

Federal IT

Trends

in 2024

Outlook

for 2025



INSIDE:

- What is a CAIO?.....3
- Defense tech strategies.....6
- Data progress at HHS.....17

SPONSORED BY



From the editor's desk



Sarah Sybert, Managing Editor

Setting the Stage

Federal IT achievements in 2024 reflect the transformative potential of emerging technologies, particularly artificial intelligence. Across government, agencies have expanded on modernization, innovation and security strategies to enhance efficiency, transparency and mission delivery.

This election year brought new anticipated shifts to the federal IT landscape. As president-elect Donald Trump prepares to take office, fresh federal leadership and approaches to funding, developing and regulating emerging technology will redefine the nation's approach to national security and innovation.

Under President Joe Biden's administration, we saw new policy emerge in 2024 that have shaped the progress with emerging technology. Top of my list is the National Security

Memorandum on Advancing U.S. Leadership in AI, which outlines a comprehensive national security strategy and policy for AI, accompanied by a governance and risk management framework.

Inside, we'll dive into how federal agencies have made significant milestones over the year, harnessing AI to improve workflows and drive operational efficiencies. These advancements reflect a strategic approach to leveraging technology to create a more user-centric and future-ready environment, aligning with agencies' overarching mission objectives.

These efforts highlight federal government's forward-thinking approach to technology, showcasing how innovation can drive mission success and improve public service. 🌟

Table of Contents



Sarah Sybert,
Managing Editor



Ross Gianfortune,
Senior Staff Writer



Nikki Henderson,
Staff Writer



INTERVIEW

A Federal Chief AI Officer's Perspective

Labor's Mangala Kuppa highlights initial priorities in her new chief AI officer role.

BY SARAH SYBERT



ARTICLE

Defense Tech Developments to Watch in 2025

The Pentagon bolsters AI, zero trust and the workforce.

BY ROSS GIANFORTUNE



PARTNER INTERVIEW

Adapting to New Realities of Cyber Threats

Emerging probabilistic computing is showing promise for cybersecurity and artificial intelligence.

Hansang Bae, Public Sector CTO, Zscaler U.S. Government Solutions



ARTICLE

AI and Data Sharing Drive Health Innovation in 2024

Strides in AI and data sharing drive transparency and patient outcomes.

BY NIKKI HENDERSON

A Federal Chief AI Officer's Perspective

Labor's Mangala Kuppa highlights initial priorities in her new chief AI officer role.

BY SARAH SYBERT

This year, the Office of Management and Budget (OMB), under direction from Biden's earlier artificial intelligence executive order, told federal agencies to appoint chief AI officers to oversee AI initiatives and manage associated risks.

The Labor Department (DOL) is leveraging AI to enhance efficiency and workflows as it looks ahead to 2025. DOL Chief AI Officer Mangala Kuppa is working to integrate AI responsibly, while promoting collaboration, innovation and transparency.

In a Q&A with GovCIO Media & Research, she discussed her role, the agency's AI strategy and how AI is being used to create a worker-focused, future-ready environment.

What brought you into the role at Labor overseeing AI?

Kuppa My journey to becoming the chief AI officer at the department felt like a natural progression. For more than two decades, I've held leadership positions in both the public and private sectors, and I also serve as Labor's CTO. My responsibilities include overseeing enterprise architecture, emerging technologies, our enterprise data warehouse solutions and records management. All these areas are integral to AI initiatives.

My academic background also played a significant role in this journey. During my postgraduate studies, I focused on AI and image processing while not realizing at the time how pivotal those technologies would become.



Mangala Kuppa
CTO and Chief AI Officer,
Labor Department

“Centralized governance is critical to ensure we use AI responsibly. This includes identifying and mitigating risks, maintaining transparency and embedding AI into our overall strategic framework.”

— Mangala Kuppa, CTO and Chief AI Officer, Labor Department

I previously was the director of business application services, managing mission systems for 27 DOL agencies. This experience gave me a deep understanding of the challenges and opportunities in technology, which helps me lead AI strategy and implementation at DOL effectively.

Labor’s CAIO role includes defining our AI strategy, engaging stakeholders across different levels and ensuring we implement AI responsibly. It’s a role that requires balancing technological innovation with our mission to serve workers effectively.

How is Labor using AI?

Kuppa We’re leveraging AI to enhance workflows, improve efficiency and ultimately better serve the public. Some of our key use cases include:

- Generative AI tools: We’ve made secure generative AI available to staff, allowing them to summarize documents, draft memos and write emails more efficiently.
- Natural language processing (NLP): We’re using this to convert text to voice for training programs and voice to text for recording interviews, which reduces manual work and improves data accuracy.
- Custom modeling and fine-tuning: By fine-tuning generative AI models with our data, we’re creating applications like auto-coding, which speeds up development processes and enhances productivity.
- Augmented and mixed reality: We’re exploring augmented reality training environments to prepare inspectors for hazardous worksites, improving safety and readiness.
- AI in software development: We’re equipping developers with AI tools to streamline coding, reducing time-to-market for new applications and improving overall project delivery.

These use cases highlight the potential of AI to not only make our work more efficient, but also improve how we serve workers and the public.

How are you addressing skepticism and fear about AI?

Kuppa Communication is key. We're making a concerted effort to educate and engage our workforce through AI literacy programs. Our acting secretary has set a clear, worker-centered vision for AI, emphasizing that its purpose is to enrich jobs, not replace them.

We hold regular training sessions, open forums and discussions to ensure employees feel confident in their understanding of AI. Our goal is for every staff member to have a clear grasp of what AI is, how it can be applied in their roles and the risks involved. When people understand AI from their own perspective, it becomes less intimidating and more of a tool to support their work.

How does DOL partner to advance AI across government?

Kuppa Collaboration is essential, especially with a technology that's evolving as quickly as AI. Within the federal government, I'm part of the CIO Council, chaired by the OMB and the Office of Science and Technology Policy (OSTP). We meet regularly, share ideas and discuss challenges and solutions.

Beyond government, we engage with private-sector vendors, academic

institutions and industry experts to stay informed about the latest advancements. We also share what we've learned. For instance, use cases are shared on AI.gov. This constant exchange of knowledge ensures we're not reinventing the wheel and can build on each other's progress.

How has your agency built a foundation for AI governance?

Kuppa Governance and collaboration are cornerstones of our AI strategy. At DOL, we've established an AI Governance Board, which includes union partners — an invaluable addition to our decision-making process.


We also host monthly forums with all 27 DOL agencies to share updates, ideas and challenges. Additionally, we've created a community of interest for all staff to participate in training sessions and discussions about AI. These forums ensure that everyone, from leadership to frontline workers, is part of the conversation about how AI impacts their work.

Centralized governance is critical to ensure we use AI responsibly. This includes identifying and mitigating risks, maintaining transparency, and embedding AI into our overall strategic framework.

What excites you about the future of AI?

Kuppa I'm an optimist by nature and a technologist at heart, so I'm excited about AI's potential to transform how we work and serve the public. I look forward to seeing AI tackle challenges we once thought insurmountable.

That said, I'm also aware of the risks. AI is a powerful tool, and if not governed responsibly, it can lead to unintended consequences. My primary focus is ensuring we're intentional about using AI for good and aligning its capabilities with our mission to protect and empower workers.

I believe humanity will find a balance. With thoughtful collaboration and governance, we can create a future where AI is not just a tool, but also a force for meaningful progress. 



Defense Tech Developments to Watch in 2025

The Pentagon bolsters AI, zero trust and the workforce.

BY ROSS GIANFORTUNE

Successful implementation of zero-trust cybersecurity strategies in government requires a significant cultural and systemic shift.

The Defense Department is modernizing technology across the enterprise to remain a dominant fighting force worldwide. Its new Fulcrum strategy, artificial intelligence and workforce issues dictated technology talk in 2024 that will likely shape priorities in the new year.

“In the modern battlefield, technology and new innovations are crucial,” said Rep. Adam Smith, ranking member of the House Armed Services Committee, about national security priorities. “We have put a variety of provisions to help move toward [innovation and fielding new technology].”

Fulcrum Plan is the ‘Nexus’ of Strategic Priorities

Released in June 2024, Fulcrum is DOD’s plan to modernize its IT systems and capabilities. The strategy focuses on four key areas: providing joint warfighting IT capabilities, modernizing information networks and compute, optimizing IT governance and strengthening digital workforce.

According to DOD Acting CIO Leslie Beavers, Fulcrum aims to expand strategic dominance, improve efficiency and enable the deployment of emerging



technologies to support the warfighter.

“It is called ‘Fulcrum’ because it sits at the nexus between our national security strategy, our strategic management plans, our really big thinking strategies, our workforce implementation strategies, our software modernization strategies, our cybersecurity strategies, and it gives you tangible steps to take to



turn that strategic vision into an operational reality,” Beavers said during the AFCEA TechNet Cyber conference in Baltimore in August 2024.

DOD Deputy Customer Experience Officer Robert Franzen said that the strategy is a “North Star” for department IT initiatives, bridging the gap between strategies and technology. He emphasized the importance of collaboration across the department for successful implementation of the plan in the coming years.

“It’s an integrated approach where we build upon the workforce, further improve governance, also addressing the big rocks for modernization, which all really leads into the fact that Fulcrum is about leveraging technology as a strategic enabler to improve decision advantage for the warfighter on the battlefield,” Franzen told GovCIO Media & Research.

Zero Trust Implementation Gets Updates

Cybersecurity is a key pillar of Fulcrum and informs the department’s zero-trust implementation goals laid out in the 2021 executive order on cybersecurity.

“To move fast, we want to have zero trust baked in,” DOD Director of Cloud and Software Modernization George Lamb told GovCIO Media & Research at AFCEA TechNet Cyber. “It’s an inherent part of everything we do.”

Similarly, DOD released in June 2024 an updated zero trust overlays document to help department components implement zero trust. The document outlines plans to phase in zero-trust controls and conduct a gap analysis to help DOD reach its goals, according to Will Schmitt, division chief at the DOD Zero Trust Portfolio Management Office.

“Zero trust is a data-centric strategy for security,” Schmitt said. “You’re protecting the data itself. You’re moving that protection boundary from the perimeter right down to what’s critical to be protected, and what that means is that everybody has to be authorized and authenticated to access that piece of information.”

“The overlays are given the ability to quickly determine that 70% and 90% of the controls are in place. They’re there so we can be confident as we operate,” said Lamb of the overlays.

Implementing zero trust at DOD comes with its share of challenges like multiple classification environments. Randy Resnick, director of the DOD Zero Trust Portfolio Management Office, highlighted that there are many ways to implement zero trust.

“You can improve where you have existing in the ground, we call that course of action one. You could do commercial cloud, which we’re engaging in with the [Joint Warfighting Cloud Capability] vendors right now to see whether or not they could do zero trust in their clouds — and that’s aggressively being worked. And of course, action three would be on preliminary private cloud, which we are aware a number of companies are doing on their own,” he said at the GovCIO Media & Research Defense IT Summit this year.

Zero-trust implementation is a cornerstone of the national security mission. National Geospatial-Intelligence Agency CIO Mark Chatelain said that zero trust is essential to protecting against both external adversaries and insider risks during the DoDIIS Worldwide conference in Omaha.

“Zero trust is a very important initiative, and I think it’s going to really have a major effect also on the way that we do cyber defense because we recognize that we’re moving from more network-centric defenses to data-centric defenses,” Chatelain said. “If you assume that the network is compromised, you’re in a much better position.”

Artificial Intelligence is the Future ... and the Present

The Pentagon’s Chief Digital and Artificial Intelligence Office (CDAO) has been working to promote AI modernization initiatives. In September, the office launched its new acquisition plan, the Open Data and Applications Government-owned Interoperable Repositories. Its chief, Radha Plumb, said that the plan will

make buying AI easier for DOD.

“Let’s make a layer cake instead of a vertically integrated stack,” said Plumb. “Let’s figure out how we buy each of those pieces. ... Let’s create some acquisition pathways, both on the prototype and challenge side, and if you’re successful, [it will show] what a scaled enterprise can look like. And then let’s do that in a predictable, repeatable way.”

AI uses more processing power than traditional applications, and Defense components are working to find the computing to run AI systems. They also cost money that is not necessarily in budgets. Collaboration and smart budgeting come together to solve these problems, Space Force Chief Data and Artificial Intelligence Officer Chandra Donelson said at the NVIDIA AI Summit.

“We need industry’s help ... understanding what our compute and infrastructure needs are, and then helping us map out our strategy to be able to scale that across the department,” said Donelson. “We do want to invest





heavily into compute this year for fiscal year 2025. It's something that is a top priority for me."

The Navy is developing more AI and autonomous systems for the future of war, said Chief of Naval Operations Adm. Lisa Franchetti during a Defense Writers Group meeting. The Navy's "Project 33" plan operationalizes robotic and autonomous systems to meet China's technological progress.

"It's pretty clear that, based on what [China President Xi Jinping] has said, his military forces need to be ready by 2027 for war," said Franchetti. "My objective in the navigation plan is to make sure that we are, going forward, fully able to integrate the man-unmanned teaming concepts through these platforms, whether it's under the sea, on the sea or above the sea."

AI development is a "modern-day arms race" for the Defense Department. Emerging tech can be a force multiplier on and off the battlefield, Defense Innovation Unit's (DIU) AI/ML Program Manager Jamie Fitzgibbon said at GovCIO Media & Research's AI Summit.

"The first one to finish gets to write the rules. It behooves us to do it responsibly, but to move fast," said Fitzgibbon.

The Pentagon is finding new ways to use AI to solve new problems. In 2024, DOD launched GigEagle, an AI-powered platform that helps connect short-term tech talent with agencies that need them, to supplement its workforce needs. According to 75th Innovation Command Chief Talent Officer Maj. Craig Robbins, GigEagle can identify hundreds of potential candidates within seconds, making the process significantly faster and more efficient.

"The whole concept of a skills marketplace is new to the Department of Defense," Robbins told GovCIO Media & Research. "It's relatively new to the workforce at large. ... GigEagle aligns with the Army People Strategy by enabling the army to shift from simply distributing personnel to a more deliberate process of managing the talents of our soldiers and civilians, especially those who are serving in the reserve and the National Guard." (ctd.)

The Workforce Drives Security

DOD needs a modern workforce to meet its modernization goals. The Defense Innovation Board unanimously voted in favor of recommendations aimed at driving innovation through personnel and collaboration during the group's July public meeting.

"Innovators often can't get promoted, can't get the good jobs, and in that frustration, they oftentimes leave," said board member Adm. Mike Mullen, former chairman of the Joint Chiefs of Staff. "Leaders have to provide top cover for innovators. We do that as mentors and leaders notionally. But for the 'mavericks' that are amongst us, those that can really bring innovation, we've got to find a place for them, promote them and make sure they have a future to eventually get into positions of leadership themselves."

DOD is short thousands of cybersecurity professionals, according to

Principal Director for Resources & Analysis Mark Gorak. The department, however, is making progress on its cyber workforce strategy implementation plan released last year.

"If you're only operating at 70% of your strength, you are not fulfilling your full mission, and then our workforce becomes overworked and overburdened," Gorak said. "We don't execute as proficiently as we would like. Our goal is above 90% across the board, which is a pretty good goal, and we're at 75% now."

Evolving cybersecurity threats require a modern workforce throughout DOD. Department of the Navy CIO Jane Rathbun told GovCIO Media & Research that her office is leveraging all available resources to secure the entire cyber domain.

"Getting the right workforce — who really understands this environment and understands how to work and improve the control and management of data

Photo Credit: Staff Sgt. Jacob Osborne, U.S. Marine Corps



from a security perspective — is critical,” she said. “We are leveraging the myriad authorities that we’ve been given, ... like the [DOD] Cyber Excepted Service, the cyber workforce, all of our people have been tagged, we are working on training initiatives and really pronouncing more loudly the role that they play in delivering capability to the warfighter.”

A partnership between DIU and the Naval Postgraduate School (NPS) wants to accelerate adoption of commercial tech for national security applications and develop the future leaders to manage said solutions. DIU and NPS signed a memorandum of understanding in April to collaborate on these goals.

“[The memo] facilitates a seamless integration of talents and technologies, allowing NPS faculty and students to gain hands-on experience with cutting-edge defense technologies at DIU, while DIU personnel benefit from NPS’s advanced research resources,” NPS Director of Research Innovation Kaitie Penry told GovCIO Media & Research. “Regular exchanges of personnel and ideas ensure that best practices and lessons learned are shared, accelerating the development of innovative solutions.”

Defense components need to train the workforce to use AI responsibly and effectively. The Innovation Directorate Army Recruiting Command is focusing on education, fluency and literacy to ensure better workforce adoption. The command’s acting director, Col. Kris Saling, said that a data literacy course for members of the workforce has helped staff become more critical consumers of data. The course has been adopted for its professional military education, and now, everyone at the command receives the training.

“You need the folks who are the engineers who are going to build the car, but what do we actually need for the folks who are going to drive it? Or the folks who aren’t necessarily driving it, but they need to know it’s on the road. This leads kind of how we’re tackling that problem,” Saling said at GovCIO Media & Research’s AI Summit. 🌟



“Fulcrum ... gives you tangible steps to take to turn that strategic vision into an operational reality.”

— Leslie Beavers, Acting CIO, Defense Department



Adapting to New Realities of Cyber Threats

Emerging probabilistic computing is showing promise for cybersecurity and artificial intelligence.

What are some of the key challenges that you are currently seeing in the public sector space?

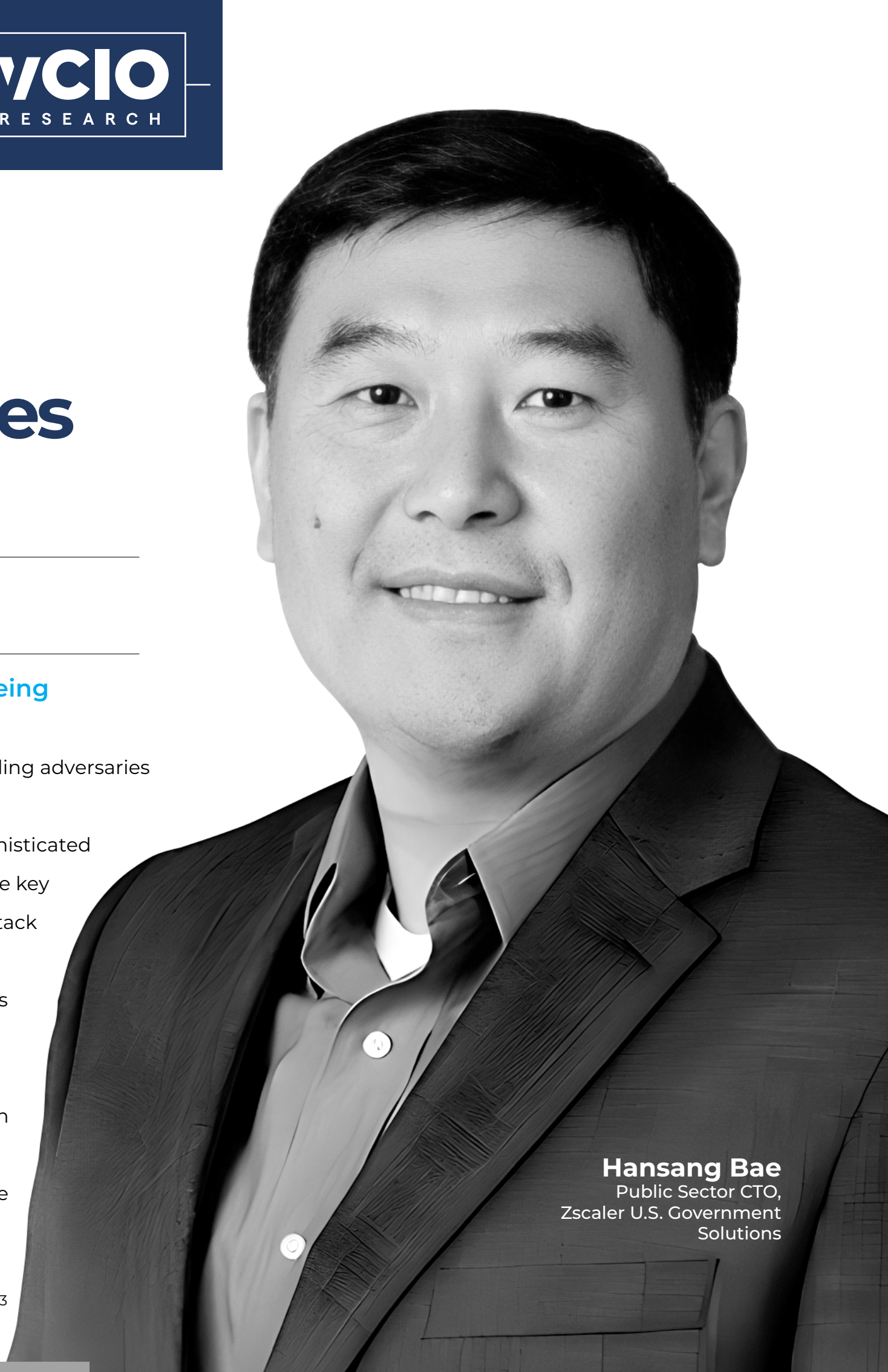
Bae AI's growing accessibility is democratizing cyber and phishing attacks, enabling adversaries to strike faster and easier than ever before.

Even though federal agencies and their industry partners have firewalls and sophisticated perimeter defenses, they remain vulnerable to the evolving threat landscape. Also, the key tenet of zero trust is to not depend solely on perimeter defenses. We're seeing the attack vector change as well.


The first line of contact for any organization is their help desk; however, as threats evolve, bad actors are leveraging new tools like sophisticated AI bots to attack when we're least expecting it – and it's working.

The enemies are no longer at the gate. They're inside your defenses, and research shows that they have probably been there for 270 days before they are discovered.

With adversaries that are this agile, we must change our thinking and reduce the bureaucratic processes that limit our ability to respond quickly and effectively. (ctd.)



Hansang Bae
Public Sector CTO,
Zscaler U.S. Government
Solutions

 **What are some of the successes or use cases for technology that you have seen?**

Bae Cyber strategies and tools must be network independent, location independent and device independent if they're going to be successful. The protection must follow the user wherever they may be.

We're now seeing cyber tools that are both resilient and adaptable. Since our adversaries are extremely agile and can implement new types of attacks quickly, we should analyze past indicators of what the user clicked on, where they went and what time they logged in to identify anomalies. We can bring that data into our neural network and say, "wait a minute, your actions are different than before, so I'm now going to dial your protection up higher." This has always been the goal, but the maturity and availability analytics engine is

finally bringing it to fruition.

At Zscaler, we're now seeing 500 trillion signals a day. 500 trillion. We use those signals to train our AI to adapt quickly to real-world attacks that we've never seen before.

Successful cyber tools require three things: resiliency, adaptability and effectiveness.

 **What are you looking forward to over the next year?**

Bae Hardware is evolving to meet the demands of neural networking and AI training.

Nvidia is taking the lead with its Blackwell architecture, offering advancements not only in performance metrics but also in reducing thermal

“With adversaries that are this agile, we must change our thinking and reduce the bureaucratic processes that limit our ability to respond quickly and effectively.”

— Hansang Bae, Public Sector CTO, Zscaler U.S. Government Solutions



and energy consumption. This is particularly significant as datacenter environmental constraints are becoming a critical challenge.

That said, I'm most excited for probabilistic computing as opposed to the binary computing we're used to.

The best way I can explain it is the difference between AI and generative AI. If I show AI an apple, it says, "okay, that's an apple," but if I take a bite out of it, the AI will say, "that's not an apple," because it's never seen an apple with a bite taken out of it.

Generative AI takes the data you have to propose an answer. You generate something new that didn't exist before from all the training data that you have.

Probabilistic computing thrives in situations where uncertainty is the norm, not the exception.

Today, to train AI, we create what's called a gradient descent. It's an example of an optimization algorithm that says, "okay, I know the answer. I'm going to peek at the answer and go, oh, I was wrong. Let me try again. I see something. I'm going to guess again. I look at the answer and say, I got it right. I now have an optimized solution for that problem." It now tells every other core, "I found the best way of identifying and solving this problem."

When the hardware can keep up, probabilistic computing comes front and center and will make our cybersecurity efforts flexible and adaptable. 🌟



Secure. Simplify. Transform.

Protect your agency with the most accredited security cloud in the world. FedRAMP Moderate and High, DoD IL5 and StateRAMP authorized.

- Protect data from cyberthreats
- Reduce IT cost and complexity
- Improve user experience
- Meet mandates with confidence

Learn more at
zscaler.com/federal



AI and Data Sharing Drive Health Innovation in 2024

Strides in AI and data sharing drive transparency and patient outcomes.

BY NIKKI HENDERSON

The Department of Health and Human Services (HHS) has made significant strides in integrating artificial intelligence and advancing the Trusted Exchange Framework and Common Agreement (TEFCA) over the past year, Assistant Secretary for Technology Policy and National Coordinator for Health IT and Acting Chief AI Officer Micky Tripathi told GovCIO Media & Research.

Tripathi reflected on these accomplishments, noting the transformative potential of AI in enhancing internal processes and improving healthcare outcomes. TEFCA has made substantial progress in achieving nationwide network interoperability, connecting hospitals, clinicians and public health jurisdictions across the country.

Tripathi outlined HHS's data and technology priorities for 2025, focusing on the continued expansion of digital infrastructure, interoperability and AI transparency, all aimed at improving patient care and health care system efficiency.

How did HHS' realignment this year shift your tech strategies?

Tripathi HHS underwent a reorganization to focus on two key areas: consolidating cybersecurity efforts and enhancing technology policy. The cybersecurity responsibilities were spread across various parts of the agency, and the reorganization aims to centralize these activities to improve accountability, leadership and resource concentration.



Micky Tripathi
Assistant Secretary for Technology Policy, National Coordinator for Health IT, Acting Chief AI Officer, Department of Health and Human Services

“We are working extensively on AI to ensure transparency. It’s important that providers feel confident in using AI technologies, which we believe will greatly benefit both patients and providers.”

— Micky Tripathi, Assistant Secretary for Technology Policy, National Coordinator for Health IT, Acting Chief AI Officer, Department of Health and Human Services

As part of the restructuring, the Administration for Strategic Preparedness and Response (ASPR) became the central hub for cybersecurity resources in the health care sector. The reorganization also created the Office of the Chief Technology Officer, which will focus on innovation in technology and work closely with the Chief Information Officer’s office. Additionally, a Chief AI Officer role was established to coordinate AI activities both internally and in the department’s broader mission. The creation of the chief data officer role further supports a forward-looking strategy for data use across HHS. By consolidating these functions, the department aims to foster better collaboration among closely related areas.

How is HHS prioritizing AI moving into 2025?

Tripathi Like many large organizations, AI is beginning to take root in various parts of HHS. Last year, HHS published an AI use case inventory as part of President Biden’s executive order, which identified 163 different AI applications. The department is now working on the next round of use cases, set to be published in December. Spoiler alert — they’re going to be a lot more than we had last year.

The agency is already using AI in a wide variety of ways. For example, it helps analyze comments on regulations, reviews policies more quickly and processes grant applications. The Centers for Disease Control and Prevention (CDC) is using AI to improve tuberculosis screenings for immigrants. Some agencies, like the Indian Health Service, also use AI, while HHS policies primarily focus on the private sector’s use of AI technologies. New regulations, set to take effect Jan. 1, 2025, will require transparency regarding AI technologies in electronic health record (EHR) products, which the department believes will greatly assist providers as AI becomes more integrated into patient care. (ctd.)

Can you talk a little bit about this year's updates to TEFCA?

Tripathi TEFCA is a nationwide network interoperability initiative. The 21st Century Cures Act directed the Office of the National Coordinator for Health IT (ONC) and the Administration for Strategic Preparedness and Response (ASTP) to establish a nationwide approach to network-to-network interoperability, similar to how cell phone networks connect with each other, allowing users to experience a single network regardless of their provider. The goal was to apply the same concept to private sector networks.

Network-to-network interoperability went live in December 2023, and in less than a year, millions of transactions have taken place over the TEFCA-based exchange. Seven approved networks are currently live, with three more

set to go live soon. By the end of the first quarter of 2025, 10 networks will be operational. More than 400 hospitals, over 100,000 individual clinicians, more than 5,000 ambulatory practices, 200 long-term post-acute care and behavioral health centers and over 50 public health jurisdictions are already exchanging information via TEFCA. We are excited about its collaboration with the private sector and looks forward to even more activity as these three new networks come online and existing networks expand.

How do partnerships boost interoperability?

Tripathi The CDC has been a tremendous partner, and we've been closely collaborating with them. Our teams are integrated to support their goals with the CDC Data Strategy and the Data Modernization Initiative, a significant federal investment to improve public health infrastructure across the country.

More than 50 public health jurisdictions — state, local, territorial and tribal—are now live on TEFCA, utilizing modern, secure network infrastructure for electronic case reporting. This is a major step forward for public health. During the pandemic, many public health jurisdictions lacked modern technology, leading to overwhelmed systems that either shut down or relied on outdated methods like faxing and phone calls — far from the system we expect in the U.S.

In collaboration with the CDC, we are working on nationwide data standards, known as the U.S. Core Data for Interoperability. These minimum data standards are required for EHR vendors to support, making information sharing easier and more efficient. This effort helps integrate public health with the health care delivery sector, ensuring that both clinical care and public health use the same standards. Most of the data public health relies on comes from clinical systems, like hospitals and physician offices, so aligning these standards will streamline data access and enable more effective public health actions. (ctd.)



What are your tech and data priorities in 2025?

Tripathi We're targeting three key areas. First, we will continue to build the digital foundation. The U.S. has invested heavily in EHRs, with 97% of hospitals and 80% of physician offices now using certified EHRs, a significant achievement. Over the past decade, both public and private sectors have worked hard to reach this point, but we must keep strengthening this digital infrastructure.

Our healthcare system is increasingly digital, and we must ensure that it remains strong with no long-term gaps. The Post-Acute Care and Behavioral Health sectors didn't benefit from incentive funds from Medicare and Medicaid, so we're focused on helping them adopt key technologies and data standards. These minimum standards are updated annually, and we aim to continue expanding them to make information sharing easier.

Second, we aim to simplify interoperability. By establishing standard network interoperability and APIs, we're working to make data sharing as seamless as the technologies that power our cell phones and apps. We want interoperability to be that simple. The electronic health record systems we require to use the Fast Healthcare Interoperability Resources (FHIR) APIs are also now being adopted by health insurers for claims data. Our goal is for patients to experience the same ease in healthcare that they do when tracking a pizza order — knowing where their care is at every step.

Finally, we are working extensively on AI to ensure transparency. It's important that providers feel confident in using AI technologies, which we believe will greatly benefit both patients and providers. By increasing transparency, we help ensure that providers trust the AI tools in their EHR systems and are able to use them effectively to improve patient care. 