

The **FUTURE**

of

Implementing

ZERO TRUST

INSIDE:

- The Pentagon's Next Steps in Zero Trust Application 3
- Infographic: The Pillars of CISA's Zero Trust Maturity Model 6
- Navy Leaders Connect Security with CJADC2 11
- Aligning the White House and CISA on Zero Trust 12

SPONSORED BY

FORTINET
FEDERAL[®]



From the editor's desk



Ross Gianfortune, Managing Editor

Zero-Trust Architecture Will Mean Stronger Defenses

Agencies throughout the federal government need to secure networks, data and systems. Modernizing systems means embracing zero trust as a security model. The continual vetting of access is crucial to cybersecurity operations, though the Cybersecurity and Infrastructure Security Agency notes that adopting zero trust may require a change in an organizations' philosophy and culture. CISA updated its Zero Trust Maturity Model this year to help agencies in implementation.

Zero trust works in concert with modernization for many

agencies. At the Navy, for example, identity management and verification will be critical to making sure data access is secure. At the same time, the Pentagon writ large is targeting zero trust adoption by 2027 as it faces the challenging reality of shifting away from a perimeter-based security model.


Zero trust implementation is ongoing, but necessary because it will make agencies better equipped to deal with threats. As DOD Senior Information Security Officer David McKeown noted, "The act of defenses will get stronger because we're going to log everything." 

Table of Contents



Anastasia Obis
Staff Writer/
Researcher



Jordan McDonald
Staff Writer/
Researcher

ARTICLE

Pentagon Eyes Next Step in Zero Trust Implementation

The Defense Department is reviewing zero-trust implementation plans from the services.

BY ANASTASIA OBIS

ARTICLE

Zero Trust Synonymous with CJADC2 Operations, Navy Leaders Say

The military's integration of systems under the CJADC2 umbrella will require stronger zero-trust measures.

BY JORDAN MCDONALD

INFOGRAPHIC

The Four Pillars of CISA's Zero Trust Maturity Model Version 2.0

Released in April, version 2.0 of the model is one path that an agency can take in implementing a transition to zero trust.

PARTNER INTERVIEW

Deploy Zero Trust Architecture to Secure Systems

Zero Trust Network Access can help prioritize and ensure greater protection of high-value assets.

William (Bill) Lemons, Director, Solutions Architecture, Fortinet Federal

ARTICLE

CISA Updates Zero Trust Maturity Model to Align with White House Directives

CISA's updated guidance provides more technical depth across the five pillars of zero trust and adds a new maturity stage.

BY ANASTASIA OBIS

Pentagon Eyes Next Step in Zero Trust Implementation

The Defense Department is reviewing zero-trust implementation plans from the services.

BY ANASTASIA OBIS

The Defense Department (DOD) is working on its zero trust overlay for the National Institute of Standards and Technology (NIST) 800-53, which will complete the full set of documentation the Pentagon is required to provide to help the enterprise implement zero trust architecture.

DOD already released its zero trust strategy and reference architecture to guide the military departments and Fourth Estate working toward 2027 zero trust target levels.

“Target level for us means being able to stop the adversary. There’s a lot of science that goes behind how we define our activity level and our capability level,” Randy Resnick, director of DOD’s Zero Trust Portfolio Management Office, said at a conference in May 2023. “A lot of it has to do with a lot of other information not found on classified networks that made us develop the definition the way we did.”



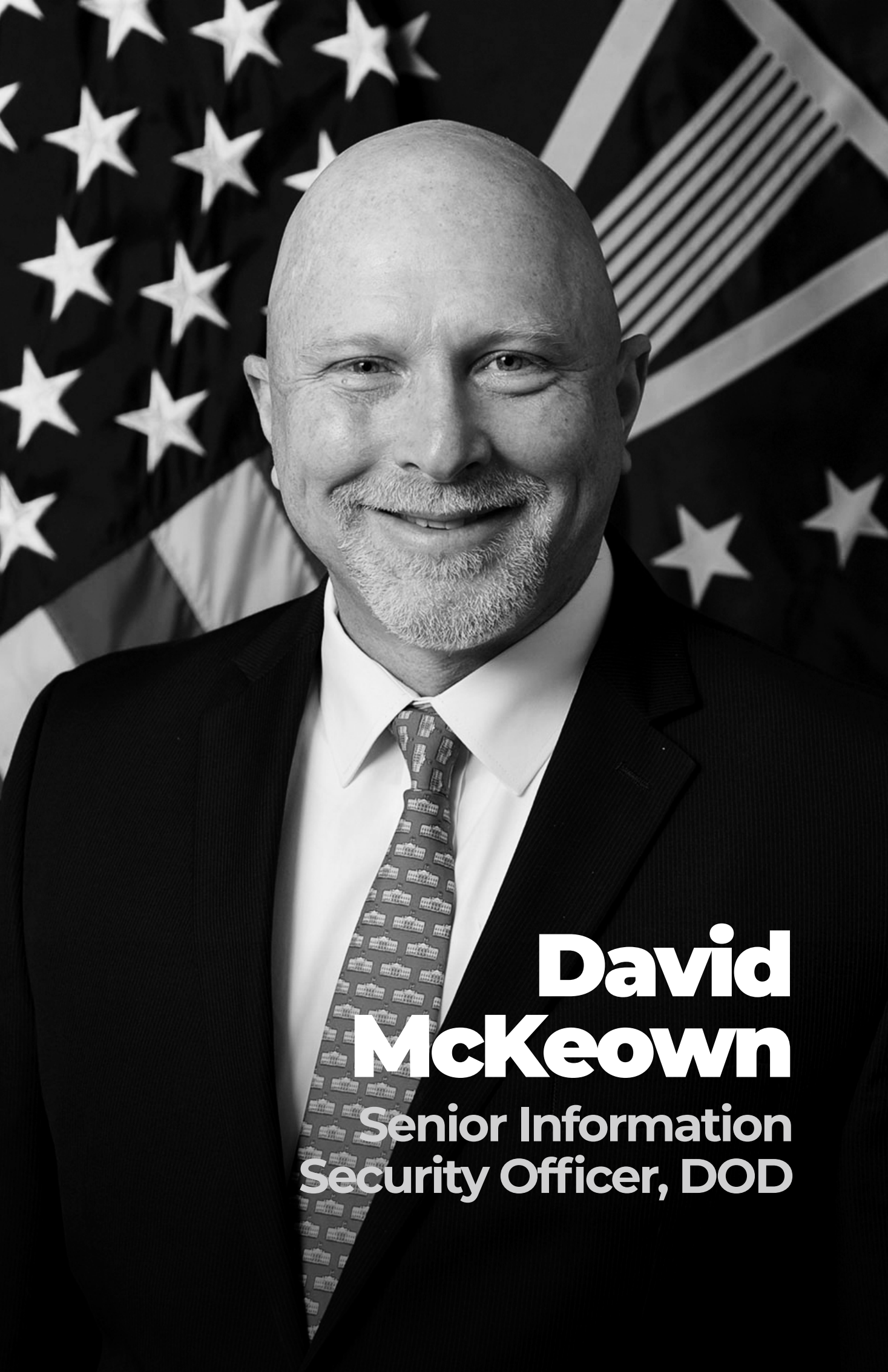
DOD CIO John Sherman said department-wide zero trust implementation is currently one of his highest priorities. He identified three approaches the services are able to choose from to go after implementing the zero-trust framework.

“We’ve also laid out our strategy, kind of a pick-your-own adventure. Folks may remember those books are a little like ‘Do you slay the dragon? Or do you go into the cave,’” Sherman told GovCIO Media & Research in an on-site

podcast interview at TechNet Cyber 2023.

One is the Brownfield approach, where the military services can build capabilities over their existing infrastructure. Or, they can leverage the Joint Warfighting Cloud Capability (JWCC) contract and rely on commercial zero trust solutions offered by the JWCC awardees: Amazon Web Services (AWS), Google, Microsoft and Oracle. The third route is through private cloud adoption.

Ensuring successful implementation of the zero trust framework does not



**David
McKeown**
Senior Information
Security Officer, DOD

just require an IT fix, but also policies, training and doctrine.

Three zero trust courses are available for military service members and civilian employees, and DOD is “seriously” considering mandating the course.

“You have to remember that people that are going to be installing zero trust need to understand what they’re working with, need to write policies and rules to do it correctly. That requires training,” Resnick said.

Resnick’s office is currently reviewing submitted implementation plans from the services that he estimates will take through the rest of 2023. Resnick said the journey will be long and arduous, and DOD will work component by component to implement the architecture and meet the deadlines outlined in the zero trust strategy. While funding is essential in this effort, successful implementation also means staying on schedule and ensuring interoperability between cybersecurity services and solutions for an effective zero trust model.

“We really want to see multiple vendor integrations. Not one vendor is going to solve this problem. We want to see interoperability, we also want to see API security. And lastly ... applications ... they need to be written to be aware of their ZTE (zero trust edge) surroundings going forward. It needs to be aware of ICAM systems, it needs to be able to take some ins and outs of rules and policies. This is what I’m talking about being ZTE-aware,” Resnick said.

Scaling zero trust will require automation.

“The act of defenses will get stronger because we’re going to log everything. We’re going to have analytics over those logs, we’re going to do automation of responses versus a human in the loop. So that piece of it is big,” said DOD Senior Information Security Officer David McKeown.

Lt. Gen. Maria Barrett, commanding general of U.S. Army Cyber Command, emphasized the importance of automation in the cybersecurity process so as to continuously verify and identify for unusual or suspicious activity.

“We fly planes on autopilot, we land them on autopilot. This is not scary to run a network in an automated way,” Barrett said. (ctd.)

“The act of defenses will get stronger because we’re going to log everything. We’re going to have analytics over those logs, we’re going to do automation of responses versus a human in the loop.”

**—David McKeown,
Senior Information
Security Officer, DOD**

Sherman said the zero trust approach might have prevented the recent leak of classified documents containing sensitive information about the ongoing Russia-Ukraine war.

“As you look at those seven pillars of zero trust, you have pillar number seven: visibility and analytics, other pillars automation and orchestration... Bringing all this together to prevent somebody, whether it’s external or internal, from moving laterally across the network, getting to data, not the system, but the data they’re not supposed to have access to, that’s what zero trust is really about,” Sherman said. ❁

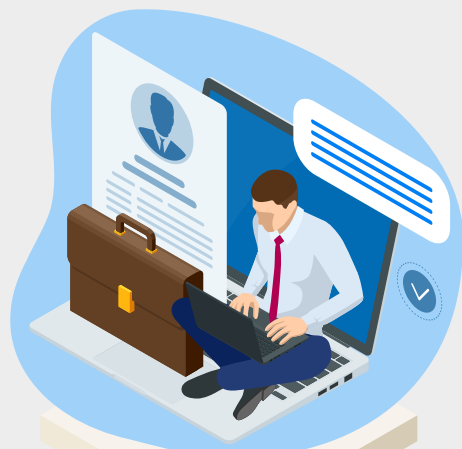
The Four Pillars of CISA's Zero Trust Maturity Model Version 2.0

The Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model provides an approach to achieve strong modernization efforts related to zero trust within an evolving landscape. Released in April, version 2.0 of the model is one path that an agency can take in implementing a transition to zero trust architecture.

1

IDENTITY

Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access.



2

NETWORKS

Shift away from traditional perimeter-focused approaches to security. Enable agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity and enhance enterprise-wide network visibility.



3

APPLICATIONS AND WORKLOADS

Agencies should manage and secure their deployed applications and should ensure secure application delivery. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats.



4

DATA

Agency data should be protected on devices, in applications and on networks in accordance with federal requirements. Agencies should inventory, categorize, and label data; protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration.






**FORTINET
FEDERAL®**

Deploy Zero Trust Architectures to Secure Systems

Zero Trust Network Access can help prioritize and ensure greater protection of high-value assets.

 **What are the difficulties in implementing compliant zero trust architectures and how are agencies working around these obstacles?**

Lemons As agencies move toward zero trust operational environments, a significant challenge is the thoughtful development of a comprehensive implementation plan that results in an architecture that not only improves the overall security posture of the organization, but also creates practical and effective user experiences. Effective plans are based on an understanding of all asset locations and how users need to access them, as well as details of the IT and security architectures in place and how the organization can leverage common resources across the environment. If the user experience is not carefully considered, users may resist adoption and/or work around imposed system access restrictions. (ctd.)

William (Bill) Lemons,
Director, Solutions Architecture,
Fortinet Federal




“Zero Trust Network Access provides additional real-time threat intelligence to inform security operations staff about unauthorized intrusion attempts.”

**William (Bill) Lemons,
Director, Solutions
Architecture, Fortinet Federal**


 **How can Zero Trust Network Access (ZTNA) help U.S. government agencies improve their cybersecurity operations and management?**

Lemons ZTNA allows agencies to take a step toward zero trust architecture (ZTA) while minimizing the effort to start an enterprise-wide zero trust architecture implementation. Implementation of ZTNA does not require a wholesale change to an agency's IT architecture and can be used to augment VPN access solutions. The focus of ZTNA is to constrain user access and ensure continual monitoring of user behavior by providing additional information about each user's identity, device and network access permissions. In this way, ZTNA helps system administrators ensure that specific users should or should not be granted access to particular applications, data and other network resources.

 **How does ZTNA allow system administrators and users to migrate away from traditional VPN tunnels that allow unrestricted network access?**


Lemons Many agencies still rely on VPNs that may allow broad access to network devices with few restrictions, an approach that does NOT align with the “least privilege” concept required by ZTA. ZTNA provides system administrators with the tools to implement a finer-grained approach to ensuring specific resources are scrutinized over time. Some solutions today can effectively coexist with VPN gateways already in place which are familiar to users, allowing for a smooth and gradual transition away from traditional VPNs to a ZTNA environment. In short, ZTNA provides a means to be specific about how an organization chooses to guard its resources, enabling system administrators to prioritize and ensure greater protection of high-value assets.

(ctd.)

 **Can a user tell whether the system administrator has fenced off a particular asset for ZTNA limitations or is it transparent to the user?**

Lemons With a focus on improving the user experience, it is possible to make ZTNA mostly transparent for authorized users. In addition, ZTNA can be used to obscure the identity of a resource from those who may gain access to a specific data set, application or other network asset. This flexible implementation approach provides system administrators with information on access denials while masking the denial from the user. In this way, ZTNA provides additional real-time threat intelligence to inform security operations staff about unauthorized intrusion attempts—without informing, confirming or denying any unauthorized user that their actions were monitored.

 **Give us an overview of how zero trust strategies will enable a U.S. government organization to converge networking, security and access in an integrated and resilient solution?**

Lemons The convergence of networking, security, and access is a significant driver for agencies as they move towards zero trust environments. Agencies can use this transition as an opportunity to evaluate all components of their IT architectures and make thoughtful decisions about how to leverage zero trust architecture implementation to secure and simplify their IT operations. We recommend that agency professionals look for proven platforms that deliver interoperability and support multi-vendor solutions; flexibility; and increased capabilities to grow and change with the environment. 





Start the Journey to Zero Trust with Zero Trust Network Access

Continuous, validated and
secure access.
Everywhere you need it.

[LEARN MORE](#)



Zero Trust Synonymous with CJADC2 Operations, Navy Leaders Say

The military’s integration of systems under the CJADC2 umbrella will require stronger zero-trust measures.

BY JORDAN MCDONALD

As the U.S. military edges closer to its goal of a united CJADC2 warfighting concept, ensuring the security of its sensors and systems will be critical. The military has adopted a zero-trust approach to cybersecurity in the warfighting space, which enables forces to securely communicate and share data.

Zero-trust systems, like CJADC2, is not a single solution, but a collection of cybersecurity capabilities that enable commanders to make better decisions in the field.

The comment came from Navy Director of Enterprise Networks and Cybersecurity (OPNAC N2N6D) Scott St. Pierre, who spoke on a recent panel.

St. Pierre said the Defense Department must move away from the trusted environments of the 1960s and 1970s and toward an environment where each person’s clearance and access to secure information is verified. St. Pierre added that cybersecurity can’t be an afterthought, but rather needs to be at the forefront of any military system.

Identity management and verification are “key to the whole cybersecurity strategy in accordance with zero trust, not only for those identifying parameters and verifications, but more importantly to help enable the right people with the right clearances to access the correct data at the right time,” said Mark Wiggins, vice president of defense, intelligence and systems integrators at Fortinet Federal.

St. Pierre said it’s critical that a broader perspective is taken at the enclave-



and platform-level because JADC2 and zero trust are “synonymous.” He said that when cybersecurity is integrated with command and control systems, combat effectiveness is also improved.

For more on this, check out the full GovFocus panel “Zero Trust Enabling the Future Joint Force” available now. <https://governmentciomedia.com/govfocus/zero-trust-enabling-future-joint-force> 🌟

CISA Updates Zero Trust Maturity Model to Align with White House Directives

CISA's updated guidance provides more technical depth across the five pillars of zero trust and adds a new maturity stage.

BY ANASTASIA OBIS

After two years, the Cybersecurity and Infrastructure Security Agency (CISA) published an updated Zero Trust Maturity Model introducing significant changes to the initial document released in 2021.

The biggest changes to the updated version are aligned with the memorandum released by The Office of Management and Budget (OMB) establishing the federal zero trust architecture strategy and requiring agencies across the federal government to meet certain zero trust objectives by 2024.

"I would say that this has been one of the most remarkable times I've seen where you have CISA, the Office of Management Budget and the agencies having really fundamental discussions about their plans, about their budgets and making sure that priority is given to cybersecurity and not as an afterthought," John Simms, CISA's senior technical advisor, told GovCIO Media



& Research. "I think this is probably one of the first times I've seen where that discussion is very transparent and honest in terms of what it actually will take to implement the executive order and secure agency environments."

For more than two decades, federal agencies relied on a perimeter security model to protect their enterprise data. The biggest challenge now is shifting away from the existing infrastructure built on implicit trust and align with zero trust principles.

Recognizing that federal agencies are starting the transition from different points, the updated version adds an "initial" stage to the existing traditional, advanced and optimal stages to enable an easier transition for the agencies in their shift to zero trust architecture. The idea is that agencies can take gradual steps across the five pillars of zero trust that include identity, devices, networks, applications and workloads, and data to reach a state where an agency is at an optimal stage across all five pillars of zero trust.

John Simms

CISA Senior
Technical
Advisor



One of the key concepts of zero trust is to treat the agency network as a hostile network, and one of the OMB memorandum's requirements for the agencies was to expose at least one moderate system to the internet.

"What that required agencies to do was think about what the architecture would need to be, and what the capabilities would need to be ... to protect that system," Simms said. "We had a number of discussions with agencies about ... what the real intent of that was, and the real intent behind that task was to provide agencies with an opportunity to gain confidence in their ability to provide that level of security on an application workload to gain confidence to ensure that would withstand any type of attacks or malicious use."

After releasing the initial Zero Trust Maturity Model version, CISA went into a request-for-comment period and received roughly 375 comments, with each pillar receiving between 50 to 100 different comments about how to further expand on the content provided in the initial version. The comments CISA received came from agencies and trade associations, but the most significant portion of comments came from the vendor community.

"They were at about 70% of the comments that came back, which is great because it gave us a chance to ... get their insights and perspectives in terms of some of the concepts that were a little raw in our initial version of the maturity model," Simms said. "Some things we expected, given that we put it together very quickly ... we knew we would get a lot of comments about adding depth in technical areas. And really looking at how we could structure the capabilities across the different pillars."

OMB released FISMA metrics for fiscal year 2023, but there is no exact number on where agencies are in the zero trust maturity journey.

"There have been a number of discussions about how long does it take ... I would say in the next year or two, we'll be in a better place in terms of ... understanding how best to measure progress," Simms added. ❁

“What that required agencies to do was think about what the architecture would need to be, and what the capabilities would need to be...to protect that system.”

—John Simms, CISA Senior Technical Advisor