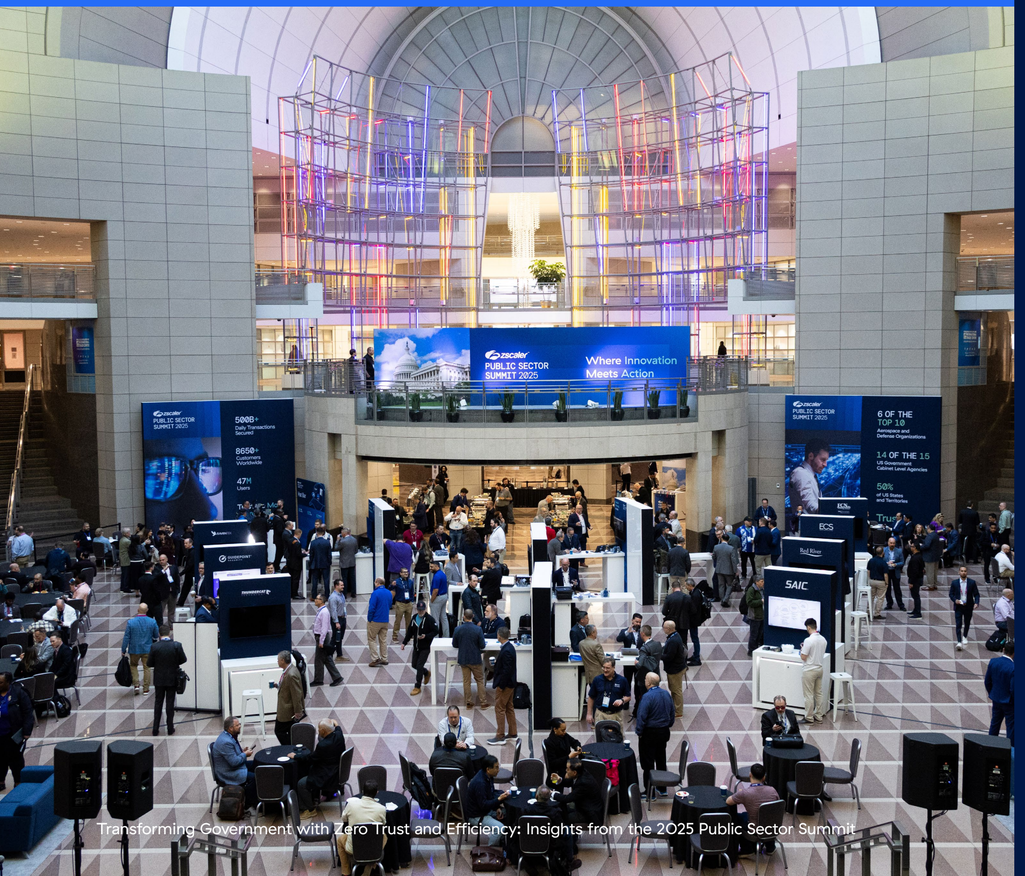
Transforming Government with Zero Trust and Efficiency

Insights from the 2025 Public Sector Summit

EBOOK

Table of Contents



Foreword

The rapid evolution of cyber threats, and the increasing dependence on technology for agencies to ensure national security and better serve U.S. citizens, has created a pressing need for strategic modernization. The 2025 Zscaler Public Sector Summit served as a platform to explore these challenges and share innovative solutions across cybersecurity, digital transformation, and operational efficiency.

Federal agencies, state governments, and local municipalities face common challenges: safeguarding sensitive information, ensuring seamless citizen services, and combating the growing sophistication of adversaries. This ebook distills key themes from summit sessions into actionable guidance for public sector leaders, providing the foundation for a secure, efficient, and forward-thinking digital future.

Everything starts with passion and drive.

JAY CHAUDHRY
CEO and Founder, Zscaler

01

Reimagining Network Security Through Zero Trust Everywhere

A Modern Philosophy of Security for Public Sector Transformation

As cyber threats grow more sophisticated and target the very foundation of public sector operations, Zero Trust has emerged as a vital response—a philosophy that not only defends against attacks but also transforms how government agencies operate securely in the digital age. At its core, Zero Trust Everywhere extends the principles of "never trust, always verify" beyond traditional IT systems to encompass data, workloads, applications, Internet of Things (IoT) devices, Operational Technology (OT), and more.

Unlike outdated perimeter-based security models, Zero Trust Everywhere assumes that no entity—whether internal or external—can be trusted by default. This approach is especially critical in the public sector, where a single breach can compromise sensitive citizen data, national security infrastructure, or mission-critical operations.

Government leaders must adopt Zero Trust not as a singular initiative but as a comprehensive framework. By embedding Zero Trust into every layer of their security architecture, agencies can confidently embrace cloud-first strategies, remote work arrangements, and digital innovation without sacrificing security.

Voices from the Summit

During the keynote, Vu Nguyen, Chief Information Security Officer at the Department of Justice, shared how moving to a Zero Trust Everywhere model has amplified their ability to protect sensitive assets while enabling operational agility. "Zero Trust is not a singular technology—it's a philosophy that protects what matters most. Zero Trust is about full accountability—it lets you see all activity, from the user logging into the device they're using down to the data and application they're trying to access" — Vu Nguyen, CISO, Department of Justice

Jay Chaudhry, CEO of Zscaler, further expanded on this idea, noting that Zero Trust must adapt beyond users to secure everything—devices, applications, workloads, campuses, and data. It's about rethinking what government security needs to look like amid evolving threats.

"Protecting military data begins at the strategic edge—it's about flipping the old perimeter mindset inside out to prioritize data security."

—**SAM SALINAS**, LEAD, ENTERPRISE COMPLIANCE SERVICES, RTX

"We demonstrated scenarios ranging from employee access to collaboration across enterprises, showing how Zero Trust works in hybrid environments with on-prem, cloud, and branch setups."

—**ALPER KERMAN**, CYBERSECURITY ENGINEER AND PROJECT MANAGER, NATIONAL CYBERSECURITY CENTER OF EXCELLENCE AT NIST

"Zero Trust starts with users, but it must extend to IoT, OT, workloads, servers, and campuses—protecting every environment seamlessly."

—**DHAWAL SHARMA**, EVP, PRODUCTS AND HEAD OF PRODUCT STRATEGY, ZSCALER

What Does Zero Trust Everywhere Mean for the Public Sector?

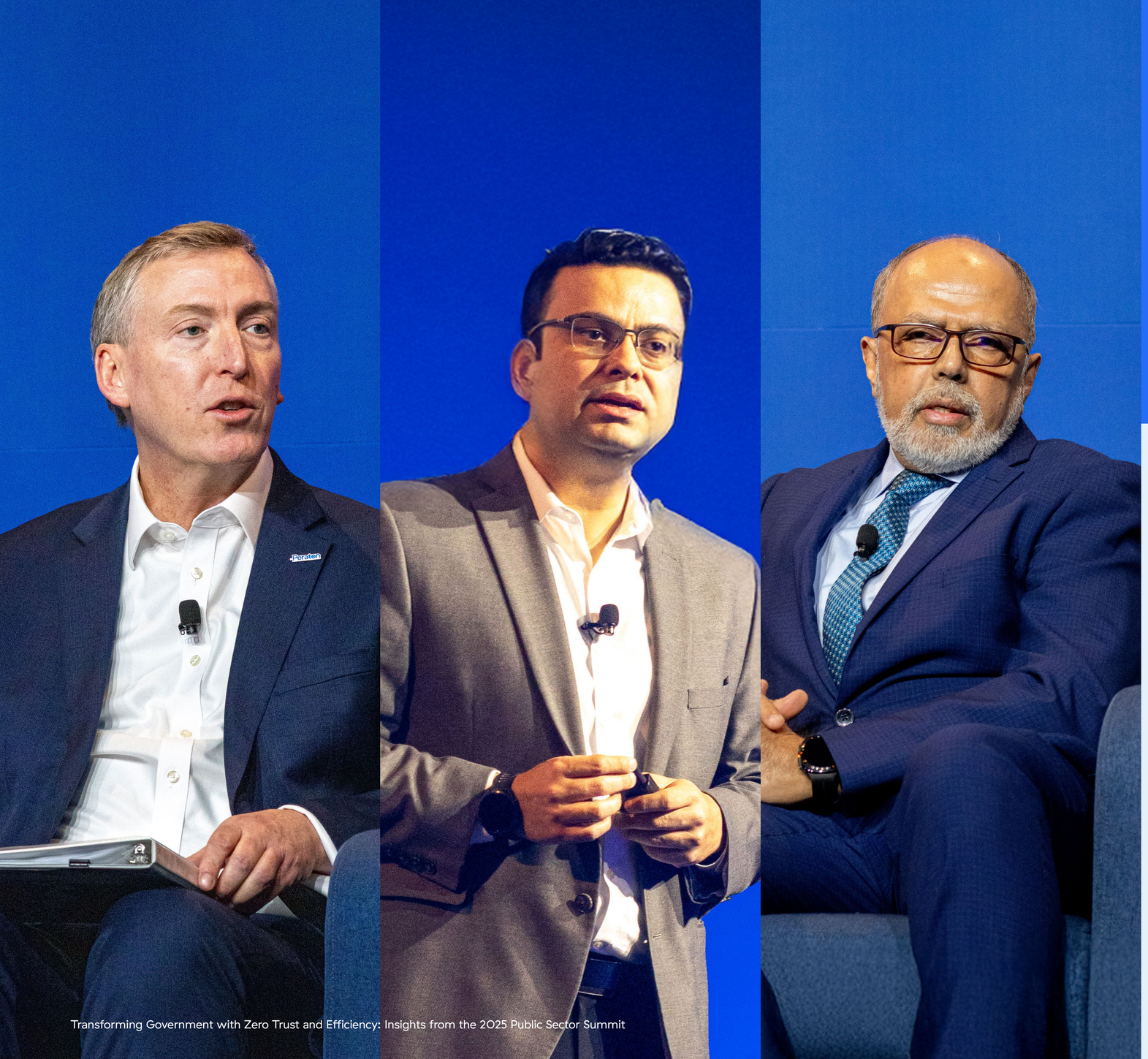
Zero Trust Everywhere mandates that agencies apply the philosophy to every element of their IT and operational environments:

- **Users and Identities:** Every user, whether internal or external, must be verified using robust identity and access management tools before being granted access to resources.
- **Devices:** Protect every endpoint by ensuring all devices meet strict security baselines, checking for posture (e.g., updated patches and configurations) on every interaction.
- **Workloads and Applications:** Extend Zero Trust principles to workloads running in the cloud, on-premises, or in hybrid environments while ensuring secure access to applications.
- **IoT and OT:** Secure non-traditional devices such as IoT sensors or OT equipment, safeguarding critical infrastructure like power grids, healthcare systems, and water utilities.

This comprehensive approach ensures agencies remain resilient across all facets of their operations, even as the attack surface continues to expand in scope and complexity.

Key Takeaways:

- **Adaptive Security Across Layers:** Zero Trust Everywhere applies continuous identity verification, device health checks, workload access vetting, and dynamic application monitoring to secure every layer of an organization's architecture.
- **Breaking IT Silos for Unified Operations:** Public sector leaders must move beyond fragmented tools and unify efforts under a cohesive Zero Trust framework, reducing complexity and improving security efficiency.
- **Empowering Digital Transformation:** By embedding Zero Trust principles throughout their operations, agencies can adopt cloud, hybrid, and multi-cloud setups without compromising security.



02

Protecting National Assets Through Modern Network Transformation

Safeguarding Critical Infrastructure in a Global Threat Environment

Protecting national assets—such as energy grids, transportation systems, and defense infrastructure—is a top priority for public sector leaders. From ransomware attacks to nation-state espionage, the risks associated with targeting critical infrastructure are escalating in scale and complexity.

Modern network transformation offers public sector organizations the opportunity to build systems that are more resilient, agile, and secure. Zero Trust serves as the bedrock of these efforts, replacing legacy systems with identity-driven, AI-enhanced architectures that anticipate the needs of tomorrow's adversaries.

Voices from the Summit

Scott Stephens, Chief Solutions Architect at Sandia National Laboratories, described how Zero Trust has enabled transformative shifts at the lab. "Zero Trust is a catalyst for the transformation of our networks, ensuring resilience against adversaries."

Sandia's Jason Crenshaw, Director of Information Security, highlighted the importance of combining ZTA with dynamic threat intelligence to safeguard the nation's most sensitive projects. "Modernizing infrastructure to focus on transactions, endpoints, and user activities rather than traditional network forces greater security control."

"IoT devices were designed to be simple and connected—not secure. That creates vulnerabilities we must urgently address, especially across critical infrastructure."

—**JEFF BERLET**, SR. TECHNOLOGY DIRECTOR, CYBERSECURITY DIVISION AT PERATON

"Black Swan events are going to happen, so failing to plan is planning to fail. We cannot work in a vacuum, especially in critical infrastructure."

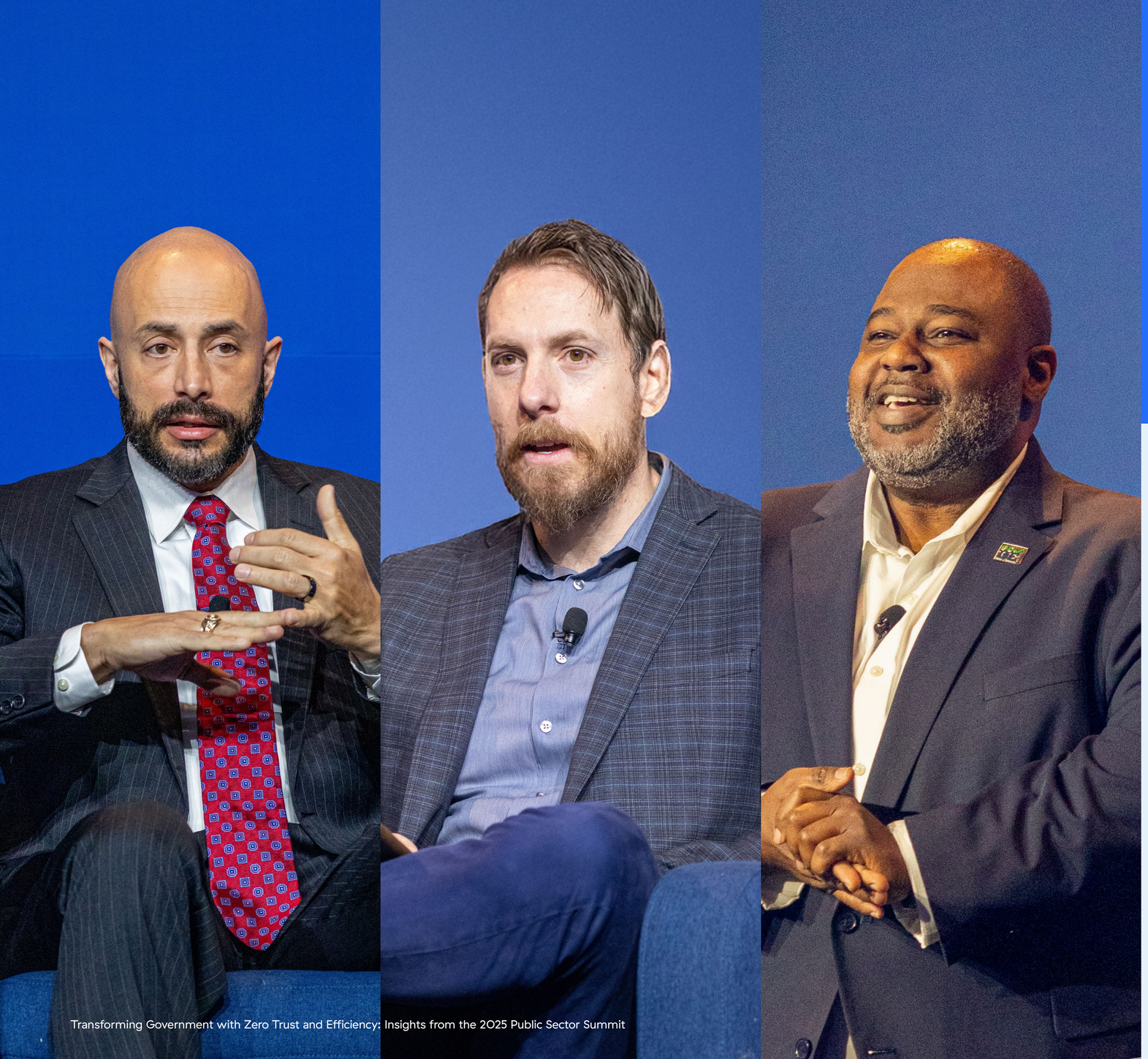
—**RAFI KHAN**, CISO NEW JERSEY TRANSIT

"Disconnected Zero Trust environments ensure mission-critical services keep running even during catastrophic events like internet outages or disasters."

—**DHAWAL SHARMA**, EVP, PRODUCTS AND HEAD OF PRODUCT STRATEGY, ZSCALER

Key Takeaways:

- **Dynamic Security for Mission-Critical Tasks:** Agencies can use Zero Trust frameworks to secure national laboratories, defense systems, and energy grids, ensuring continuity even during active attacks.
- **Early Threat Detection:** Continuous visibility and AI-driven anomaly detection enable agencies to respond to threats before they escalate.
- **Interagency Collaboration:** Partnerships between federal agencies, such as those facilitated by the Cybersecurity & Infrastructure Security Agency (CISA), multiply resources and capabilities needed to defend essential infrastructure.



03

Driving Efficiency Through Modernization in Government Operations

Building Scale for Future-Ready Public Services

Advancing government operations requires a purposeful blend of efficiency and effectiveness via technology modernization. Federal, state, and local government agencies are under pressure to lower costs, streamline workflows, and adapt to citizen expectations for seamless digital services.

Speakers at the summit shared how automation, cloud adoption, and operational optimization can help agencies break down silos and reduce dependency on costly legacy systems. These strategies create new opportunities for scalability while ensuring reliability during times of crisis, such as natural disasters or cyberattacks.

Voices from the Summit

Derrick Pledger, Chief Digital Information Officer at Maximus, spoke about the importance of balancing innovative modernization with accountability to taxpayer dollars. "Efficiency alone isn't enough—we must strive for effectiveness to truly modernize. Efficiency is not just about cost savings. If you save 10% on your operational budget but introduce friction in user experience, then you've failed."

Chris Soong, EVP and CIO at Huntington Ingalls Industries, discussed how the defense contractor leverages technology to enhance productivity while fulfilling critical government contracts. "Concentrate on user experience—put yourselves in their shoes and test technology as they would: from a hotel, a coffee shop, or a remote location. That's how you learn."

"We spent years ensuring adversaries couldn't get in; now we focus on minimizing the impact when they do—controlling the blast radius is essential. Traditional technologies weren't designed for Zero Trust—you need a mindset shift to move to solutions that truly deliver."

—**SOLOMON ADOTE**, FORMER CISO, STATE OF DELAWARE

"Cybersecurity can say, 'Yes, if...' instead of just 'No,' by proving its value as a mission enabler, not just a cost center. It's really important right now, as we have new people coming in, for them to understand what the return on investment of zero trust is."

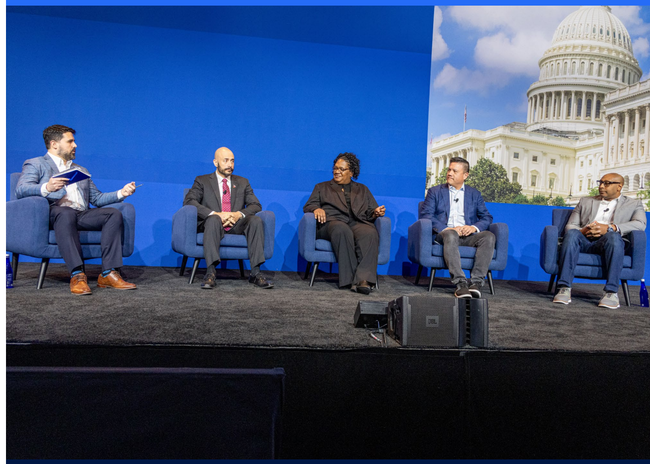
—**JUSTIN FANELLI**, ACTING CTO, NAVY

"Modernization needs a dual focus—on saving costs and creating measurable, effective outcomes for users and stakeholders...Efficiency isn't just about cutting costs – it's about creating seamless experiences that empower users to deliver mission-critical services securely and effectively."

—**DR. JOE LEWIS**, VP, CYBERSECURITY SOLUTIONS HEALTH AND CIVIL SECTOR, LEIDOS

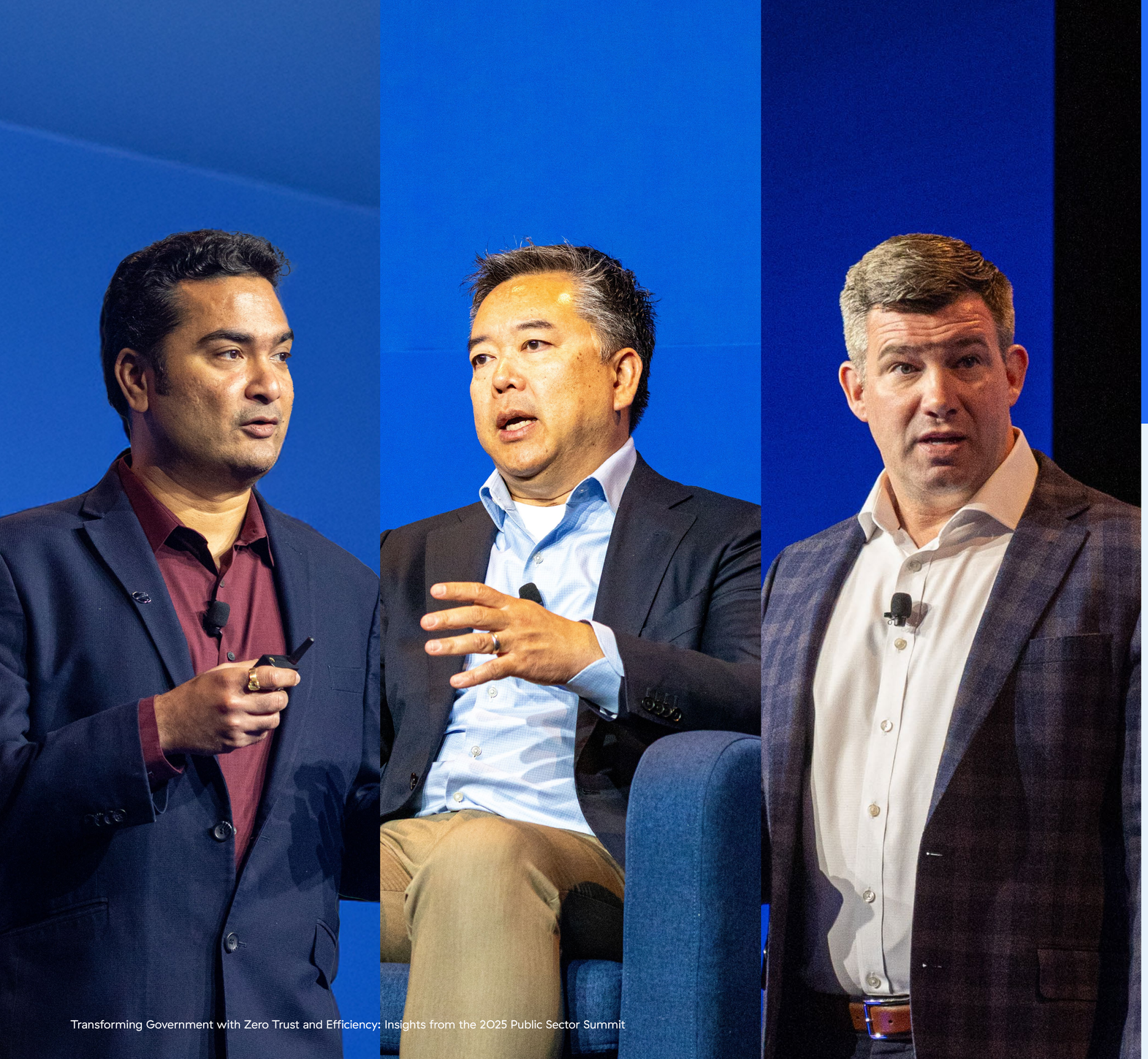
"To me, a strong zero trust implementation will pay for itself down the line. What it does for us is that it shifts our security model from a reactive mentality to a more proactive one with continuous monitoring verification, because zero trust helps us to detect the suspicious activity as it's happening," Nguyen said. "And on top of that, it helps us to contain it [and] respond to it before it can cause significant damage." –

—**VU NGUYEN**, CISO, DEPARTMENT OF JUSTICE



Key Takeaways:

- **Cloud Solutions Empower Scalability:** Leveraging cloud technologies ensures agencies can rapidly adjust to shifting workloads while delivering citizen services with speed and precision.
- **Automation Brings Speed and Accuracy:** Public sector entities using AI-driven automation can reduce errors in high-volume workflows while reallocating human resources toward strategic initiatives.
- **Resiliency Amid Disruption:** Integrated systems equipped for backups and failover ensure continuity in critical services while minimizing downtime.



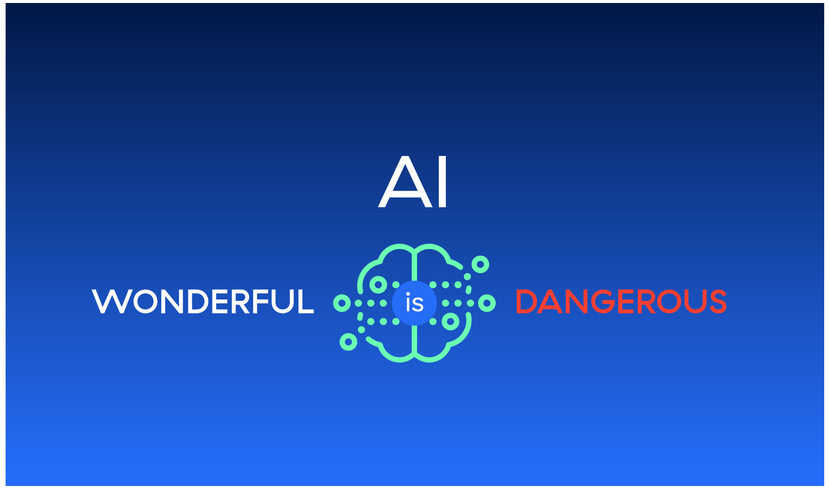
04

Addressing Cyber Threats with AI and Zero Trust

Mitigating AI-Driven Cyber Threats in the Age of Automation

Generative AI has significantly increased the sophistication and frequency of cyberattacks. Public sector agencies are facing adversaries armed with AI tools capable of automating reconnaissance, credential theft, data exfiltration, and even penetration testing.

Zero Trust frameworks remain the strongest defense against AI-enabled attacks, offering a proactive security stance rather than reactive measures. By integrating AI threat detection systems and leveraging telemetry data, government agencies can predict, defend against, and outpace attackers.



Voices from the Summit

Jay Chaudhry, CEO and Founder of Zscaler, shared his concerns about the rise of AI-fueled offenses and advocated for urgent adoption of AI-powered defense systems. “Generative AI-fueled attacks have raised the stakes—we must prepare to defend against highly dynamic and automated threats.”

“AI-powered breach prediction models allow us to detect scenarios early and provide actionable recommendations to mitigate breaches before they occur.”

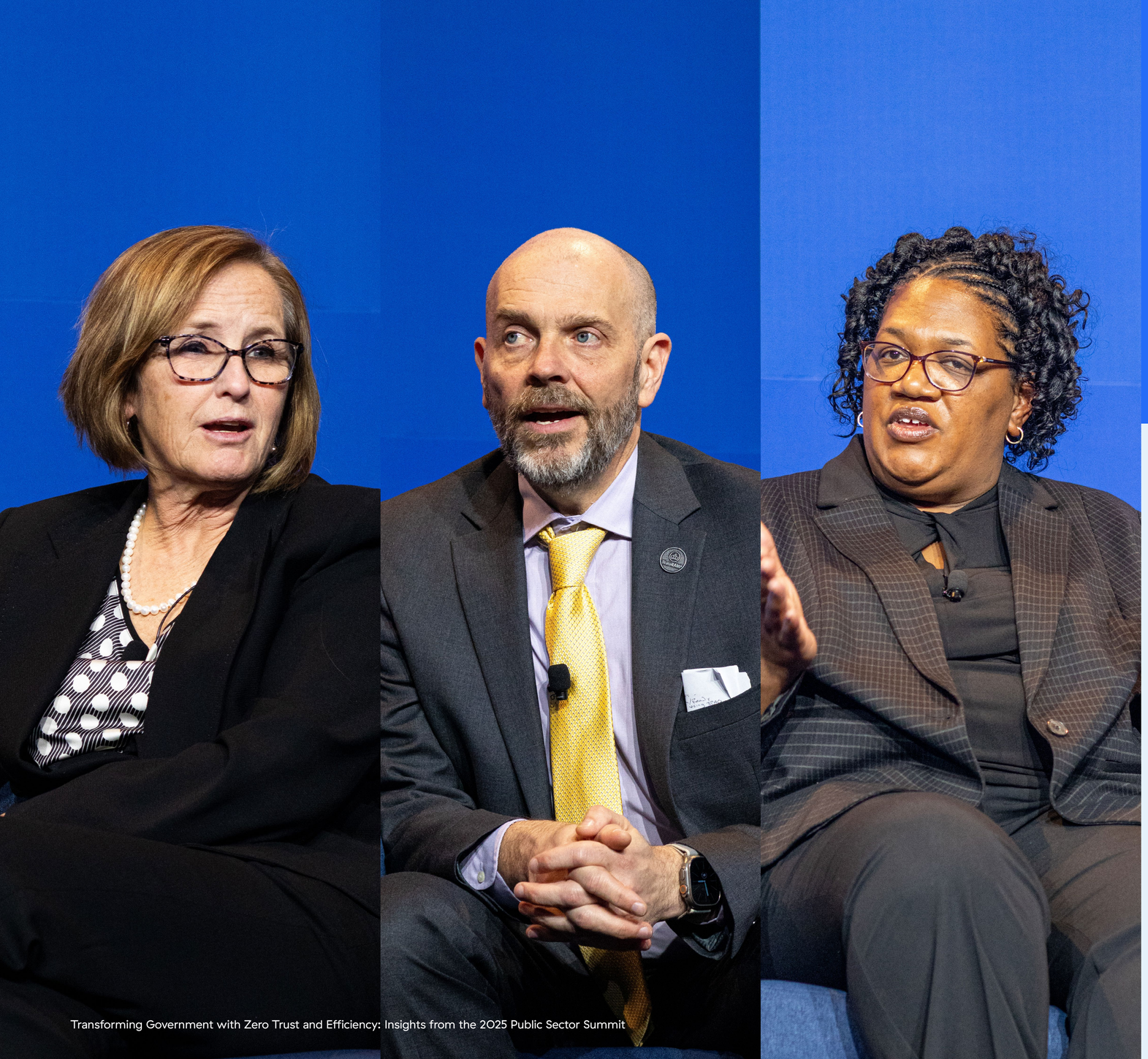
—**DEEPEN DESAI**, CISO, ZSCALER

“We can’t protect something we can’t see. Even if there are devices we can’t patch, we need visibility into the OT networks and to apply AI for managing risks and augmenting critical staffing gaps.” —

—**JOE NGUYEN**, DIRECTOR, CORPORATE INFORMATION SECURITY, CYBERSECURITY INFRASTRUCTURE, LOCKHEED MARTIN

Key Takeaways:

- **AI in Defense:** Tools like machine learning-based intrusion prevention systems and predictive analytics can identify and stop threats before they escalate.
- **Zero Trust with AI:** Combining Zero Trust principles with AI-driven anomaly recognition enables granular visibility into suspicious behaviors.
- **Adapting Policies for AI:** Federal agencies must revise security protocols to account for AI-enhanced phishing, malware, and lateral movement within networks.



05

Leadership in Transformation: Collaboration and Strategic Visioning

Driving Results Through Purposeful Leadership Automation

Effective leadership is the foundation for digital transformation. As agencies embrace modernization, leaders must foster collaboration, build strategic partnerships within the public and private sectors, and articulate a clear vision for change to overcome bureaucratic inertia and resistance.

Voices from the Summit

"Half the battle lies in changing the mindset—from seeing cybersecurity as a roadblock to understanding how it can be an enabler for users and organizations." Vu Nguyen, CISO, DOJ

Pete Amirkhan, Senior Vice President of Worldwide Public Sector at Zscaler, underscored the role of leadership in innovation. "Transformation requires vision, action, and collaboration."

Vanetta Pledger, CIO of the City of Alexandria, shared her approach to achieving city-wide transformation by aligning local priorities with scalable cloud-based architectures. "You're not just introducing a technology change; you're impacting the culture, the way people work, and ultimately creating opportunities they didn't have before."

"The strength of GovRAMP lies in collaboration—between governments, cloud providers, and the public sector—to harmonize compliance and make security achievable. We aim to unify compliance through overlays that reduce duplicative work, starting with CJIS and planning for health information next."

—**FRED BRITTAIN**, EXECUTIVE ADVISOR, GOVRAMP (FORMERLY STATERAMP)

"Partnerships with integrators and best-of-breed technologies are critical for scaling Zero Trust across diverse environments...Zero Trust requires rethinking how organizations, employees, and security teams perceive their roles. It instills a shared responsibility model, emphasizing collaboration and the integration of security across all layers of operations."

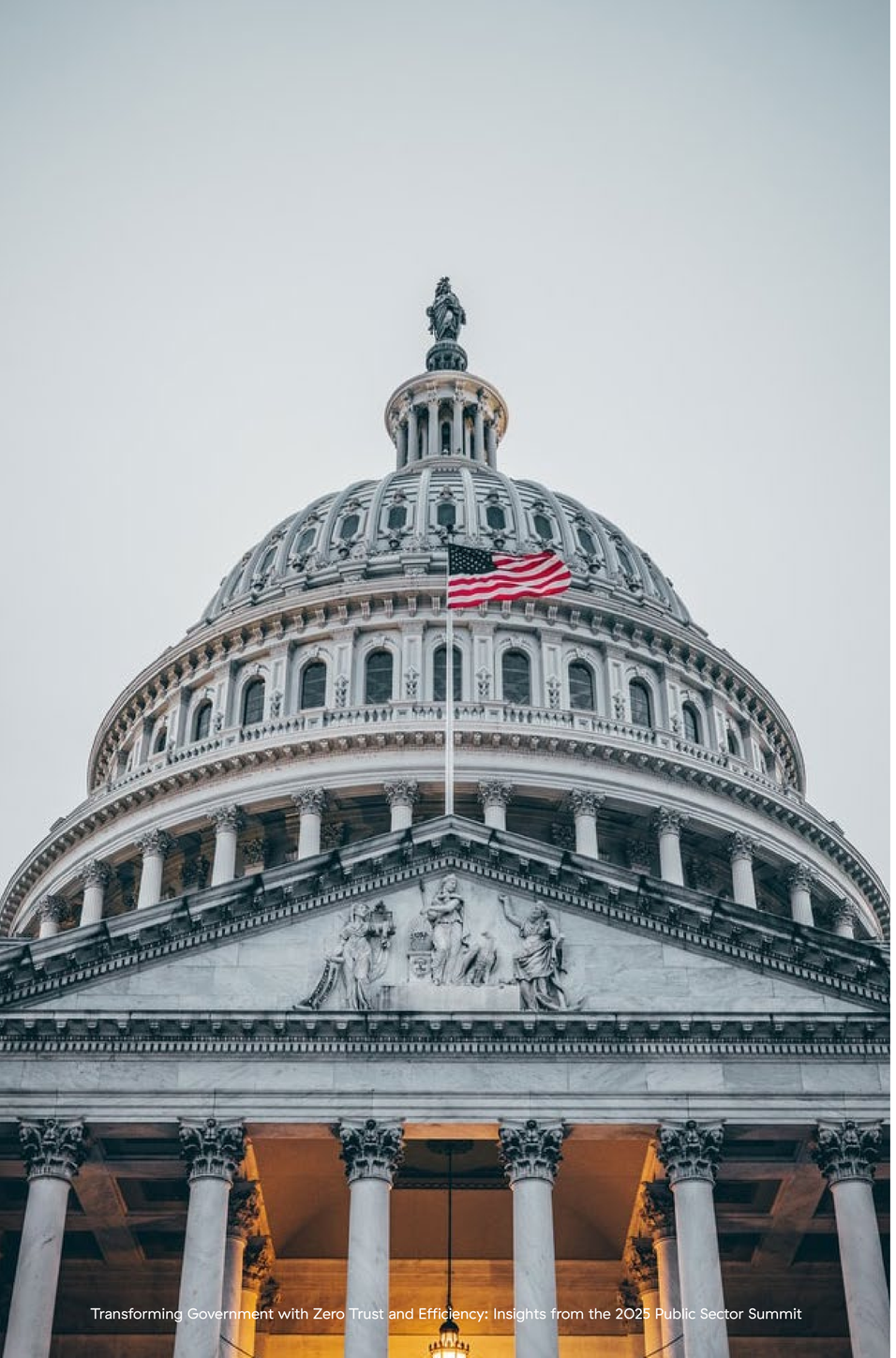
—**KEITH JOHNSON**, TECHNICAL DIRECTOR OF DEFENSE SOLUTIONS, AWS

"[CMMC] is something we need to do as a nation. If we want to protect our lifestyle, we want to protect the way that we in this nation have grown to be the innovators and the leading edge for technology."

—**STACY BOSTJANICK**, DEFENSE DEPARTMENT'S CHIEF DEFENSE INDUSTRIAL BASE CYBERSECURITY AND DEPUTY CHIEF INFORMATION OFFICER FOR CYBERSECURITY

Key Takeaways:

- **Collaborative Ecosystems:** Establishing strong relationships with technology providers and interagency partnerships accelerates rollouts and expands capabilities.
- **Feedback Loops:** Leaders must create mechanisms for continuous improvement and adjust strategies based on real-world experience and data.
- **Visionary Planning:** Leaders must embrace emerging trends like AI, hybrid work models, and digital delivery systems to anticipate future demands.



Conclusion

Building the Foundation for Tomorrow's Government Services

The insights shared at the 2025 Public Sector Summit weave a cohesive narrative of transformation, resilience, and innovation. Public sector leaders at the federal, state, and local levels are navigating an era defined by accelerating digital change, growing cybersecurity risks, and ever-evolving citizen expectations. From embracing Zero Trust Architecture and generative AI-driven defense systems to optimizing operations with cloud technologies and automation, the roadmap to a secure and forward-thinking government has never been clearer.

Modernization isn't merely about deploying new technologies—it's about fostering collaboration, maintaining adaptive leadership, and ensuring operational continuity amid disruption. Whether safeguarding critical infrastructure, mitigating cyber threats, or delivering seamless government services, agencies must adopt holistic strategies rooted in the practical lessons discussed during the summit.

As we move forward, public sector organizations have the opportunity to redefine government operations for the better. Through shared vision, strategic implementation, and a commitment to innovation, these agencies can rise above today's challenges to deliver secure, resilient, and future-ready services.

Let the ideas in this ebook serve as inspiration and guidance for leaders stepping boldly into this transformative era. Together, we can build the secure and efficient governments that citizens trust and depend on.

To dive deeper into the discussions and insights, watch the 2025 Public Sector Summit sessions on demand. Hear directly from industry experts and government leaders as they share their vision for transformation and security across the public sector. Access the recordings at Zscaler Public Sector Summit On-Demand.

Zero Trust Everywhere

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**