GovExec

GovExec's Cyber Resilience Summit: Transforming Strategy into Capability

Reston, VA

Thursday, November 19, 2026

8 AM EST
55 MINS

Registration & Breakfast

Join us for registration, check-in, and a networking breakfast before the summit begins. Connect with fellow federal technology and cybersecurity leaders over coffee and light breakfast while preparing for a morning of insightful discussions and collaboration.

Agenda times and programming are subject to change.

8:55 AM EST
5 MINS

Opening Remarks

Tom Suder
Founder
ATARC

9 AM EST
20 MINS

Morning Presentation

Dr. Gregory Bird
Deputy, Associate Director, Infrastructure Assessments & Analysis
Cybersecurity and Infrastructure Security Agency

9:20 AM EST
15 MINS

Emerging Technology Talk

Shea Connelly
Executive Editor, GovExec Branded Content
GovExec

Chris Klein
Head of GCP Security Sales
Google Public Sector

9:35 AM EST
40 MINS

The Evolving Cyber Threat Landscape: Challenges and Priorities

Vivek Agnish
Portfolio Manager, National Security Systems(NSS) Governance Office of the Chief Information Security Officer Office of the Chief Information Officer
U.S. Department of Homeland Security

Grace Dille
Technology Reporter
Nextgov/FCW

Rebecca McWhite
Technical Lead for Cybersecurity Supply Chain Risk Management
Computer Security Division of the Information Technology Laboratory at the National Institute of Standards and Technology

Dr. Oluwafemi Akintunde
Subordinate Authorizing Official, Office of Special Investigations
U.S. Air Force

Dr. Jim Chen
Professor
National Defense University

Dr. William Streilein
Vice President and Chief Technology Officer
Noblis

Cyber threats are growing more sophisticated, persistent, and difficult to contain across today's government environments. This panel will explore how agencies are applying Zero Trust principles to improve cyber resilience, strengthen incident response, and reduce risk across users, devices, applications, and networks. Speakers will discuss how Zero Trust supports broader cybersecurity strategies, including threat detection, continuous monitoring, and secure access across distributed systems. Attendees will gain insight into how agencies are using Zero Trust to build stronger, more adaptive defenses while supporting mission continuity.

10:15 AM EST
10 MINS

Securing Federal Identity for AI and the Quantum Future

Kelvin Brewer
Director, Public Sector Sales Engineering
Ping Identity

Join Kelvin Brewer, U.S. Public Sector Field CTO at Ping Identity and Industry Chair of ATARC's Identity Management Working Group, for a discussion on strengthening Federal identity security. Kelvin brings experience advancing Federal ICAM practices, including coauthoring ATARC's Federated Identity Management Framework for Civilian Agencies and Defensible Zero Trust: A Strategic Playbook.

Explore practical approaches to governing AI agents as workforce identities, preparing the identity layer for post-quantum cryptography, and extending Zero Trust controls to legacy applications and operational technology while maintaining mission continuity.

10:25 AM EST
15 MINS

When Trust Changes: Fireside Chat

Kynan Carver
Vice President, Cybersecurity
Maximus

Iris Konstant
Editor of Branded Content
GovExec

As threats evolve and circumstances change, how can federal agencies maintain digital trust while balancing security, resilience, and accountability? This fireside conversation will explore how agencies can adapt to emerging risks, reassess trust in real time, and maintain clear governance and human oversight throughout the decision-making process.

10:40 AM EST
30 MINS

Modernizing Cybersecurity for Mission Resilience

Dan Austin
Cybersecurity SME
COL (USA-ret), OT Advocate, Contractor

Derrick Davis
Senior Fellow
Center for Research and Emergent Manufacturing, University of Maryland Baltimore County

Christopher Wallace
Chief of Cybersecurity, Portfolio Acquisition Executive for Medical Digital Solutions
Defense Health Agency

Chris Teale
Managing Editor
Route Fifty

Modernization efforts across government are reshaping infrastructure, applications, and enterprise technology environments, and Zero Trust is becoming a critical part of that transformation. This panel will examine how agencies are integrating Zero Trust principles into broader modernization strategies, from infrastructure upgrades and cloud migration to application transformation and enterprise architecture. Speakers will share lessons learned on balancing security, interoperability, and mission performance while moving away from outdated systems. Attendees will gain practical perspectives on how Zero Trust can support modernization in ways that strengthen both resilience and long-term operational readiness.

*Session recording will **not** be published post-event. Thank you for your understanding.

11:10 AM EST
15 MINS

AI: The Threat, the Defense, and the Mission

Garrett Lee
RVP, Public Sector Sales
Broadcom, Enterprise Security Group

AI amplifies the need for Zero Trust. How attackers, defenders, and government organizations are leveraging AI, and the evolving data security challenges as AI accesses, analyzes, and derives sensitive insights from information.

11:25 AM EST
20 MINS

Break in the Emerging Technology Showcase

11:45 AM EST
20 MINS

Accelerating the Digital Warrior: Building an SI-Ready Workforce

MAJ Brad Worley
Chief of Cyber & SI Programs
U.S. Air Force Test and Evaluation

• How organizations can move beyond understanding SI to embedding it into real operational and cyber decision-making.
• Balancing rapid adoption with security, risk and accountability.
• Transforming skills, roles and ways of working while creating the Data-First culture needed to make SI effective at scale.

*Please note this presentation will not be available for on-demand viewing post-event.

12:05 PM EST
15 MINS

The Agents Have Other Plans

Scottie Ray
Director, Cloudflare One Specialist Solutions Engineering
Cloudflare

You asked for a summary. Your AI agent accessed three systems, shared a file, and called another agent. Helpful—or a security incident? As federal agencies explore AI that acts, familiar trust assumptions need a rethink. This session examines how identity, least-privilege access, data protection, and visibility can keep autonomous agents on mission. Learn where existing controls hold up, where gaps emerge, and how to enable autonomy without handing over the keys.

12:20 PM EST
25 MINS

Protecting What Matters: Data Security Across the Enterprise

Rudolf Rojas
Information Technology Manager
USDA

Ashley Jones
Cybersecurity Advisor
Washington D.C. – Region III, Cybersecurity and Infrastructure Security Agency

Iris Konstant
Editor of Branded Content
GovExec

In a government environment defined by growing data volumes and expanding digital operations, protecting sensitive information has become central to Zero Trust implementation. This panel will focus on how agencies are using Zero Trust to strengthen data security, improve visibility, and enforce protections across increasingly distributed environments. Speakers will discuss approaches to data access, segmentation, governance, and monitoring, as well as the challenges of securing information across systems, users, and mission functions. Attendees will gain a clearer understanding of how Zero Trust can support stronger data protection and more informed decision-making across the enterprise.

12:55 PM EST
1 HR

Closing Remarks & Lunch in the Emerging Technology Showcase