

# ZERO TRUST

## Securing the Supply Chain

### INSIDE:

White House: Secure the Supply Chain.....	3
Zero Trust Will Protect JADC2 Supply Chain .....	10
Software Supply Chain Needs Transparency .....	14

SPONSORED BY

**FORTINET**  
**FEDERAL**<sup>®</sup>





# From the writer's desk



Kate Macri, Deputy Editor

## Zero Trust and Supply Chain Security are the Same

**Y**ou can't have zero trust without supply chain security. Sometimes the cybersecurity community discusses zero trust and supply chain security as two separate disciplines, but they're actually symbiotic.

Zero trust, at its core, assumes all users and devices could be the source of a breach and requires constant verification and assurances to allow data access. Because so many applications, devices, lines of code, users and vendors contribute to an

organization's IT supply chain, zero trust becomes more important than ever to ensure a strong cybersecurity posture throughout all possible access points.

Amid White House executive orders and major software supply chain breaches such as the SolarWinds and Log4j incident, industry and government are coming together to address supply chain security with a zero trust mindset to limit future vulnerabilities and damage when breaches inevitably happen. ✨



# Table of Contents



Kate Macri,  
Deputy Editor



Sarah Sybert,  
Staff Writer

ARTICLE

## **White House Issues New Memo to Secure Supply Chain**

OMB's new supply chain memo calls on agencies to utilize software that has been built following common cybersecurity practices.

BY SARAH SYBERT

INFOGRAPHIC

## **A Software Tree of Materials**

Tracing the Supply Chain to Secure with Zero Trust.

PARTNER INTERVIEW

## **Zero Trust's Role in Supply Chain Management**

**Felipe Fernandez, Sr. Director, Systems Engineering, Fortinet Federal**

Strong ICAM solutions play a crucial role in protecting federal networks.

ARTICLE

## **CISA, DISA are Focusing on Transparency to Secure Supply Chain**

SBOMs and transparency are key to resilient cybersecurity models.

BY SARAH SYBERT

ARTICLE

## **Zero Trust 'Essential' and 'Integral' to JADC2**

DOD leaders say you can't have JADC2 without zero trust and a 'data-centric' approach to cyber.

BY KATE MACRI



## White House Issues New Memo to Secure Supply Chain

OMB's new supply chain memo calls on agencies to utilize software that has been built following common cybersecurity practices.

BY SARAH SYBERT



The Office of Management and Budget (OMB) issued a memo on Enhancing the Security of the Software Supply Chain through Secure Software Development Practices Wednesday. The directive calls for agencies to use software built with common cybersecurity practices.

“With the cyber threats facing federal agencies, our technology must be developed in a way that makes it resilient and secure, ensuring the delivery of critical services to the American people while protecting the data of the American public and guarding against foreign adversaries,” Federal CISO and Deputy National Cyber Director Chris DeRusha said in a briefing.

The memo was issued under President Biden’s May 2021 cybersecurity executive order that aims to identify, deter, protect against, detect and respond to cybersecurity threats.

The rule will require federal agencies to use a standardized self-attestation

form consistent with the National Institute of Standards and Technology (NIST) Software Supply Chain Security Guidance before using a vendor’s software. Agencies must use the form for all third-party software, including software renewals and major version changes.

“By strengthening our software supply chain through secure software development practices, we are building on the Biden-Harris Administration’s efforts to modernize agency cybersecurity practices, including our federal zero trust strategy, improving

our detection and response to threats, and our ability to quickly investigate and recover from cyberattacks,” DeRusha added.

The memo also set new deadlines for federal agencies.

Within 90 days, agencies must inventory all software and create a separate inventory for “critical software.”

Within 120 days, agencies must develop a consistent process for



# Chris DeRusha

Federal CISO and Deputy  
National Cyber Director



communicating relevant requirements and collect letters of attestation from software providers.

Within 180 days, agency CIOs must assess organizational training needs and develop training plans for the review and validation of attestation.

OMB has called on the Cybersecurity and Infrastructure Security Agency (CISA) and the General Services Administration (GSA) to help develop requirements for a central repository for software attestations and artifacts.

“Within 1 year from OMB’s establishment of requirements, CISA, in consultation with GSA and OMB, will establish a program plan for a government-wide repository for software attestations and artifacts with appropriate mechanisms for information protection and sharing among federal agencies,” the memo said.

DeRusha noted that guidance will enable OMB to build trust and transparency across the digital infrastructure and will allow the agency to fulfill its commitment to protect national and economic security.

“[The memo] is part of a larger enterprise cybersecurity and information technology modernization plan that ensures we can deliver a simple, seamless and secure customer experience,” DeRusha said. 🌟

**“With the cyber threats facing federal agencies, our technology must be developed in a way that makes it resilient and secure, ensuring the delivery of critical services to the American people while protecting the data of the American public and guarding against foreign adversaries...”**

**— Chris DeRusha, Federal CISO and Deputy National Cyber Director**

## A Software Tree of Materials

Tracing the Supply Chain to Secure with Zero Trust

1

The software supply chain starts with a single line of code.

2

Coders and software developers house code in open source software libraries, which can be “open source” (aka, free) or commercial (i.e., can be sold for use by other developers).

3

They can then build on that code with software development methodologies, such as DevSecOps, to create applications.

4

Developers can then build on those applications to create new applications that interface with each other and run on hardware (i.e., Microsoft Word or Adobe on a laptop).

5

Coders and developers can then issue software updates to modify the code on an application to address vulnerabilities or improve performance.





# FORTINET FEDERAL®

## Zero Trust's Role in Supply Chain Management

Strong ICAM solutions play a crucial role in protecting federal networks

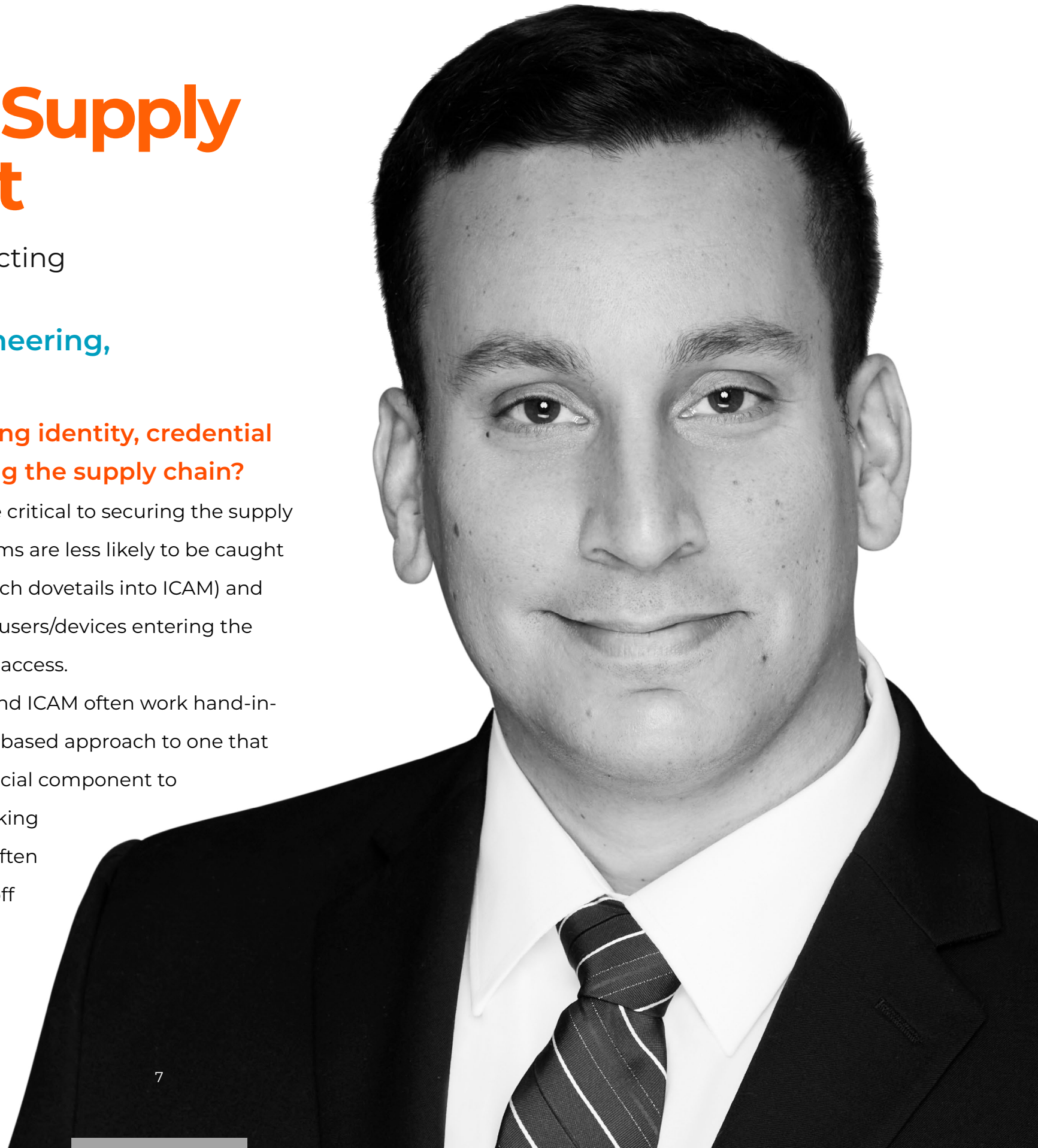
**Felipe Fernandez, Sr. Director, Systems Engineering, Fortinet Federal**

 **What is the importance of zero trust and harnessing identity, credential and access management (ICAM) solutions for securing the supply chain?**

**Fernandez** Zero trust architecture (ZTA) and ICAM solutions are critical to securing the supply chain. By assuming all network activity is a security threat, cyber teams are less likely to be caught by surprise. ZTA integrations like enhanced identity governance (which dovetails into ICAM) and micro segmentation give administrators maximum control over the users/devices entering the network and every protected piece of the network those users try to access.

ICAM plays a similar role in securing supply chains. In fact, ZTA and ICAM often work hand-in-glove. Since zero trust involves moving beyond a network perimeter-based approach to one that requires constant user authentication, identity management is a crucial component to a successful zero trust strategy. This is especially important when talking about supply chains within the federal government since agencies often heavily rely on contractors whose credentials must be turned on or off depending on the project.

 **The increase in cloud-based applications and**





**“In the event of an attack that involves compromised credentials, identity management can provide a roadmap for what went wrong.”**


**— Felipe Fernandez,  
Sr. Director, Systems Engineering,  
Fortinet Federal**

**“internet of things”-connected devices has expanded the attack surface for many organizations. How do identity management services help track and trace the supply chain of user and device activity to mitigate threats and prevent breaches?**

**Fernandez** The increase in cloud-based applications and connected devices has expanded the attack surface, giving cybercriminals more opportunities for targeted attacks. Many of today’s most damaging security breaches have been due to compromised user accounts and passwords exacerbated by groups of users being provided with inappropriate levels of access.

ICAM provides a way to understand every user that moves through the network, preventing them from wandering into restricted areas before an attack can happen rather than trying to identify them once they’ve already breached those areas.

ICAM is just as important for those leaving an organization. Manually de-provisioning access privileges of a former employee can be delayed or even forgotten. Identity management prevents this by automatically de-provisioning access rights once a user leaves the company or as their role within the organization changes.

 **In the event of a breach, how can identity management help organizations locate the source of malware and mitigate the damage?**

**Fernandez** In the event of an attack that involves compromised credentials, identity management can provide a roadmap for what went wrong. Since ICAM solutions track every user’s movement along with the history of the permissions set for each user, cyber teams can run the tape to

(ctd.)



see when and where the attacker was able to take over the identity of the compromised user.


This can also be instructive for mitigating future breaches. As bad as it is to experience an attack, it's even worse to not learn from it. By understanding how the attackers were able to gain access to the network, cyber teams can make sure that vulnerability is patched and not present among other users.

### **How can agencies approach directives and policies around zero trust? What more needs to be done?**

**Fernandez** Agencies should not reinvent the wheel. Taking stock of their inventory or systems and how they're guarded is a good start. That will give an agency a better understanding of their own security posture. We can't move

forward if we don't know where we stand.

Beyond that, it's important for agencies to partner with other organizations both in the public and private sector that have been there before and understand the challenges of deploying a zero trust architecture that fits the government mission.

Smaller agencies can follow the lead of CISA, DoD and DHS, utilizing their battle-tested guidance to understand their own ZTA journeys. And agencies of all sizes should look to private sector security companies for a view of the latest, leading-edge technology and threat intelligence. We all have a huge part to play in securing government networks. No one should have to take on the mammoth task of deploying an effective and efficient zero trust strategy on their own. 



# CISA, DISA are Focusing on Transparency to Secure Supply Chain

SBOMs and transparency are key to resilient cybersecurity models.

BY SARAH SYBERT

Large-scale vulnerabilities discovered in Log4j, SolarWinds and more have prompted federal cybersecurity leaders to “know what’s under the hood” of their applications, leveraging software bills of materials (SBOMs) to drive resiliency and security management.

“Log4j has really taught us that it’s not just enough to say, ‘well, my asset management knows this...’ We need to know what’s under the hood,” CISA Senior Advisor and Strategist Allan Friedman said at the Billington Cybersecurity Summit in Washington, D.C., Thursday. “SBOMs are saying ‘this software depends on this software, depends on this software. It’s a nice little tree. It’s a list of ingredients.’”

SBOMs enable organizations to respond quickly, efficiently and cost effectively, driving cyber resiliency. DISA’s Hosting and Compute Center (HaCC) technical director Korie Seville said his agency is looking at cybersecurity in two parts: vulnerability patching and remediation.

“It’s transforming the way you look at security and transforming the way you look at vulnerability management,” Seville said. “There’s vulnerability patching, and how do we deal with that? Do we move more toward environment-as-code ... [so] we can make these changes on the fly to secure our environment? That’s only one piece. The other piece is if someone’s in your environment, how do you respond? A lot of that is moving toward better security practices along with a zero trust model.”



DISA’s Hosting and Compute Center (HaCC) Technical Director Korie Seville (center) at the Billington Cybersecurity Summit in Washington, D.C., Sep. 8, 2022.

DISA is focusing on DevSecOps to better secure its software and perform static analysis. Seville noted that historically DISA has been caught in a “reactive mode” or responsive vulnerability assessment after a breach or attack happens. The agency is pivoting to partnering with industry throughout the acquisition and procurement process to better understand the components

A portrait of Allan Friedman, a man with dark curly hair and a beard, wearing a dark suit jacket over a light-colored shirt. The image is overlaid with a semi-transparent orange filter. The text is positioned in the upper left corner of the image.

# Allan Friedman

Senior Advisor and  
Strategist, CISA

and security within applications.

“Having that open line of communication between us helps us to mitigate problems faster, instead of waiting for a vulnerability notification to come out or waiting for a vulnerability scanner to pick it up,” Seville said.

President Biden’s executive order on Improving the Nation’s Cybersecurity requires agencies to move toward a high security model, referencing static analysis tools, multi-factor authentication and adopt SBOM. Friedman explained that these features will promote transparency and better define responsibility.

“Everything that we know that we need to do to detect and prevent those attacks starts with that level of transparency,” Friedman said.

Seville said that cybersecurity is on a sliding scale of responsibility between the agency and the vendor. Depending on the type of product, there should be a shared responsibility for risk between the provider and consumer. As government moves toward shared services, like commercial cloud platform providers, industry and government should work together to address and mitigate vulnerabilities.

“That true partnership is really going to be the key to securing those things,” Seville said.

“We’ve got a good group of individuals growing together here, and I think that put us on even better footing as we face down things like SolarWinds, Log4j and other threats that have come our way,” DOD CIO John Sherman said. “Looking at things like SBOMs ... and other measures we need to take. It is a group responsibility.” ❁



**“Log4j has really taught us that it’s not just enough to say, ‘well, my asset management knows this...’ We need to know what’s under the hood. SBOMs are saying ‘this software depends on this software, depends on this software. It’s a nice little tree. It’s a list of ingredients.’”**

**— Allan Friedman,  
Senior Advisor and Strategist, CISA**



# Start the Journey to Zero Trust with Zero Trust Network Access

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

[LEARN MORE](#)





## Zero Trust ‘Essential’ and ‘Integral’ to JADC2

DOD leaders say you can’t have JADC2 without zero trust and a ‘data-centric’ approach to cyber.

BY KATE MACRI

**D**efense Department leaders say zero trust will be “essential” to their Joint All Domain Command-and-Control (JADC2) effort, which focuses on the idea of “data centrality” to improve information-sharing, data interoperability, and increase warfighter efficiency and accuracy in theater.

“For JADC2, zero trust is essential,” said DOD Cyber and Command, Control, Communications and Computers (C4) Deputy Director Stuart Whitehead during a recent Potomac Officers Club earlier this month. “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.”

Data-tagging is DOD’s first step toward implementing JADC2 and operating under a zero trust security framework.

“If I can tag my data, know who the person is who wants to access it, operating in a zero trust environment, that gives me a great advantage to manage my data effectively,” Whitehead said.

Whitehead wants DOD to consider zero trust holistically within the context of JADC2: every device or sensor connected to the network is a potential source of risk and should be treated as such.

“When we talk about zero trust or identity management, the same holds true for machines,” he said. “Machines have identities. Sensors have identities. The extent that we understand or should understand what sensors are out there and what information they’re producing is the starting point. The



Sailors assigned to Navy Cyber Defense Operations Command monitor, analyze, detect and respond to unauthorized activity within U.S. Navy information systems and computer networks.

conversation we’re having right now is, when do I actually implement those [metadata] tags? We’d like to implement at the point of creation.”

Brig. Gen. Chad Raduege, C4 director and CIO of Headquarters U.S. European Command for the Air Force, said getting to JADC2 and zero trust requires a cultural shift around how DOD thinks about data.

“It’s really a cultural shift of, I’m willing to send the data, and I’m willing to

# Stuart Whitehead

Deputy Director,  
Cyber and Command,  
Control and Computers,  
DOD



trust the data I receive from someone else,” he said at the Potomac Officers Club event. “I think that’s what the information-sharing and data centrality models of the future will get to. We’re seeing that right now in the European theater.”

Capt. Christina Hicks, who leads the Navy Cyber Defense Operations Command, said “data is the new bullet, so we need the new trigger puller.”

The new “trigger puller” is tech-savvy talent, which is a challenge for DOD. The department recently announced a shift toward prioritizing software factories like the Air Force’s Kessel Run, which develop, secure and iterate software on a continuous cycle to meet mission needs at the speed of relevancy.

One prong of DOD’s IT modernization plan is to turn soldiers into software engineers, which will be a critical component of implementing JADC2.

DOD’s plan requires major cultural overhaul, but the cost of doing so is too high given the increasing interconnectedness of communications and battle systems, the accelerated rate of malicious cyber activity and the willingness of the enemy to “take risks” with new, more agile technology that outperforms DOD systems.

“We continue to struggle with cybersecurity not being baked in from the onset,” Hicks said, which is something the DevSecOps approach of the DOD software factories aims to address. “We continue to bolt it on. From my perspective, where policy is not pacing technology is how we’re managing risk. We’ve been following compliance-based risk-adverse policy and it’s hampering our ability to onboard new technology.”

During a Bloomberg Government event, DOD CISO David McKeown described zero trust as “integral” to JADC2 implementation, signaling a top-down approach to ensure zero trust concepts are “baked in” to every combatant command and service branch.

“We’ve fought for dollars in the department to realign under this new architecture,” he said at the event. “We’re part of a cross-functional team working with the JADC2 community, there’s a specific line of effort dealing with





all the communications, whether it be cloud communications, zero trust or [data] transport. We engage early and often to make sure we're baking in all these zero trust concepts from the beginning. I think it's a good initiative, and we're happy to bake in zero trust from the beginning on a new evolving system."

Despite bad Russian actors' recent infiltration of default multi-factor authentication protocols — a core pillar of zero trust — McKeown believes the incident only reinforces the importance of a zero trust approach.

According to McKeown, it's common for phishers to infiltrate DOD and "wander around" and take what they need and get out, only for DOD to discover the breach 18 months later. Zero trust won't necessarily keep phishers

out, but it will improve DOD's ability to respond quickly.

"Zero trust is not perfect," McKeown said. "What it will allow you to do through the detection of anomalous behavior, find out those credentials have been stolen and flag that earlier. Once you're in the system with these credentials, zero trust will also stop you from escalating privileges, it segments you from other parts of the network, it restricts you to specific servers [so you can't] just wander about the network smashing and grabbing whatever you want. SolarWinds could potentially still happen [again], but the saving grace is we would detect it earlier, respond quicker, find the source of the anomaly quicker and return to normal operations much quicker." ❁

**“When we talk about zero trust or identity management, the same holds true for machines. Machines have identities. Sensors have identities. The extent that we understand or should understand what sensors are out there and what information they’re producing is the starting point. The conversation we’re having right now is, when do I actually implement those [metadata] tags? We’d like to implement at the point of creation.”**

**—Stuart Whitehead, Deputy Director,  
Cyber and Command, Control and Computers, DOD**