FORTINET FEDERAL

carahsoft


# CyberSmart 2025: Navigating Today's Cyber Landscape with AI, Zero Trust & Identity Management

## FedInsider & Fortinet Federal Mission Brief

Thank you for downloading the FedInsider CyberSmart 2025 mission brief sponsored by Fortinet Federal! Carahsoft is the reseller for Fortinet Federal cybersecurity solutions available via GSA Multiple Award Schedule and other contract vehicles.

To learn how to take the next step toward acquiring Fortinet Federal's solutions, please check out the following resources and information:

For additional resources:
carah.io/FortinetFederalResources

For upcoming events:
carah.io/FortinetFederalEvents

To purchase, check out the contract vehicles available for procurement:
carah.io/FortinetFederalContracts

For additional Cybersecurity solutions:
carah.io/CybersecuritySolutions

To set up a meeting:
FortinetFederal@carahsoft.com
866-468-3868

For more information, contact Carahsoft or our reseller partners:
FortinetFederal@carahsoft.com | 866-468-3868

FEDInsider

# CyberSmart 2025

# Navigating Today's Cyber Landscape with AI, Zero Trust & Identity Management

*Federal agencies look to strengthen the security of their networks under an expanded attack surface as they embrace a digital world.*

Cyber environments are constantly changing and evolving with advancements in technology, updates to policy, shifts in the use of zero trust architectures, increased use of artificial intelligence and more. And while new tech brings innovative ways to detect and mitigate cyberattacks, it also brings new elements of risk. Agencies are looking to embrace a digital world that allows them to navigate that risk and adapt to properly secured network needs.

In a series of recent **FedInsider webinar**, panels, thought leaders from government and industry discussed today's cyber threat landscape, the evolution of zero trust, the role of AI in preventing attacks while also increasing risk, and leveraging advanced technologies to bolster security.

## Evolving AI Threats

As AI advances, so do cyber threats. Experts like Scott Stephenson, Blackwire Labs Cyber Community of Excellence member, and Suneel Cherukuri, chief information security officer in the Office of the Chief Technology Officer for the Government of the District of Columbia, highlighted both the dangers and opportunities for AI in cybersecurity.

AI-powered attacks like deepfake impersonations, phishing campaigns and adaptive malware are among the most concerning. It's one thing to understand AI offenses, but Stephenson stressed that "on the defensive side, we really need to automate." Automation and orchestration are vital for detecting, flagging and responding to cyber threats.

Cherukuri explained that combining both approaches reduces false positives and ensures that high-severity threats always trigger meaningful, automated responses instead of overwhelming analysts with constant alerts. Still, AI alone won't solve all security problems. "Just because a system tells you something is right or wrong, does not make it right or wrong. You still need to apply conditions to it to establish whether that is correct," Cherukuri said.

Both security leaders also stressed the importance of embedding privacy and compliance standards into AI-enabled technologies. After their part of the presentation, many other experts expanded on those thoughts, and stressed the importance of key defensive elements like zero trust and identity management.

## Combating Today's Cyber Landscape With Zero Trust and Cloud

The federal government has mandated moving towards a zero trust framework as a baseline security measure to help strengthen cybersecurity. However, adopting cloud and zero trust architectures has been challenging across government according to Lt. Col. Jason Carter, Operations Officer for the U.S. Marine Corps Cyberspace Operations Group.

"Each service within the DOD has a unique mission, so we design a unique network to get after that mission. And that creates the unique situation that we have," Carter said. Not all of the Department of Defense's data exists in the cloud.

The Marine Corps is taking a more modern approach to cybersecurity by building a common firewall and boundary to protect all the data in a standardized way. "Instead of everyone finding their own cloud, I think zero trust is a framework that we center around now since it is a DOD requirement," Carter said.

From an industry perspective, adopting zero trust in government starts at the procurement level – educating procurement officers, integrating zero trust into the selection process and getting different departments to talk, according to Michael Woolfe, AVP of Product Management and Cloud at Fortinet Federal.

## Featured Experts:

- **Suneel Cherukuri**
  *CISO, Office of the CTO,* Government of the District of Columbia

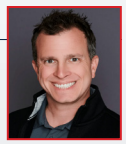
- **Scott Stephenson**
  *VP, Sales & Business Development & CCOE,* Blackwire

- **Lt. Col. Jason Carter**
  *Operations Officer,* Marine Corps Cyberspace Operations Group

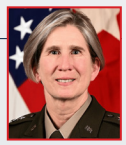
- **Kashif Ansari**
  *AVP, Sales Engineering,* Commvault

- **Jeffrey L. Berlet**
  *Senior Director, Technology,* Cyber Mission Sector, Peraton

- **Michael Woolfe**
  *Acting Vice President, Product Management & Cloud,* Fortinet Federal



- **MG Jacqueline D. McPhail**
  *Commanding General,* U.S. Army NETCOM



- **Tyler Harding**
  *Senior Technical Advisor,* Office of the CIO, DOD

- **James K. Jennings-Roche**
  *CISO,* Dept. of Defense Cyber Crime Center (DC3)

- **Rahul Dubey**
  *Vice President, Global Public Sector Solutions,* CyberArk

"Zero Trust touches so many elements in digital operations and human processes since the methodology's nature is to challenge assumptions – a person is on this sacred network, so they must be trusted, right? Or... the application assumes that a security capability is in place because something can talk to it, " Woolfe said. Allowing those teams and those operational systems to communicate is key, to fulfill the mission, yet in a manner that forces "humiliating" transparency to reach the point of zero assumptions.

And while many government agencies have already moved to the cloud, most also retain an on-prem hosted environment and data center – and multi-cloud environments make security and data protection even more complex, increasing the attack surface and the number of attack vectors.

Jeffrey L. Berlet, senior director for technology in the Cyber Mission Sector at Peraton, said zero trust is a solution for the current expanded threat landscape. "If we have a zero trust architecture in place with the right microsegmentation, an attacker cannot get into one of the cloud service provider environments and then move laterally through the entire system," he said.

Considering the type of sensitive data that defense and other federal agencies are collecting, analyzing, using and moving, all data must be treated as critical when migrating from on-prem environments to the cloud. According to Kashif Ansari, senior director of sales engineering at Commvault, this requires agencies to rethink governance, networking and resilience – especially in disconnected or tactical environments.

"When you are planning for migration from a hardened data center that you are used to, and moving some of your data to a cloud environment... you have to take a hard look at all the services you are using in your data center and those available in the hyper-scalar. Do they meet your security requirements? Because it impacts what you can use," Ansari said. These security requirements, however, can also be inserted into a zero trust framework.

## Bolstering Identity Management to Meet Today's Security Needs

Protecting users' identities is a critical component of proper cybersecurity hygiene. That's where Zero Trust comes in – it's about never trusting and always verifying a user's identity. Still, advancements in AI are creating false personas that appear to be real, so agencies are adopting various new approaches, processes and technologies to detect and dodge them.

Maj. Gen. Jacqueline D. McPhail, Commanding General in U.S. Army NETCOM, believes biometrics and multi factor authentication will improve user experience while ensuring strong security for deployed forces, moving away from just an ID card or token. "User experience is not necessarily sitting at your desk in the Pentagon. It can be downrange on a mission. And that is where we have to look at it and how we apply all this new technology," McPhail said.

At the DOD, Tyler Harding, the department's senior technical advisor in the Office of the CIO, said they're looking to centralize identity management through its ICAM program while also keeping an eye on the user experience.

"The department is moving in the direction of something called Attributes to Access Control," Harding said. "The ICAM infrastructure has to be capable to support what I have today, which is the legacy, that is often based on Active Directory – but it has to support our future, which is based on what we call their attributes."

Attributes can be things that uniquely identify a person, and they can determine the access to data that a user has in a shared environment. This way all three pieces – Identity Governance and Administration, Identity Provider and the master record – work together as the department also works towards automation with IGA. "We get efficiencies, improved user experience and most importantly, we improve security," Harding said.

James K. Jennings-Roche, CISO for the DOD's Cyber Crime Center, said that the current identity verification methods at DC3 face challenges in secure environments where personal devices are restricted. He can use the Microsoft Authenticator application to access certain DC3 accounts, but users working in secure spaces can't. Instead, they rely on expensive Common Access Cards.

Yet, as DC3 moves investigations from physical hardware into the cloud, zero trust and ICAM will become critical. "We only allow DC3 employees to have access to these networks where we are doing our investigations. As we move into the cloud, we call it 'federated forensics or forensics-as-a-service,'" Jennings-Roche said. "We are looking at expanding our user base outside of DC3." This requires having zero trust and identity verification at the highest level.

Rahul Dubey, vice president of global public sector solutions at CyberArk, is focused on identity in the context of AI and privileged access. He looks at AI in three dimensions: defending with AI, defending against AI and defending for AI.

"AI can be used and abused both ways," Dubey said. IT offers both risks with deepfakes and automated attacks, and it also offers opportunities with advanced analytics and behavioral monitoring. "Using AI, you can look at the analytics and how you analyze the behaviors, but it all comes down to user and machine behavior," Dubey said. Automation, least-privilege principles and emerging models like zero standing privileges should also be part of the identity management discussion moving forward.

Identity is foundational to cybersecurity, especially as advances in AI become widely adopted and leveraged for good and bad. Experts agree that security requires a team effort, continuous improvements and a strong culture of shared responsibility.

**TO LEARN MORE, VISIT CARAH.IO/CARAHSOFTAI**


FEDInsider

**Hosky Communications Inc.**
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft

**Carahsoft**
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Katherine Mulholland**

(571) 662-4865
Katherine.Mulholland@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft