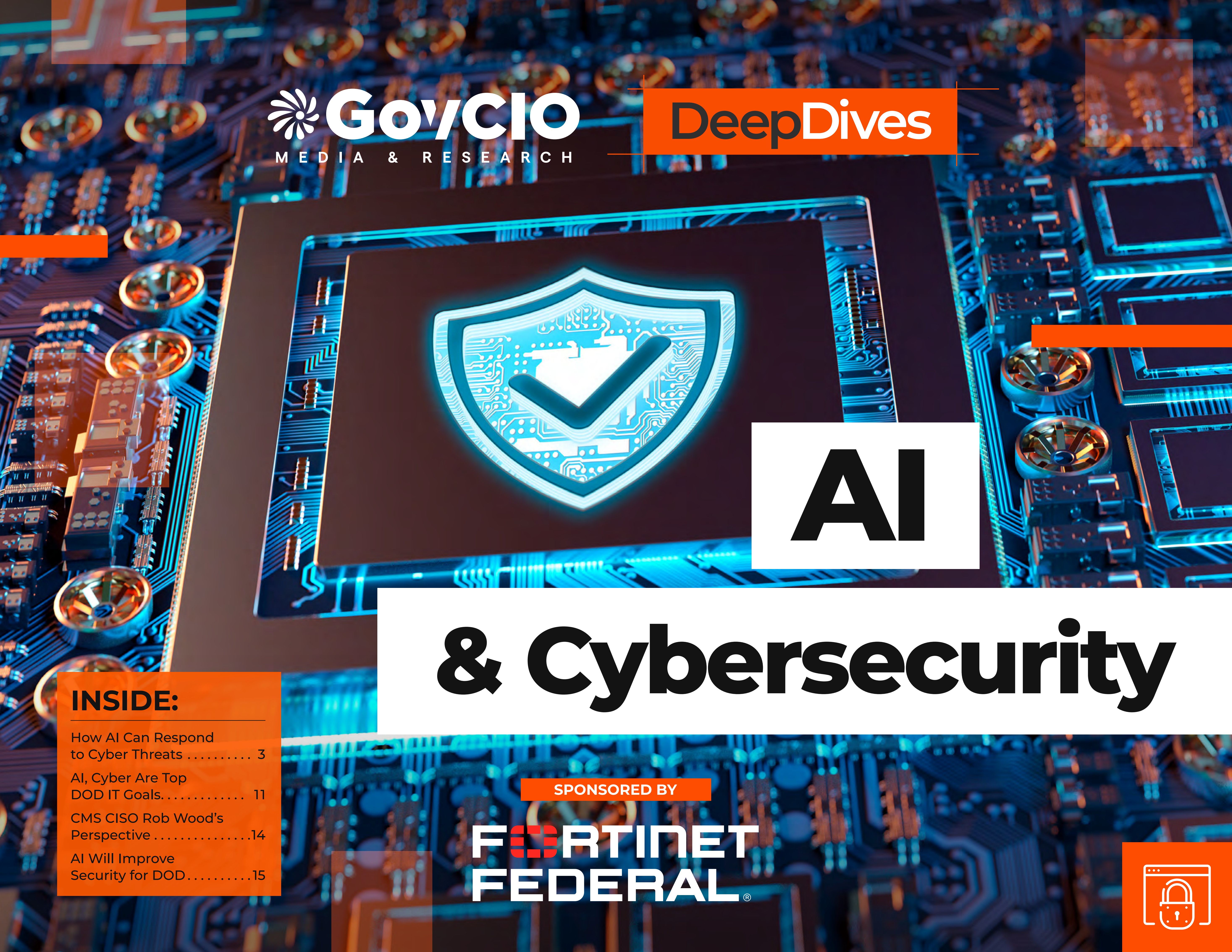
GovCIO
MEDIA & RESEARCH

DeepDives

AI & Cybersecurity



INSIDE:

SPONSORED BY

FORTINET FEDERAL®

GovCIO
MEDIA & RESEARCH

From the writer's desk

Kate Macri, senior staff writer

AI and Cybersecurity Define the Future of IT

The IT infrastructure of the future relies on the successful marriage of AI and cybersecurity. AI can automate security responses and solutions to respond to cyber threats as they happen, and streamline the user experience when users log on to networks and systems securely. Similarly, new technologies — such as data-collecting sensors — need intelligent cyber protections in place to avoid mission compromise.

The COVID-19 pandemic-induced shift to remote work forced many federal entities to re-evaulate cyber protocols and IT infrastructure investments. For some agencies, it meant total IT overhaul to meet new mission needs.

As civilian and defense agencies modernize their networks and IT systems, they're interfacing with industry to harmonize best cyber practices with emerging technologies for total, secure digital transformation.

Table of Contents

Kate Macri,
Senior Staff
Writer

Michael Hoffman,
President,
GovCIO Media
& Research

AI is Helping Secure Critical Infrastructure

Use cases for the technology are enabling full national security protections across government.

BY KATE MACRI

The Cybersecurity and Infrastructure Security Agency (CISA) looks at artificial intelligence from three perspectives: how the agency itself can use it to accomplish its mission to protect critical infrastructure, how critical infrastructure stakeholders plan to deploy AI, and how adversaries may use AI.

Martin Stanley, branch chief for strategic technology at CISA, said these three perspectives anchor CISA's strategy to incorporate AI into cybersecurity practices and processes.

“We're building out an infrastructure where we can rapidly deploy and determine the feasibility of various analytics and use them against live data and collaborate with our partners in critical infrastructure and the federal civilian space,” Stanley said during a November 2021 GovCIO Media & Research event.

Cybersecurity and national security are interwoven and often synonymous in national strategies as nation-state actors increasingly use cyberspace to undercut American critical infrastructure. Stanley said CISA wants to use AI to “reduce the burden on cyber defenders” as the rate of cyberattacks soars.

“The time to respond is getting below what humans can actually do,” he said at the event. “So obviously automation, AI is going to support our leadership to get the information they need to determine decisions and direct response and put in place protections and mitigations when threats are realized. The best thing we can do for our leadership today and tomorrow is put in place an infrastructure that gives them the information they need to make good and effective decisions in our mission space.”

AI is also an instrumental tool at Special Operations Command (SOCOM), where it could help analysts detect threats and make decisions in milliseconds, said SOCOM Chief Data Officer Thomas Kenney.

“The human solution doesn't exist anymore,” he said on a prior panel at the

Photo Credit: ipopba/iStock

Martin Stanley

Branch Chief, Strategic Technology

event. “The capabilities that we need to be able to deploy on the cyber warfare landscape in particular have got to be intelligent systems … that have the ability to learn, to see trend analysis, to be able to recognize in seconds, even milliseconds, the potential for an attack, a foreign attack or a breach and be able to make decisions.”

From an acquisition perspective, SOCOM is thinking about AI technologies in terms of how they are are actually learning. This means getting the foundations in place first to train models on complete and accurate data.

Over the past 20 years, CISA and more broadly the Department of Homeland Security have integrated cybersecurity into their IT systems. The lessons learned from this work informs CISA’s strategy for incorporating AI.

“We need to determine, what are the skillsets that we need, and we’re actually doing that as part of the DHS AI strategy,” Stanley said. “We’re doing implementation plans around that now. A lot of those … mirror the lessons learned from cyber and make sure we mitigate some of the things that didn’t work so well. We’re going to have entirely different teams when this technology gets integrated into operations.”

For federal agencies interested in implementing AI, Stanley advised developing use cases and “rules of the road” for successful implementation.

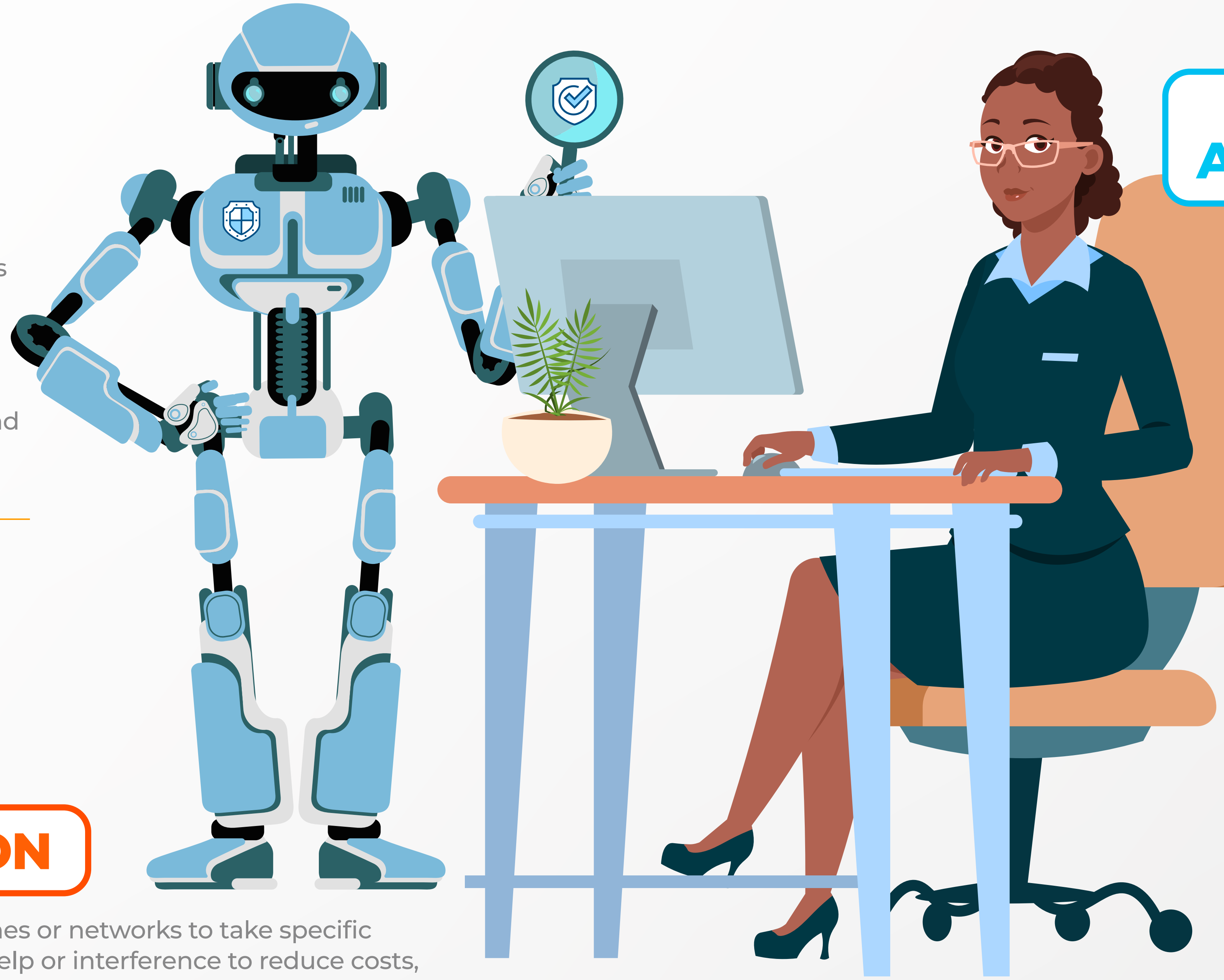
“Choose high-impact and low-regret kinds of scenarios to automate [with AI],” Stanley said. “If it doesn’t go well you don’t want to regret it big time. You want to identify use cases that are easily understandable so you can deal with that ‘explainability’ concern and things that don’t have a lot of complexity.”

> "The best thing we can do for our leadership today and tomorrow is put in place an infrastructure that gives them the information they need to make good and effective decisions in our mission space."
>
> — Martin Stanley, Director, Strategic Technology, CISA

GovCIO MEDIA & RESEARCH

DeepDives

How AI Improves Cybersecurity



ZERO TRUST

An approach to cybersecurity that focuses less on protecting a network perimeter and more on protecting the data on the network by controlling user access and continuously monitoring network activity.

AI can help manage machine identities.

AUTOMATION

A way to program machines or networks to take specific actions without human help or interference to reduce costs, human error, and the time taken to complete tasks.

Automation is often best applied to rote tasks and can allow human workers to focus on more complex projects and tasks.

MULTI-FACTOR AUTHENTICATION

The process by which a network verifies a user's identity before allowing access to the network.

AI can constantly monitor a user's behavior to detect breaches.

THREAT-HUNTING

The practice of actively searching for cyber threats on the network, such as malicious code or unauthorized users.

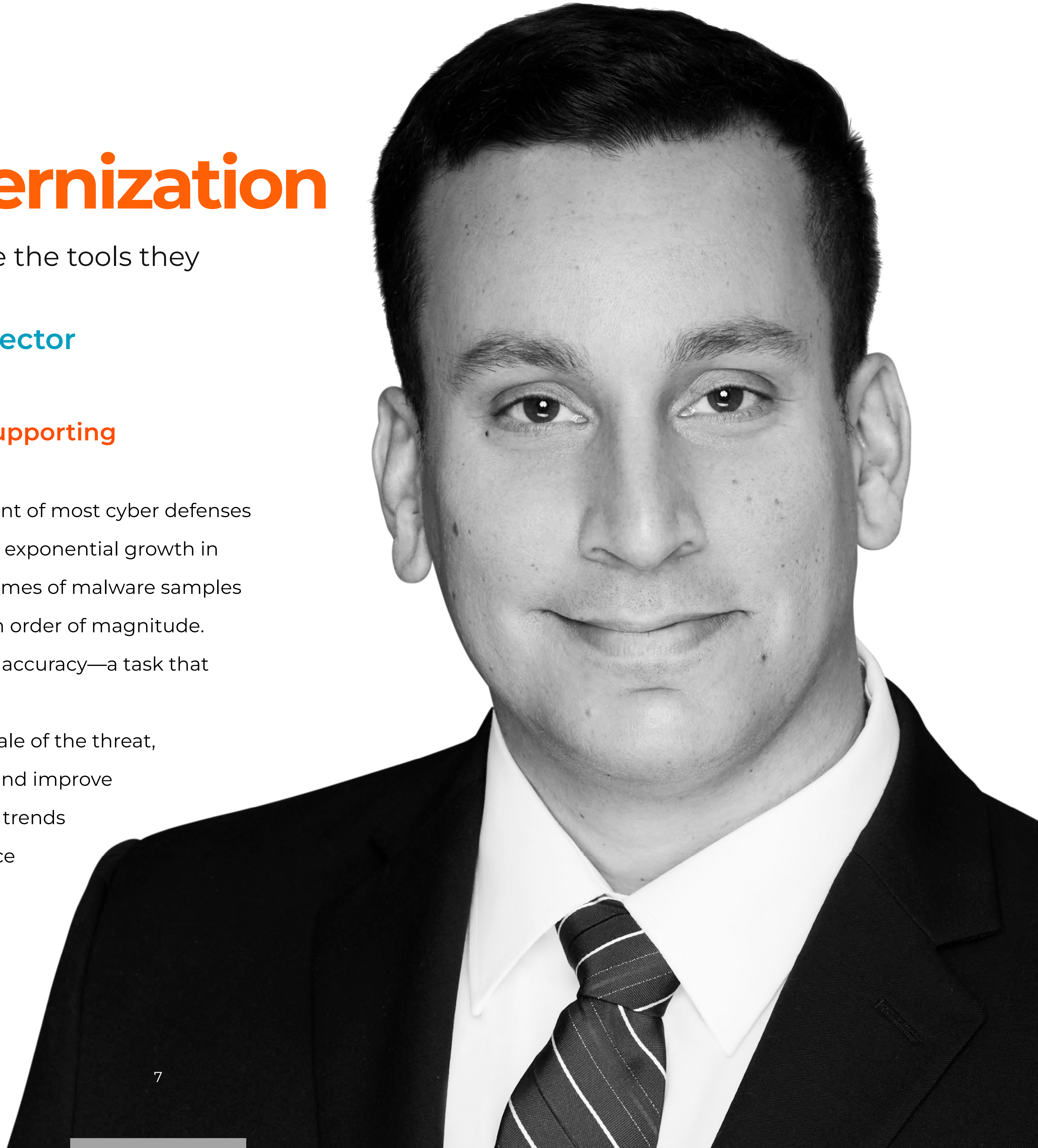
Predictive threat hunting can help identify threats even before they are known by humans.

FORTINET
FEDERAL®

AI's Critical Place in Cybersecurity Modernization

Fortinet Federal ensures cyber professionals have the tools they need to combat sophisticated security threats.

Felipe Fernandez, Fortinet Federal Senior Director of System Engineering



What are some of the advantages that AI has in supporting security efforts?

Fernandez Artificial intelligence became an essential component of most cyber defenses amid the advent of heuristic and adaptive malware, which produced exponential growth in malware variations almost overnight. Today, AI can process high volumes of malware samples and malicious vectors faster and more accurately than humans by an order of magnitude. FortiGuard AI analyzes millions of samples per day with near-perfect accuracy—a task that would normally require thousands of human analysts.

In addition to giving cyber professionals the tools to meet the scale of the threat, AI enhances traditional security solutions to help increase vigilance and improve threat detection, reduces time to detect and can even predict threat trends based on historical data. These capabilities are critical to keeping pace with the increasing use of AI by criminals to circumvent protective security measures such as to solve CAPTCHAs and bypass authentication measures or gather open-source intelligence at scale to facilitate attacks.

(ctd.)

> **“AI can help alleviate the pressure on the government cyber workforce by providing a wealth of actionable threat intelligence.”**
>
> **— Felipe Fernandez, Fortinet Federal Senior Director of System Engineering**

How is AI supporting federal cybersecurity strategies?

Fernandez Some tools such as robotic process automation are already in use among government agencies. RPA is used to automate rote tasks while minimizing the incidence of error by using fixed rule sets for standard inputs — for example, NASA deploys RPA “bots” to transfer data from encrypted emails to internal systems. AI takes RPA to the next level by learning new rules on the fly, thus its potential for cyber applications in government extend far beyond speeding up administrative work securely.

The Technology Modernization Fund, a GSA and OMB-administered funding vehicle aimed at expediting the implementation of innovative technology solutions, supports several projects advancing the use of AI across the federal government, including leveraging AI to advance zero trust. As part of this effort, GSA will seek to adopt AI-driven algorithms to connect diverse data sources, highlight threats and strengthen cyber supply chain risk management and ultimately enhance security operations centers to include governmentwide public-facing digital services.

How can government be best positioned to unlock AI’s full potential for cybersecurity?

Fernandez In the near term, AI can help alleviate the pressure on the government cyber workforce by providing a wealth of actionable threat intelligence, allowing cyber defenders to focus on complex decisions that require human expertise and alleviating workforce burnout. In the long run, however, agencies should look beyond AI’s immediate gains to its paradigm-shifting applications. Married with automation, data analytics, machine vision and natural processing, AI has the potential to power ecosystems and platforms of interoperable security across the federal government.

What are some of the challenges to work through in the federal environment for integrating more robust AI capabilities?

Fernandez According to a recent report from FortiGuard Labs, at the end of 2021, organizations faced a relentless barrage of approximately 150,000 individual ransomware detections per week. As the federal government partners with the private sector to mitigate escalating cyberattacks and secure high-value targets such as critical infrastructure, AI can play a critical role in accelerating both threat detection and response.

Despite its promise, AI is only as accurate and effective as the information it has been fed. To build a strong foundation for governmentwide adoption of AI-powered cyber technologies, agencies must work with industry partners to develop a coordinated strategy that effectively manages data and supports the secure sharing of threat intelligence.

Photo Credit: thinkhubstudio

DOD Under Secretary Seeks New Cyber Sensor, Autonomous Flight System

Defense leader Heidi Shyu created a new "strategic capital director" with the responsibility of finding funding for small businesses.

BY MICHAEL HOFFMAN

Defense Department Under Secretary for Research and Engineering Heidi Shyu outlined a few of her wishlist items for new cybersecurity and artificial intelligence programs during her keynote at the Special Operations Forces Industry Conference (SOFIC) in Tampa, Florida.

Like many of the U.S. Special Operations Command (SOCOM) leaders who have spoken at the conference, Shyu focused more of her time highlighting information technology, cyber and intelligence systems programs versus platforms and weapons.

Sitting on stage with Lisa Sanders, SOCOM's director of science and technology, Shyu was asked to identify cybersecurity and AI programs she is excited about. She said she couldn't share too many details because of security clearances, but she did hint at two.

First, she identified the need to further develop AI technologies to fly autonomously in contested airspaces. The military has sought autonomous search and rescue aircraft to fly and pick up critically injured troops behind enemy lines.

Shyu also offered insight into the cybersecurity technologies she wants to use her budget to further develop.

"I'm interested in pushing technology toward developing a single sensor that has the ability to listen, ability to jam, ability to communicate, ability to inject — all in one," Shyu said.

Defense Under Secretary Heidi Shyu addresses attendees at Special Operations Forces Industry Conference (SOFIC) May 18, 2022

Currently, DOD has a wide variety of systems that tackle these security tasks, but Shyu made sure to emphasize that she wants to have one sensor achieve all four — listen, jam, communicate and inject.

Shyu highlighted a new fund called the Rapid Defense Experimentation Reserve. As the name implies, Shyu said the reserve will be spread across DOD to boost experimentation on multiple programs. DOD leaders requested $377

Photo Credit: NDIA

Heidi Shyu

Under Secretary for Research & Engineering, DOD

million over five years to fund the reserve, according to DOD's budget request documents.

Shyu said DOD has already received over 200 white papers seeking funding through the reserve and has kickstarted the process to review those requests and issue funding in 2023.

Similar to the message delivered by SOCOM leaders, Shyu made sure to highlight the need to collaborate with small businesses. She said she visited SOCOM's small business innovation tank, SOFWERX, in nearby Ybor City and came away impressed by the level of integration with users.

However, Shyu said she's worried about small businesses running out of capital after using their funding through the Small Business Innovation Research (SBIR) program.

Shyu said DOD needs to help small businesses find capital to keep their businesses afloat beyond the funding they receive through the SBIR program. She said she's created a new position called the "strategic capital director" with the responsibility of finding funding for these small businesses.

The Air Force has a program, Shyu highlighted in her remarks. She explained how the service matches promising programs with the matching program executive office, which then provides an additional $1 million. The service then connects the company with partner venture capital firms that matches the total funding the company has already received.

"One of the things I'd like to do is take the process and the methodology and let's bring it across DOD," Shyu said.

“I’m interested in pushing technology toward developing a single sensor that has the ability to listen, ability to jam, ability to communicate, ability to inject — all in one.”

— Heidi Shyu, Under Secretary
for Research & Engineering, DOD

GovCIO
MEDIA & RESEARCH

GOVFOCUS

Not Just A Security Team Priority: A Practical Application of Zero Trust

Featuring: Rob Wood, CISO, CMS | **Jim Richber,** Public Sector CISO and Vice President of Information Security, Fortinet Federal | **Kate Macri,** Senior Staff Writer, GovCIO Media & Research

Click here to watch the interview!

Misconceptions and over-simplified language dominate the zero trust conversation, which can be so demanding for organizations looking for the right starting point. Rob Wood, CISO of the Centers for Medicare & Medicaid Services (CMS) and Jim Richberg, Public Sector Field CISO for Fortinet, explore how zero trust is an “insider risk program” and how to customize it so that it’s both transparent and accessible to end-users.

For our full collection of GovCasts, visit our website: https://governmentciomedia.com/govfocus

A ‘Transparent’ User Experience is the Goal of DISA’s Thunderdome Zero Trust Prototype

DISA cyber leaders will prioritize improving the user experience with cybersecurity to allow for seamless, secure network and data access.

BY KATE MACRI

As the Defense Information Systems Agency (DISA) prepares to begin development on its Thunderdome zero trust prototype, which will serve as the new backbone for cybersecurity across the Defense Department, DISA cyber leaders say improved user experience is the end goal.

DISA CIO Roger Greenwell said improving the user experience with cybersecurity is not only critical, but also practical because users will always find “workarounds” if security measures become too burdensome when trying to access data to do their jobs.

Photo Credit: Maj. Holli Nelson/DVIDS

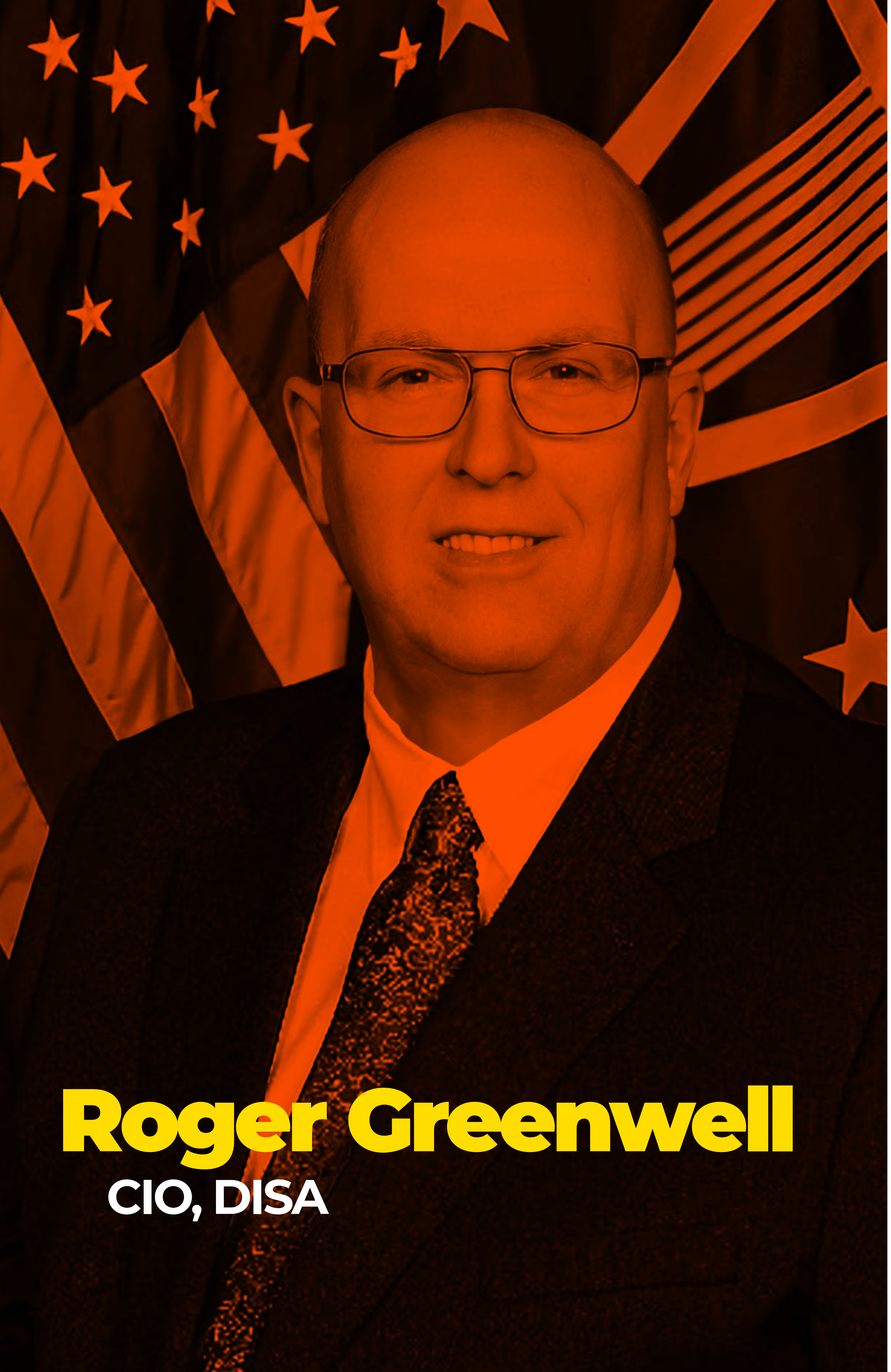
“How do we improve performance on the endpoints and making sure we put the right security on the endpoints? How do you balance security — because people will try to work around security if you make things too difficult, so we want that wide area of security around the network,” he said at the AFCEA TechNet Cyber 2022 conference in Baltimore.

Jason Martin, director of DISA’s Digital Capabilities and Security Center, said manually logging into 17 different systems with different security protocols does not encourage user compliance, which increases the likelihood of security breaches.

“It’s a fundamental rethinking, talking to the user,” Martin said during a TechNet Cyber panel this week. “When you’re out in the field we don’t have time to wait. The adversary doesn’t stop, they innovate minute by minute. I think that’s critical, it’s empowering the workforce.”

During a media roundtable, DISA CTO Stephen Wallace said Thunderdome is the first step toward a user-centric approach to cybersecurity across the DOD enterprise.

Previously, users and data would “sit together” on a given network with a “castle moat” approach to security. The shift to the cloud changed how users



Roger Greenwell

CIO, DISA

accessed the network and data on the network, and the COVID-19 pandemic catapulted DOD into a new data environment where old cyber processes were no longer sufficient.

“When we started with Thunderdome we started with the ways users we operating,” Wallace said. “In 2020 we saw a dramatic shift with the workforce scattering and accessing data in different ways. The network-oriented approach is not the right answer. The original name for Thunderdome was ‘Perimeter Evolution.’”

Wallace said they realized users were struggling to access data on the network in a timely fashion, contributing to what DISA Director Lt. Gen. Robert Skinner described as a “soul-crushing user experience” in his Tuesday morning keynote. This is where he wants industry’s help.

“Thunderdome wasn’t, ‘Hey here’s a new way of doing security;’ it was, ‘Hey, we need to provide a better user experience,’” Wallace said. “We needed to provide users a more direct result to their ultimate destination without backhauling them into the network. So how does that endpoint relate to the other portions of the network back through all the data? It starts to look like an equation — they all start to develop some level of weight. If the endpoint is in a certain condition, then we can start to allow the user access to things and be a lot more flexible about that than ever before.”

Balancing the right levels of security for different users and different data sets is a delicate dance, but a zero trust approach to security is uniquely suited to handle the challenge.

Greenwell said automation, pilots and test efforts will help DISA pinpoint the right security balance to improve user experience.

“How do we take and understand what load are we putting on the endpoints, what’s being driven from a cyber perspective, and using automation to react to the fact that you’re seeing a utilization spike,” he said. “We want the automation to be in place to help us detect those things in real

“How do we take and understand what load are we putting on the endpoints, what’s being driven from a cyber perspective, and using automation to react to the fact that you’re seeing a utilization spike. We want the automation to be in place to help us detect those things in real time and use automation.”

— Roger Greenwell, CIO, DISA

time and use automation.”

Rear Adm. Brian Hurley, director of DISA’s Joint Service Provider, said he’s optimistic about the Thunderdome prototype efforts and how they will impact cybersecurity for the DOD enterprise.

“We’re the end user of Thunderdome, and that coordination is relevant where they are actively trying to implicate and apply that into that environment, so we’re looking forward to that end-user environment,” he said.

DISA is exploring the way forward with Thunderdome, according to Martin. DISA has set up a program office for Thunderdome and discussed parameters for the prototype with the vendor, Booz Allen Hamilton. DISA awarded Booz the $7 million Thunderdome prototype contract in January 2022.

“We’re about to get a whole bunch of new security capabilities,” Wallace said. “We have to be very careful and diligent not to enable every one of those in the name of security. Too much security leads to the user going out of bounds and they will get their jobs done period. We’ve been shown that time after time. The idea is the best security is the security the user doesn’t see and is completely transparent to their experience, and that’s a lot of what we’re going for here with Thunderdome.”