GovCIO MEDIA & RESEARCH

DeepDives

Zero Trust

INSIDE:

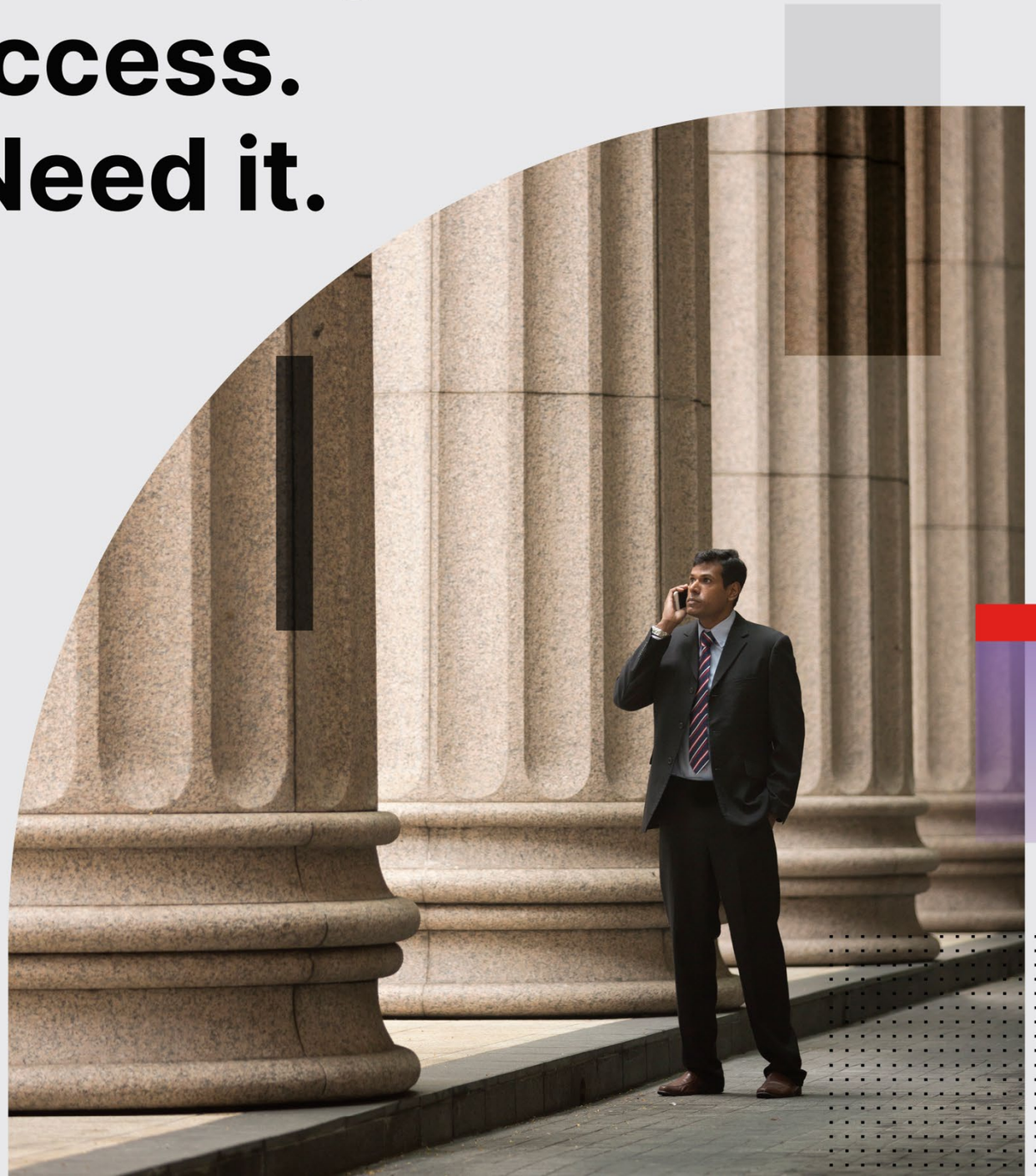
SPONSORED BY FORTINET FEDERAL®

FORTINET FEDERAL®

Increase Agency Security with Zero Trust Access. Everywhere you Need it.

Protect the possibilities with Fortinet Federal.

www.FortinetFederal.com



GovCIO MEDIA & RESEARCH

From the editor's desk

Amy Kluber, Editor-in-Chief

"In essence, zero trust means you trust no one"

An evolving technology landscape that incorporates more remote and cloud environments presents opportunities for malicious actors to breach those virtual walls.

Recent high-profile cybersecurity attacks have drawn attention from the highest leaders in federal government, leading to a White House call for agencies to strengthen their cybersecurity strategies and develop a plan of action for implementing zero trust architectures in their networks.

In essence, zero trust means you trust no one. As federal agencies draft and execute their zero trust strategies, starting with standing up identity solutions, technology-focused leaders are gearing up to enable a safer tomorrow.

Table of Contents

Kate Macri, Senior Staff Writer

Sarah Sybert, Staff Writer

What is Zero Trust? Federal Agencies Embrace Cybersecurity Innovation

From buzzword to White House imperative, zero trust can be a confusing but necessary concept for security strategies.

BY KATE MACRI

Zero trust is a popular buzzword in cybersecurity and federal IT, but still it is fraught with confusion. Sometimes it's misunderstood as a tangible product or a tool, but rather zero trust is a philosophy and approach to cybersecurity rooted in the idea that no users or devices can be trusted and all must be constantly verified in order to gain access to a network or IT system.

What is zero trust?

Stephen Marsh, an associate professor at the University of Ontario Institute of Technology, conceived the term "zero trust" in a paper on securing IT systems in 1994. The term gained popularity in 2018 when the National Institute of Standards and Technology (NIST) released a special publication titled "Zero Trust Architecture," which outlines the basic principles of a zero trust approach to cybersecurity that the IT community understands today.

"Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources," according to the NIST publication. "Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."

Microsoft describes zero trust as a new security model that "effectively adapts to the complexity of the modern environment," which includes cloud-hosted platforms and networks and mobile users.

"At its core, [zero trust is] taking a lot of principles that have been around for a long time and implementing them well, for a change," said former U.S. Customs and Border Protection CISO Alma Cole at the RSA Conference in April 2021. "You're talking about taking that security principle of least privilege access, rolling that out, and actually implementing that in a comprehensive way across your environment and users."

The Department of Homeland Security, especially the Cybersecurity and Infrastructure Security Agency (CISA), aggressively pushes zero trust adoption at federal agencies to better secure federal networks. NIST and CISA lead the federal IT community in zero trust education, research and support.

Photo Credit: matejmo/iStock

Alma Cole

Former CISO, Customs and Border Protection

What does zero trust mean for contractors?

President Joe Biden's cybersecurity executive order requires federal agencies to come up with a plan to shift to the zero trust model of cybersecurity within 60 days of the order, which was July 11. The executive order charges the head of each federal agency with implementing a zero trust architecture at their agency and providing a report on their progress to the director of the Office of Management and Budget and the assistant to the president for national security by July 11.

Many IT vendors working with the federal government have already adopted a zero trust approach to cybersecurity, but now zero trust is an imperative. Federal contractors will need to ensure they're developing IT solutions consistent and compatible with a zero trust approach to cybersecurity.

What is the industry perspective on zero trust?

In many ways, industry has led the way in zero trust implementation. Top IT and cyber vendors like Fortinet Federal, Microsoft, CrowdStrike, IBM, Forcepoint and Palo Alto Networks provide their own zero trust explainers for clients curious about their zero trust approach.

According to a 2020 Cybersecurity Insiders Zero Trust Progress Report, 72% of IT organizations plan to assess or implement zero trust practices in 2020, although 47% are "not confident" in applying a zero trust security model to their business processes, compared to 53% who are confident.

Which federal agencies have deployed zero trust architecture?

Most federal agencies have already deployed or are now in the process of deploying a zero trust approach to cybersecurity. To learn more about federal agencies' zero trust plans, head to https://govciomedia.com.

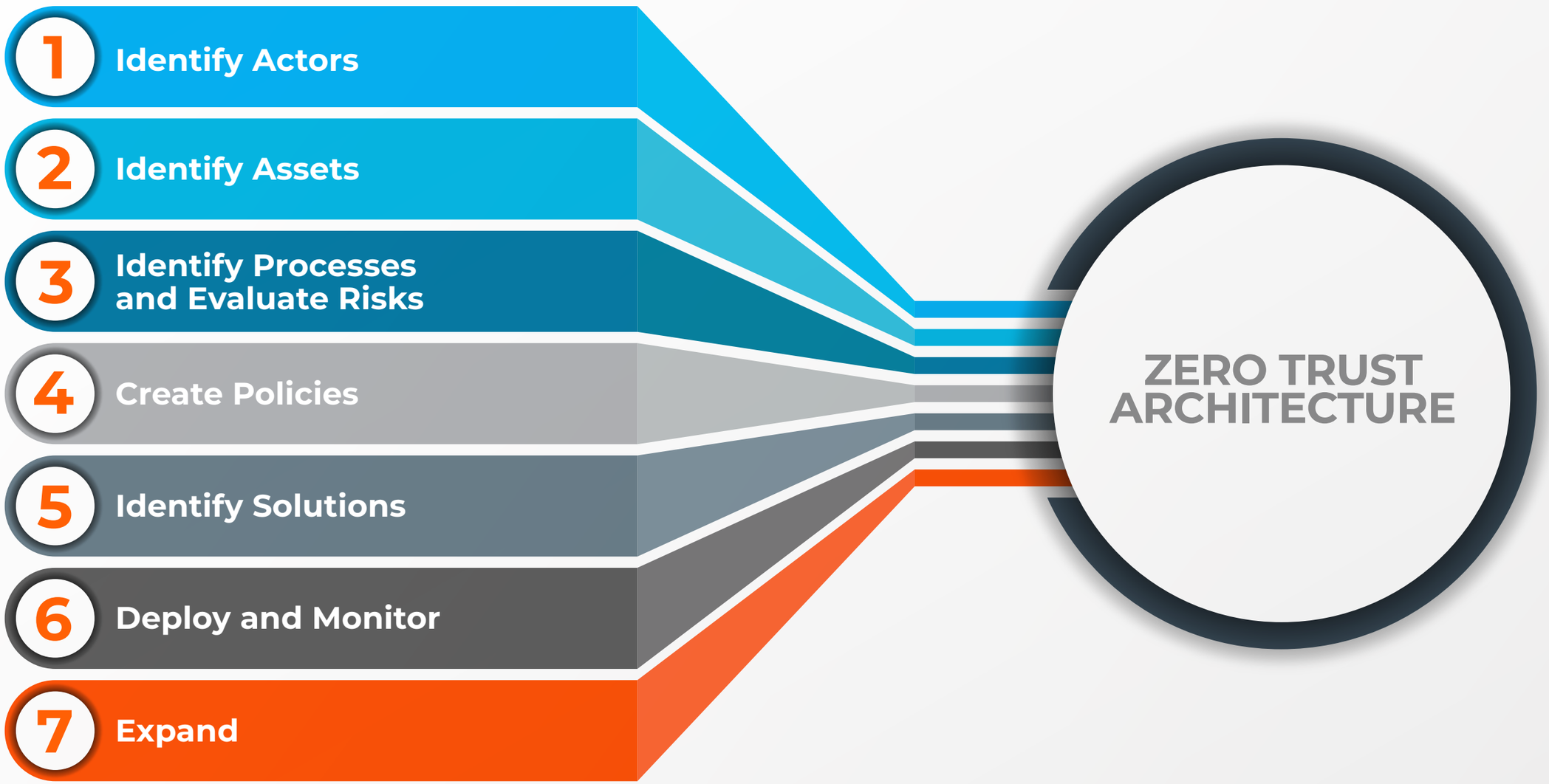
“At its core, [zero trust is] taking a lot of principles that have been around for a long time and implementing them well, for a change.”

—Alma Cole, Former CISO, Customs and Border Protection

GovCIO MEDIA & RESEARCH

DeepDives

Steps to Zero Trust Architecture in a Perimeter



Source: National Institute of Standards and Technology

FORTINET FEDERAL

GovCIO MEDIA & RESEARCH

FORTINET FEDERAL INTERVIEW

Zero Trust is a Balanced Approach to Security, ID Solutions

With modernized technology systems, increased remote access to those systems and a cybersecurity executive order in place, the pressure for federal agencies to advance zero trust architectures is real.

Fortinet Federal Senior Director of System Engineering Felipe Fernandez

Current sentiment around zero trust is positive. Many federal leaders agree it's absolutely necessary to maintaining strong security approaches in an age where data sharing and remote access to systems will continue to grow.

But zero trust is not a product you can buy, implement once and then forget about it, as security solutions provider Fortinet Federal noted. Getting to zero trust is a journey and requires a strong combination of three elements: technology, process and culture.

Fortinet Federal Senior Director of System Engineering Felipe Fernandez provides a rundown of the state of zero trust in the federal government and how organizations get support agencies in their zero trust journeys.

What trends in the security landscape do you see having great impacts to federal security strategies?

Felipe Cybersecurity trends and bad actors are getting more sophisticated; they're not just going after low-hanging fruit anymore, they are going after targets that have the highest impact, seeking the highest return on investments for themselves.

Another trend is users are everywhere now, many are working from home, which means we have new threat vectors. With the zero trust model we can answer questions like, how do we validate remote users' identities, how do we secure their access to resources that could be in a public cloud or on-prem datacenter?

(ctd.)

“Emerging use cases and the technologies that support them also usher in novel threat vectors and attacks; a Zero Trust Architecture is the only strategy that allows organizations to adopt new systems to transform user experience at the speed of business while mitigating the inherent security risks to sensitive assets.”

—Felipe Fernandez, Senior Director of System Engineering, Fortinet Federal

How should organizations approach zero trust?

Felipe Strong authentication is critically important and to their credit organizations are treating it as such. But they also need to consider investing in tools for visibility and faster response to potential threats.

Any organization moving to zero trust should have three priorities:

- Managing identity and access as well as the tools and the processes around identifying users’ applications and devices.
- Implementing tools that provide the visibility into what those users, devices, and applications are doing. It’s not just important to know who or what is on the network, but also that their activity is authorized.
- Quickly responding to anything that’s deemed questionable or malicious and being able to mitigate first and remediate as soon as possible.

What are some of the challenges you’re seeing in this space right now?

Felipe The real challenge right now is inundating the community and the security professionals with jargon and terminology that is ultimately confusing them on the appropriate next steps. It’s important to boil it down to the capabilities that organizations need for zero trust solutions, and understand exactly how a vendor can support an agency’s zero trust strategy.

When it comes to zero trust, what are your goals in 2022?

Felipe In order to ensure our federal government customers implement zero trust swiftly and effectively, and comply with the executive order enabling the cloud adoption, we are going to continue offering the most cost effective, highest performing network and security modernization technology in the market. With the Fortinet Security Fabric we can eliminate legacy technologies, and consolidate network architecture while adding zero trust capabilities anywhere organizations need them.

GovFocus: Navy Tackling ID Solutions Toward Zero Trust Goal

The service's cyber chief says identity management is key to fulfilling a zero trust strategy.

BY KATE MACRI

Zero trust is not a "silver bullet" to good cybersecurity, but can define cybersecurity conversations and strategies so as to gradually improve cybersecurity overall, according to new comments from cyber experts at the Navy and data company DLT Solutions.

DLT Chief Cyber Security Technologist Don Maclean and Navy Principal Cyber Advisor Chris Cleary discussed the White House Executive Order on Improving the Nation's Cybersecurity and some of the common pitfalls federal agencies might encounter when deploying zero trust in a new GovFocus interview with GovCIO Media & Research.

"Zero trust is a mindset change, it's not a matter of fixing everything, we're never going to get there," Maclean said in the GovFocus interview. "Most security technologies are commensurate with or supportive of zero trust. If that provides a north star or general mindset for approaching security, that's where its value lies. You're never going to get to the complete zero trust finish line."

Cleary said the group of individuals leading federal cyber policy — such as himself and the Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly — came from either the National Security Agency (NSA) or U.S. Cyber Command (USCYBERCOM), leading to commonalities in the current approach to federal cyber policy.

Cleary said organizations should treat zero trust like a mindset rather than as a set of rules or tools. The Navy will roll out a new identity management this year,

which Cleary said will lay the groundwork for zero trust.

"The Navy like the rest of DOD is pursuing an ICAM strategy right now and we were pursuing this prior to zero trust being a big thing," he said during the interview. "Identity is fundamental to a zero trust strategy. If you don't have a good identity strategy or architecture you're never going to get to a zero trust architecture. They're codependent. Zero trust has further accelerated our need for identity, it's not a pet project anymore."

Cleary and Maclean both identified culture change as a major hurdle to

implementing zero trust across the federal government. For example, the zero trust concept of least privilege, which involves limiting access and privileges to only the ones an employee needs to do his or her job, can be jarring to some organizations.

"Least privilege is one of the many essential components of zero trust," Maclean said. "All human systems and users only have the privilege they need to do their jobs. I've been involved in least privilege exercises, and what you find is, often, with the hurry to get things done, excessive privileges are given and you don't want to sit there and parse out what they don't need. Once people have privilege, they feel privileged and important. Rescinding those privileges becomes an exercise in human management and knowing what they actually need to do their jobs. That's just one example of the types of cultural things that will be difficult in implementing a zero trust program."

Funding is another issue.

"The executive order sets a tone and encourages certain sets of behaviors, [but] they don't come with the most essential piece of the puzzle, which is money," Maclean said. "My hope is the EO will set the tone and orientation for all of government and the requisite funds and staffing will become available to support that initiative."

Cleary discouraged federal agencies from treating zero trust as an all-or-nothing approach to cybersecurity. This kind of approach isn't very effective because it treats cybersecurity as if there is an end goal in mind, something Cleary said isn't realistic or resourceful. The Defense Department's "comply-to-connect" policy, he said, was treated like "the thing that was going to save us" in terms of cybersecurity until security professionals "move[d] on to the next shiny thing," which could happen with zero trust.

"This is not the last security architecture we're ever going to have," he said. "It wasn't that long ago that this would have been a comply-to-connect discussion. That was the thing that was going to save us. We're coming to the conclusion that

“Identity is fundamental to a zero trust strategy. If you don’t have a good identity strategy or architecture you’re never going to get to a zero trust architecture.”
— Chris Cleary, Principal Cyber Advisor, U.S. Navy

that’s a really really hard task. Not that zero trust is the next shiny thing, but conceptually, is it better to get to 100% [of comply-to-connect] or stop what you’re doing and try to get to a zero trust strategy? I think that’s a lot of what the debates are in organizations. How long is it going to take us to roll out a zero trust architecture at scale in the department?”

Cleary compared cybersecurity to the “War on Poverty” or the “War on Drugs” — “perpetual problems that are never going to be solved.” Their strategies should reflect that. He also said cyber risks and vulnerabilities should be prioritized and addressed like barnacles on a ship — you can’t always remove all of them, but you can address the ones that keep you from running the ship.

“There’s never going to be an architecture that’s rolled out and adversaries are like, ‘Whelp they have zero trust, we better go home,’” he said. “This is a perpetual problem that we need to manage, there’s never going to be a silver bullet. I’m never going to scrape all those barnacles off, but I’ve got to get the ones that are going to impact me the most.”

Both Cleary and Maclean are optimistic about the future of federal cybersecurity given the recent shift in mindset in response to last year’s barrage of cyberattacks.

“People are realizing that what we’re doing is not really working … it’s clear that what we’re doing now isn’t working so we do need a comprehensive approach from the ground up,” Maclean said. “A lot of technologies in zero trust are not just foundational to zero trust, they’re foundational to good security. The goal of zero trust is not zero trust, it’s to make your security program better.”

Agencies Pivot Cybersecurity Strategies to Meet New EO Requirements

GAO, VA and NASA address how they're implementing robust security frameworks to align with a recent executive order.

BY SARAH SYBERT

Technology leaders at the Government Accountability Office (GAO), Department of Veterans Affairs (VA) and National Aeronautics and Space Administration (NASA) are bolstering cybersecurity strategies to meet cross-cutting federal cybersecurity goals.

Following President Biden's Executive Order on Improving the Nation's Cybersecurity, federal agencies reevaluated what it means to be "secure," and implement new models like zero trust to take a more proactive approach on cybersecurity.

"We're trying to move to a software-defined network access infrastructure. This is going to provide us with the micro-segmentation that we need, and it lays out a critical foundation as we move toward zero trust," Mike Witt associate chief information officer for Cybersecurity & Privacy Division at NASA said during a FedInsider webinar.

Improving supply chain security is a top priority for NASA. The agency first started developing supply chain risk assessment capabilities in 2013, and created an Assessed and Cleared List to identify suppliers, components, products and services that have proactively undergone supply chain assessments and meet NASA's implemented thresholds.

NASA also developed continuous monitoring for approvals to have real-time data on these assessments, should statuses change. Witt recommended other agencies develop a community of practice to share best practices and

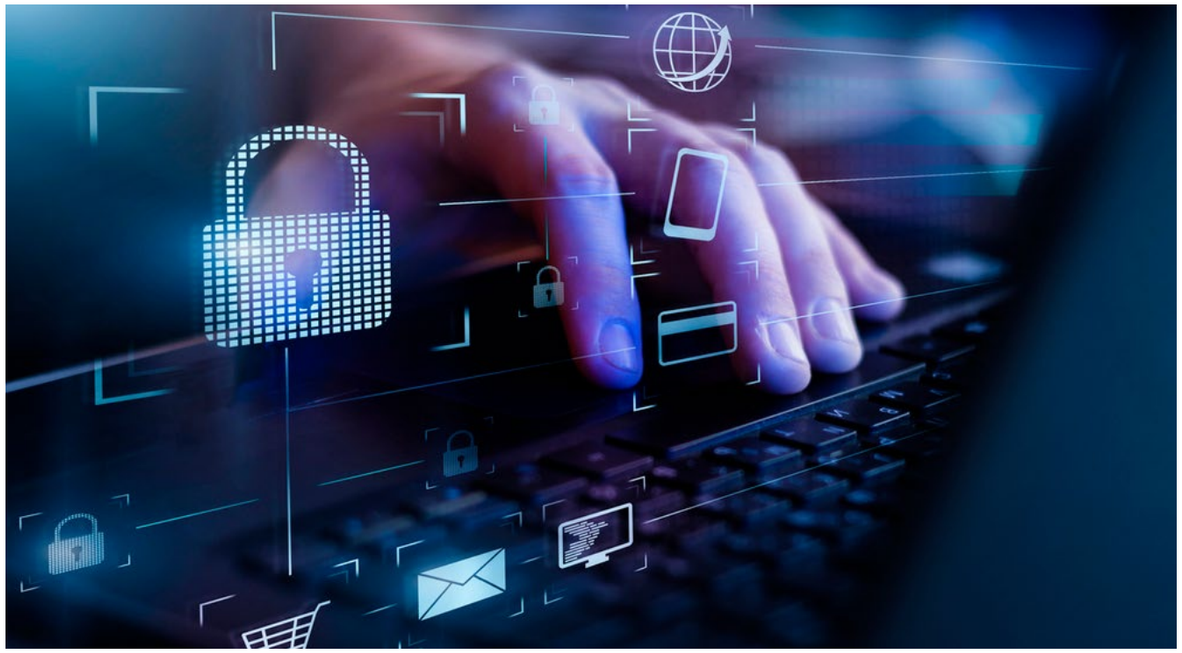


Photo Credit: Traitov/iStock

experiences, as well as common supply chain terminology to better understand supply chain standards, processes and procedures.

"This is important as you work across the inside of your organization," Witt said. "You need to understand what that terminology is and how your processes work."

Jennifer Franks, director of IT & Cybersecurity at GAO, said her agency integrated the EO's terminology so it could effectively implement and understand the new requirements. Franks works to ensure other federal agencies have a "third party context" to Congress to highlight cybersecurity implementation progress as

well as challenges.

"We work with Congress to understand how agencies are progressively improving, or not, and where some of those outliers are," Franks said. "Bringing all of those stakeholders to that environment to understand what is needed to really be invested into this new zero trust architecture and the supply chain movements of your organization."

Franks recommended agencies leverage the tools they have, like IT services, then streamline reporting requirements to align with the goals in the cybersecurity EO. Agencies also need to appropriately document cybersecurity costs, and develop a "risk-based budget projection" to help with planning and response efforts.

At VA, Gary Stevens, executive director for Information Security Policy and Strategy, said COVID-19 required his agency to leverage existing capabilities and expand upon them to meet the increased demand for secure virtual services to veterans.

"It helps put things in context, and then align it accordingly with some of the EO objectives," Stevens said. "That's been one of the major pushes that we've done to make sure that we're making the most sense of what we already have, filling in the gaps where we need to, and then addressing it accordingly and moving forward."

Looking ahead, Stevens sees the EO as a "gamechanger," and said the VA will integrate the goals of the EO into its decision-making process.

"[The EO] really does propel the overall cybersecurity state across all the federal space. The ones that I think are really the most crucial in that realm are zero trust architectures and then what we'll be able to do across cloud," he said.

“We’re trying to move to a software-defined network access infrastructure. This is going to provide us with the micro-segmentation that we need, and it lays out a critical foundation as we move toward zero trust,” —Mike Witt, Associate CIO for Cybersecurity & Privacy Division, NASA

CYBERCAST

Zeroing in on Zero Trust - HHS OIG's Plan to Boost Cybersecurity

The agency is working on the methodology behind implementing robust strategies to secure its systems and supply chain.

Featuring: Gerald Caron, CIO, HHS OIG

Federal agencies are taking charge in implementing zero trust strategies amid a Biden executive order to boost security amid recent incidents. The Department of Health and Human Services' Office of Inspector General's new CIO, Gerald Caron, discusses how zero trust and software supply chain risk management anchor not only his cyber strategy around agency audits, but also that of the entire federal government.

Listen to CyberCast on Apple Podcasts, Google Podcasts, Spotify, or wherever you listen to podcasts!