requires Clearer Standards**

Randy Resnick, director of the DOD Zero Trust Portfolio Management Office, announced an upcoming memo to eliminate ambiguity on its zero-trust guidelines.

BY JORDAN MCDONALD

## It Takes Shifting Culture to Institute Zero Trust in Government

Federal officials say that priorities in identity management are critical to cybersecurity, but it requires a mindset shift.

BY HARRISON DEITZ

Successful implementation of zero-trust cybersecurity strategies in government requires a significant cultural and systemic shift.

“[It’s like] an immune infrastructure, kind of like the way the human body works, understanding those networks, keeping the adversary out once they get in ... and then operate to compromise,” Lawrence Livermore National Laboratory (LLNL) Principal Associate Director for Global Security Huban Gowadia said at the RSA Conference in May. “All that begins with a sound cybersecurity culture.”

Former Federal CISO and Deputy National Cyber Director Chris DeRusha said that agencies will struggle without implementing zero trust, especially as teams continue to develop vulnerable applications at a rapid pace.

“You’re just going to keep being victim and you have too many holes — too many ways in,” he said.

Building a workforce that is comfortable with zero trust, identity management and other critical cybersecurity concepts are a huge part of building a more secure culture at agencies, Gowadia said. That shift, she added, is already underway.

“In the National Laboratory system today, more than 50% of us have been in the system less than five years, which is an incredible generational shift,”



Gowadia said. “I’d like to believe that a generational shift brings with it so much innate sense of cyber systems and cybersecurity. I’d like to believe that we have a shot at building a whole new culture based on a whole workforce generation that’s coming in.”

Adopting a “trust nothing” approach addresses concerns, preventing



**Huban Gowadia**  
Principal Associate Director for  
Global Security, Lawrence Livermore  
National Laboratory

vulnerabilities from being exposed by systematically reviewing and understanding the risks introduced to large environments. Culture and legacy systems make this hard to implement, according to DeRusha.

“It’s a complete re-architecture across all these different pillars, and it’s a completely different way of working,” he said. “It can be pretty scary to make that change because you’re going to potentially break some of your applications, which may be delivering critical services to hundreds of thousands of citizens.”

The White House’s plans for zero-trust implementation have made it so agencies need to think about cybersecurity in different and more immediate ways, Gowadia noted, and zero-trust implementation is a key part of the administration’s executive plans.

“I think we all felt that sense of urgency,” Gowadia said. “You see it reflected in the zero-trust strategy document. You see it in some of the timelines stipulated in the [White House Cybersecurity Executive Order] and the strategy document.”

According to DeRusha, the goal is not to flip a switch, but to set benchmarks for progress.

“A lot of it for us is getting people ready and having them do the activities that are necessary precursors to making progress anywhere,” he said. “We just try to knock over a bunch of barriers in the meantime with finally getting towards phishing-resistant multi-factor authentication everywhere and ensuring that we are getting to our high-value assets. But if you don’t have categorization of your high-value assets, your crown jewels, you can’t even do that.” ✨

**“I’d like to believe  
that we have a shot at  
building a whole new  
culture based on a whole  
workforce generation  
that’s coming in.”**

**— Huban Gowadia, Principal Associate Director for Global Security,  
Lawrence Livermore National Laboratory**

## Pillars of Zero Trust Overlays at Defense

In June, the Defense Department updated its zero trust overlays to clarify plans throughout the department. The agency's zero-trust implementation plan is partially defined by seven DOD pillars to ensure a standard execution. The pillars provide the foundational areas for the DOD's zero-trust models and architectures. According to DOD, all capabilities within the pillars must work together to effectively secure the data pillar, central to the model.



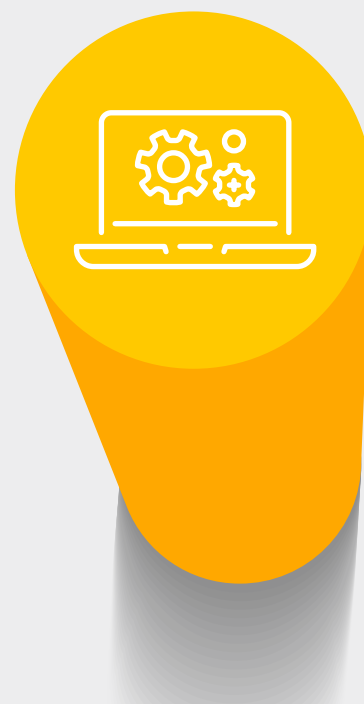
### USER

Continuously authenticate, access and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.



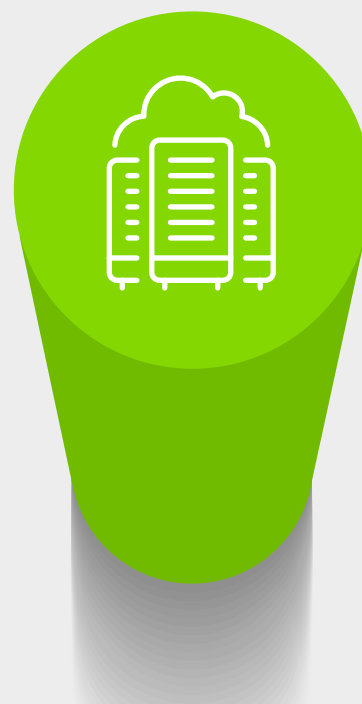
### DEVICE

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.



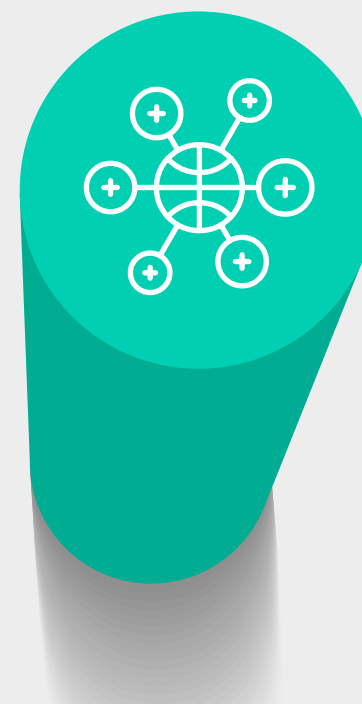
### APPLICATIONS AND WORKLOAD

Secure everything from applications to hypervisors, including the protection of containers and virtual machines.



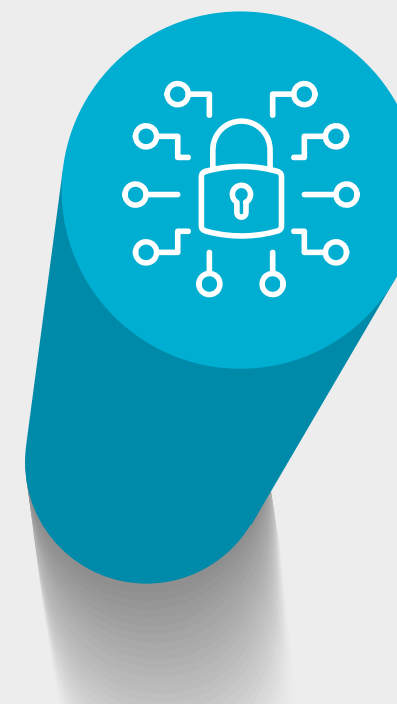
### DATA

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption and data tagging.



### NETWORK AND ENVIRONMENT

Segment, isolate, and control the network environment with dynamic, granular policy and access controls.



### AUTOMATION AND ORCHESTRATION

Automated security response based on defined processes and security policies enabled by artificial intelligence (e.g., blocking actions or forcing remediation based on intelligent decisions).



### VISIBILITY & ANALYTICS

Analyze events, activities, and behaviors to derive context and apply AI/machine learning to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.



# Zero Trust is a Catalyst for Technology Change

Agencies are establishing leadership in zero trust strategy and policy amid mandates and modernization plans.

## How is government successfully implementing zero trust?

**Connelly** Implementing zero trust can lead to many benefits for agencies and help them better serve their users, constituents and partners.

A prime example is at the General Services Administration (GSA), where CISO Bo Berlas recently spoke about the success of the agency's zero-trust journey. He said the agency leveraged a \$29.8 million award from the Technology Modernization Fund to develop and implement a comprehensive zero trust implementation plan.

The team focused on three key pillars of zero trust: users, devices and networks. GSA had a legacy networking solution leveraging a managed provider's trusted internet connections (TICs) and was able to upgrade to a secure access service edge (SASE) solution and enhance the security of its Building Systems Network.

Berlas said the agency is now fully deployed in SASE and disconnected from the TIC routing architecture. This resulted in cost savings that have been reapportioned to higher security needs, he said. It also resulted in faster



**Sean Connelly**  
Executive Director,  
Global Zero Trust Strategy  
and Policy, Zscaler



internet, improved security controls, improved user experience and reduced complexity.

This implementation of an optimized zero trust strategy shows that agencies can realize benefits by effectively meeting directives set forth in the White House's mandate.

### What are some of the challenges or lessons learned so far in federal zero trust implementation?

**Connelly** Implementing zero trust strategies has forced agency IT and cybersecurity leaders to have new discussions with other offices and teams about their security needs.

Those seeing successes with implementing zero trust have established a zero-trust office or administrator to devote time working with each of the system or mission owners within the agency.


These discussions typically begin by helping the system and mission owners break down zero trust principles. By implementing zero trust, and verifying the users, securing their devices and modernizing their networks and applications, the owners can focus on delivering better service without the risks of damaging attacks that compromise data.

Zero trust has a large focus on changing technology, of course, but it's more about improving human interaction and accelerating confidence among teams. (ctd.)

**“Zero trust has a large focus on changing technology, of course, but it’s more about improving human interaction and accelerating confidence among teams.”**

**— Sean Connelly, Executive Director,  
Global Zero Trust Strategy and Policy, Zscaler**



 **How do you see federal zero trust initiatives evolving over the next few years? How should agencies start to plan and prepare?**


**Connelly** Now that we are approaching the two-year anniversary of the Office of Management and Budget’s zero trust memo, agencies are approaching the window where they need to report back to the White House about where they are in their zero trust plans. This includes looking at their endpoint detection systems, their identity management platform and what types of users need to have extra security.

Government will probably be considering more solutions to go to the cloud or to be more zero-trust compliant. Some might also look at moving toward more SASE platforms and moving away from old firewall solutions.

Leading up to reporting on this progress, agencies will have to evaluate

their migration strategy to see where they are on the continuum from where they started to what their systems will look like when they are fully compliant with requirements.

Key to this will be having to understand that modernization is about adding new value. The push to zero trust has offered agencies a chance to reevaluate how they modernize, including how they deliver their mission and services. There are tangible benefits to improved service delivery that will make a difference in the lives of citizens.

What is often overlooked is that federal IT systems were typically considered to be behind the state-of-the-art of commercial organizations or other governmental partners in state and local governments. But the federal government has established a leadership position in zero trust strategy and policy and has moved to modernize in ways that are now being emulated by these partners. 



# ZERO TRUST + AI

Protect your agency with the most accredited security cloud in the world. FedRAMP Moderate and High, DoD IL5 and StateRAMP authorized.

- Protect data from cyberthreats
- Reduce IT cost and complexity
- Improve user experience
- Meet mandates with confidence

Learn more at  
[zscaler.com/federal](https://zscaler.com/federal)

# DOD Zero Trust Chief: Implementation Requires Clearer Standards

Randy Resnick, director of the DOD Zero Trust Portfolio Management Office, announced an upcoming memo to eliminate ambiguity on its zero-trust guidelines.

BY JORDAN MCDONALD

The Defense Department Zero Trust Portfolio Management Office is developing new language to eliminate ambiguity in zero-trust implementation standards and protocols, Randy Resnick, director of the DOD Zero Trust Portfolio Management Office, said at AFCEA TechNet Cyber in Baltimore in June.

“We wrote a [directive type memo], if it’s not out, it’s going to be out very, very soon,” Resnick said. “You will see language in it that makes it very clear what the portfolio office capabilities are and the power that we have over telling the department just how to do things in terms of policy deadlines and such. It also clearly outlines what ... the agency’s roles and responsibilities are for zero trust.”

Resnick said that the his office will release the document soon. The memo will define roles and responsibilities for zero trust in the department and eliminate “gaps” and “gray areas.”

As zero trust becomes standard for agencies like DOD, the change in posture is creating a knock-on effect for the country’s partners and allies as well. Resnick said that the department’s zero trust work inadvertently influenced other countries’ policies.

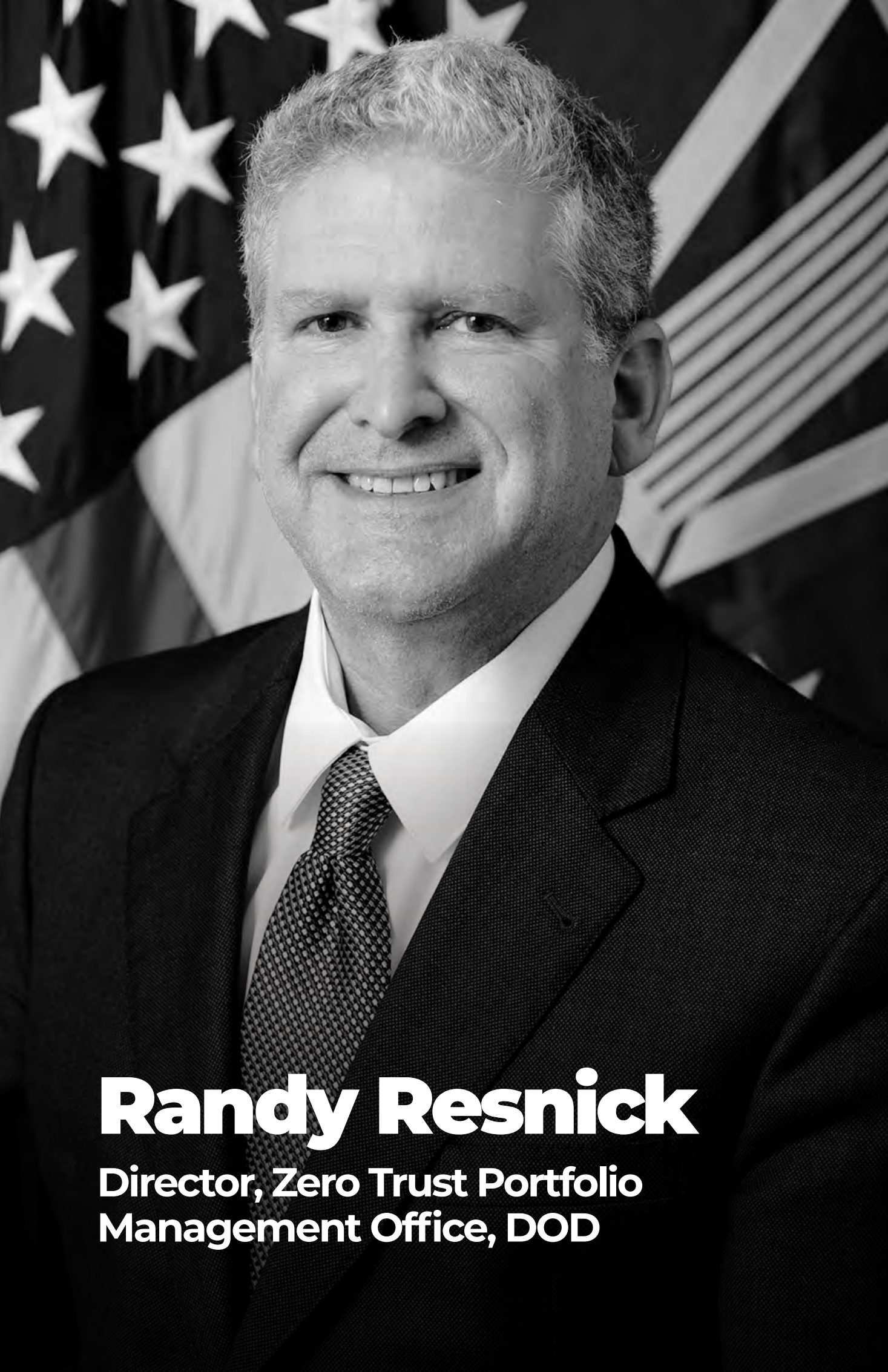
“Our allies are now following, thinking — plagiarizing — the way we do zero trust in the Department of Defense. You’ll see it within their documents,” he said. “Instead of the blood, sweat and tears of five years of [zero trust] before the portfolio



office started back at NSA, they jumped right to the solution and they accepted our hard work in the department, and they said, ‘This looks pretty good to us.’”

Though international partners might have reasons for not fully implementing the DOD zero-trust strategy, Resnick added, they take portions and develop it for their own use.

Despite this adoption, Resnick said there are still gaps in training that he



**Randy Resnick**  
Director, Zero Trust Portfolio  
Management Office, DOD

hopes industry can fill.

“There’s a role for industry to play. Industry has all kinds of training and all kinds of other things in network security, cybersecurity, and yet I still see a little gap in zero trust,” Resnick said. “I’m encouraging industry not to stand by but to actually be aggressive here, and to actually come up with zero trust training. Because, I assure you, once the training exists, they’re not going to take all the online classes only from [Defense Acquisition University] and you’re going to have a ready market for zero-trust training at whatever level, from 101 to 401 on zero trust.”

According to Resnick, the Zero Trust Portfolio Management Office is using innovative techniques to improve zero trust across the agency. This includes what he called “purple teaming,” an exercise in which red and blue teams fight and shift with each other in attacking and defending systems within a simulated environment.

To Resnick, exercises like purple teaming are critical to getting everyone speaking the same language and understanding DOD requirements when it comes to zero trust and cybersecurity.

“Right now we see that there’s no repeatable process. This is a problem. We said in the past that we really don’t know how a component gets to zero trust just as long as they get to target, but it really didn’t address the DevSecOps part of what the vendors are doing in order to keep them in the spirit of the best principles that we can think of, and have it done repeatedly so that when we go and ‘purple team’ them, we have a higher assurance that has been designed correctly,” Resnick said.

While changing the culture surrounding zero trust is critical to the health of the department, Resnick said that an employed “permafrost” is likely to never fully embrace new cybersecurity principles. Waiting them out is more likely than shifting their workflow, he added.

“We have a bigger burden of figuring out how to explain zero trust and its

fundamentals and to actually get through the culture inertia that exists in the department,” Resnick said. “The only people that push back are what I would call the middle layer, the permafrost, as we jokingly say, that is frozen in time. They feel threatened because they’re doing the old style of cybersecurity. I did it

myself. I totally understand. But these people, if they haven’t learned now, they’re never going to learn. And so I truly believe it’s a generational thing. We’re going to have to wait until they retire out, and so you won’t see this problem in another 10 years.” ❁

**“There’s a role for industry to play. Industry has all kinds of training and all kinds of other things in network security, cybersecurity, and yet I still see a little gap in zero trust.”**

**—Randy Resnick, Director,  
Zero Trust Portfolio Management Office, DOD**