ATARC × NEXTGOV FCW × Washington Technology

Thursday, February 26, 2026

8:00 AM EST
1 HR

Registration, Breakfast & Networking

Pick up your badge, grab some breakfast and network with your peers!

9:00 AM EST
15 MINS

Opening Remarks

Welcome to our Cybersecurity Futures: Built on Zero Trust!

9:15 AM EST
40 MINS
Panel

Zero Trust Beyond Compliance

Daniel Buchholz
Red Cell Section Chief
U.S. Department of State

Tyler Harding
Senior Technical Advisor/ICAM Program Manager
Office of the DoD Chief Information Officer

Dave Raley
Chief Digital Business Officer
U.S. Marine Corps Community Business

Justin Ubert
Director, Cyber Protection Division, Office of the CISO
U.S. Department of Transportation

Mike Colson
Director, Public Sector Growth
Akamai

Anna Pettyjohn
Executive Vice President, Product & Strategy
GovExec

Zero Trust is more than a compliance mandate—it is a proactive framework to enhance federal cybersecurity and resilience. This session focuses on advanced strategies for adopting Zero Trust principles while addressing the unique challenges posed by legacy systems. Discussions will explore leveraging modern tools, enhancing data protection, and integrating Zero Trust into existing infrastructures without disrupting mission-critical operations. Leaders will share practical approaches for prioritizing upgrades, implementing secure workarounds, and fostering a culture of adaptive security that evolves with emerging threats.

9:55 AM EST
15 MINS

Building an AI-Powered Zero Trust Defense: Modernizing Government Security Operations and Empowering the Future Workforce

Google Public Sector

Usman Chaudhary
Strategic Growth Executive
Google Public Sector

Tom Suder
Founder
ATARC

In this session, Google Public Sector's Usman Chaudhary will discuss how artificial intelligence (AI) can be leveraged to effectively implement and operate a Zero Trust security framework and move from reactive to proactive and predictive security.

10:20 AM EST
40 MINS

Break & Emerging Technology Showcase

11:00 AM EST
10 MINS

Zero Trust: Top 5 Best Practices

THALES

Gina Scinta
Deputy Chief Technology Officer
Thales TCT

The rise of cyber-attacks indicates the obvious—the current approach to security isn't working. Enter Zero Trust. There is not a single blueprint for implementing zero trust. EO 14028, NSM 8, and the National Cybersecurity Strategy require agencies to implement zero trust. And, DoD, CISA, NIST and OMB have all issued architecture guidance. This often
results in agencies implementing a self-defined approach made up of an assortment of single-purpose solutions. An ad-hoc approach has limitations and is not scalable, often making an environment more susceptible to security gaps and vulnerabilities.

Attend this session to learn about the best practices for implementing zero trust. The speaker will discuss the top 5 tips for putting zero trust into action.

11:10 AM EST
10 MINS

Zero Trust: Signals and Context

Netskope

Steve Riley
Vice President and Field CTO
Netskope

11:20 AM EST
35 MINS
Panel

Beyond the Bid: Cyber Expectations in Modern Defense Contracting

Derrick Davis
Senior Fellow, AI For Developing Countries Forum, Center for Research in Emergent Manufacturing (CREM)
University of Maryland, Baltimore County

Terry Kalka
Director, DoD Cyber Crime Center (DC3)/DIB Collaborative Information Sharing Environment (DCISE)
"Department of War "

Nick Wakeman
Editor-in-chief
Washington Technology

Cybersecurity is becoming a defining factor in federal contracting. What was once an IT consideration is now a core element of procurement strategy, with agencies increasingly embedding security requirements into RFPs and contract clauses. Frameworks like NIST SP 800-171 and DFARS are shaping how vendors compete, how teams are structured, and how risk is managed across the supply chain. For contractors, especially those in the Defense Industrial Base, this shift is changing the game. Compliance is no longer optional. It is a prerequisite for eligibility, partnership, and long-term viability. This session will bring together acquisition officials, cybersecurity leaders, and industry experts to explore how evolving security mandates are shaping the defense contracting environment. Speakers will discuss how requirements are being communicated in RFPs, how compliance is being evaluated, and what this means for innovation, competition, and small business participation.

11:55 AM EST
5 MINS

Lunch Remarks

Delinea

Ginelle Osworth
Director, Public Sector-Federal
Delinea

12:00 PM EST
1 HR

Lunch in the Emerging Technology Showcase

1:00 PM EST
15 MINS

Data Resilience Built on Zero Trust

Joshua Yu
Senior Systems Engineer - Federal
Veeam Software

1:15 PM EST
10 MINS

Active Resilience: The Next Evolution of Zero Trust

COLORTOKENS™

Louis Eichenbaum
Federal Chief Technology Officer
ColorTokens

Zero Trust implementation alone does not guarantee mission continuity. This session introduces Active Resilience, the operational outcome achieved when all pillars of Zero Trust work together to ensure Mission Essential Functions continue even during a cyberattack. Re-focusing on the original principle of "assume breach," the discussion highlights the critical role of microsegmentation in stopping lateral movement and containing threats before they impact high-value assets.

The session also explores how integrated security capabilities and AI-driven automation can reduce complexity, accelerate deployment, and address workforce constraints. Attendees will gain a practical framework for evolving from Zero Trust compliance to true mission assurance.

1:30 PM EST

50 MINS

Panel

Building and Measuring Success in Public Sector Security

Surendra Babu
Office Chief, Cloud Hosting and Networks Office (CHNO), Department of Technology Services
US Courts

Jeanette Duncan
Chief Information Officer, Principal Authorizing Official
Defense Counterintelligence and Security Agency

Dr. Michael Hauck
Acting Chief Data Officer
National Science Foundation

Edmond Kuqo
RAISE Technical Warrant Holder (TWH) AI/LLM | DevSecOps | Cybersecurity | Cloud
U.S. Department of the Navy

Christopher Wild
HQDA DCS G-6 Cybersecurity Integration Control Systems Division
U.S. Army

Kelvin Brewer
US Public Sector Field CTO
Ping Identity

Iris Konstant

Iris Konstant
Editor & Social Lead, Branded Content
GovExec

The Federal Zero Trust Strategy provides a blueprint for strengthening cybersecurity across agencies, emphasizing implementation and continuous improvement. This session explores practical approaches to adopting Zero Trust Architecture aligned with current Executive Orders focusing on challenges such as identity management, secure access, and legacy system integration. Leaders will also discuss methods for developing and applying key performance indicators to measure Zero Trust effectiveness, track compliance, and identify areas for improvement.

2:15 PM EST
25 MINS
Panel

Next-Gen Threats, Next-Gen Defenses: The Tech-Cybersecurity Equation

Dr. William Streilein
Vice President and Chief Technology Officer
Noblis

Frank Konkel
Editor-in-chief
GovExec

The rapid advance of artificial intelligence, automation, and synthetic media is transforming both the opportunities and risks in federal cybersecurity. In fiscal year 2024, federal civilian agencies reported more than 32,000 cybersecurity incidents to CISA, with a growing share linked to AI-enabled phishing, deepfake-based social engineering, and malware capable of adapting its behavior in real time. Automation is helping agencies cut average incident response times from initial detection to containment by as much as 40 percent, yet it also gives attackers the ability to scale intrusions and exploit vulnerabilities faster than human teams can react. This session will bring together cybersecurity leaders to examine how emerging technologies are reshaping agency defenses, where AI and automation are making the greatest operational impact, and how the convergence of advanced tools and cyber strategies is redefining resilience across the federal enterprise.

2:50 PM EST
5 MINS

Closing Remarks