GovCIO MEDIA & RESEARCH

DECEMBER 2025

DeepDives

FEDERAL IT TRENDS in 2025 OUTLOOK for 2026

SPONSORED BY

zscaler™

INSIDE:

From the editor's desk

Sarah Sybert, Managing Editor

A Year of Massive Change

The year saw massive change within the federal government. A new presidential administration took office in January and set a new direction for federal technology and modernization. The industry also experienced the longest government shutdown in history.

President Donald Trump's efficiency push through the Department of Government Efficiency called for streamlining operations, cutting redundancies and accelerating digital transformation across agencies. The shift triggered reforms across government.

At the Pentagon, officials introduced modernization efforts around acquisition and cybersecurity. They made progress on zero trust implementation and introduced a new automated risk management approach.

The Department of Veterans Affairs expanded AI efforts, restarted its EHR program and instituted various workforce reforms amid calls for efficiency.

Meanwhile, the Department of Health and Human Services unveiled an effort to modernize health care through digital services and launched a data modernization plan focused on open source.

Inside, you'll learn how these changes set the stage for a more agile, efficient and accountable government.

Table of Contents

Inside the Pentagon's 2025 Cyber, Tech, Acquisition Reforms

Pentagon officials signal era of continuous verification, operational velocity and unprecedented autonomy to meet urgent threats.

BY ROSS GIANFORTUNE

The Pentagon overhauled its approach to technology, acquisition and even its department name since inauguration day nearly one year ago.

The agency, which War Secretary Pete Hegseth now is calling the War Department, launched broad efforts around efficiency and faster fielding of technology while continuing modernization of cybersecurity plans around CMMC, risk management and zero trust.

The moves reflect Hegseth's push for quicker innovation and establishing his department as one that is ready to face growing threats from adversaries such as China and Russia.

"This urgent moment, of course, requires more troops, more munitions, more drones, more patriots, more submarines, more B-21 bombers," Hegseth said in an October 2025 speech to more than 800 of the nation's top military leaders in Quantico, Virginia. "It requires more innovation, more AI in everything and ahead of the curve."

Zero Trust: Never Trust, Always Verify

The principle of zero trust has moved from a theoretical concept to an actionable imperative across the DOW and the federal government, according to DOW officials. With a federal mandate to apply zero-trust architectures in place by fiscal 2027, the DOW made strides throughout services and national security entities in implementing zero trust.

"We've been able to show how you do [zero-trust implementation] … So now it's, how do we build on that?" Department of the Navy Deputy CIO Barry

Photo credit: Air Force photo by Airman 1st Class David S. Calcote

Tanner said in February 2025 at AFCEA West in San Diego, California. “We have a mandate to meet the basic zero trust requirements by 2027. That is really fast, that’s really hard, … [but] the assessments that were done last year will help inform all of the networks and programs that have work to do on that.”

The national security ecosystem requires zero-trust architectures because of the environment’s decentralized nature, and the growing sophistication of attacks makes cybersecurity increasingly complex, former Principal Director for Cybersecurity Gurpreet Bhatia said during GovCIO Media & Research’s March 2025 Defense IT Summit in Arlington, Virginia.

“We want to minimize the adversary’s ability to move through the network and have freedom of movement and exploit [DOW] data,” Zero Trust Portfolio Management Office Director Randy Resnick said during the May 2025 AFCEA TechNet Cyber event. “That means they can’t move laterally, they can’t break out of a micro segment, they can increase privilege escalation.”

Defense Information Systems Agency’s (DISA) zero-trust Thunderdome architecture passed 152 zero-trust exercises during testing in April 2025. Thunderdome, developed from an initial concept to a working reality with industry partners, comes two years ahead of the Pentagon’s 2027 deadline for zero-trust implementation.

“We went from a concept on a whiteboard, quite literally, to articulating that concept, that vision, to this kind of a forum right to then partnering with a number of industry partners in the room here,” DISA Deputy Director Christopher Barnhurst said at TechNet. “Dozens of products that are integrated into that design, and that is now real, and it’s real two years ahead of when the [DOW] CIO said it has to be real for the department.”

CMMC 2.0: The Rule of Law for the Defense Industrial Base

Six years in the making, the Pentagon published the final CMMC rule, establishing CMMC 2.0 into federal law and cementing its plans to enforce new

Photo credit: ImageFlow/Shutterstock

cybersecurity requirements across the defense supply chain.

DOW began enforcing the framework on Nov. 10, 2025, marking the start of a three-year rollout aimed at strengthening cybersecurity across the defense supply chain. The rule officially mandates that all DOW solicitations and contracts include CMMC 2.0 requirements for contractors and subcontractors that process, store or transmit Federal Contract Information or Controlled Unclassified Information.

Pentagon CISO Katie Arrington, one of the original architects of CMMC, framed the shift as a necessary cultural transformation for the entire defense community, telling GovCIO Media & Research in May 2025 that the "department is committed" to CMMC.

"It's a complete cultural shift. I want you to adapt the culture of zero trust. I want you to adapt the culture of cybersecurity," she said at the UiPath Public Sector Summit in April.

From Paperwork to Continuous, Automated Risk Management

DOW's implementation of a sweeping Cybersecurity Risk Management Construct (CSRMC) in September 2025 is designed to replace the outdated, checklist-driven Risk Management Framework (RMF) with a system capable of delivering real-time cyber defense. Arrington told GovCIO Media & Research in May 2025 that risk management should be "a living, breathing culture."

"Is it worth having 18 people sign off [on a project] and saying that I've tested it and it's good — Are we? Is the return on investment valuable in that?" Arrington said. "I say no. I say my money is much better spent in using tools and capabilities to ensure that the life cycle is appropriate and that the culture is appropriate, and that we're continuously monitoring, continuously updating or continuously remediating."

The CSRMC fundamentally changes the department's approach away from

“It’s a complete cultural shift. I want you to adapt the culture of zero trust. I want you to adapt the culture of cybersecurity.”

— Katie Arrington, performing the duties of CIO, DOW

“snapshot-in-time” assessments that failed to keep pace with modern threats. The new construct is built on a five-phase lifecycle that embeds security at the outset and mandates continuous, automated life cycle monitoring.

“This construct represents a cultural shift in how the department approaches cybersecurity,” said Arrington. “With automation, continuous monitoring and resilience at its core, the CSRMC empowers the DOW to defend against today’s adversaries while preparing for tomorrow’s challenges.”

Overhauling Software Acquisition

The Pentagon also established the Software Fast Track (SWFT) in May 2025 to streamline certification processes and bring commercial and mission-ready software into production faster. George Lamb, director of information networks capabilities at DOW, explained that SWFT is designed to integrate commercial off-the-shelf (COTS) software into the DevSecOps pipeline.

“Commercial technology is just software. How do we get that commercial

software into our pipeline? SWFT is a process for going to look at the authorization process," Lamb said at the 2025 Carahsoft DevSecOps Conference in Reston, Virginia.

He added that the program builds on lessons from Platform One's Iron Bank repository, which scans and evaluates software containers for risk rather than relying on a simple pass/fail model.

"We put insecure software in production all the time … Iron Bank scans it. We don't stop it. We just put caveats around it," Lamb said.

Arrington underscored SWFT's role in enabling the department's software acquisition pathway.

"The SWFT is to make more software available for the secretary's software acquisition pathway, and blowing up the RMF will make the use of the SWFT and the software acquisition pathway more adaptable, so that we can be more lethal, more efficient and provide readiness to the warfighter," Arrington told GovCIO Media & Research.

Budgetary pressures are also driving SWFT's adoption. "We're kind of in a heavy rationalization phase right now and exploring all of the ideas that we can to do things better and faster," David McKeown, DOW's special assistant for the Cybersecurity Innovation Office, at the Potomac Officers Club Cyber Summit in May 2025.

(ctd.)

Photo credit: DC Studio/Shutterstock

Pentagon Unveils Overhaul of Tech Acquisition to Speed Delivery

Hegseth announced sweeping reforms to accelerate how the department buys and fields technology in November 2025, replacing decades-old processes with what leaders call a “wartime footing” for acquisition.

“The Defense Acquisition System, as you know it, is dead. It’s now the warfighting acquisitions system,” said Hegseth.

The reforms include canceling the Joint Capabilities Integration Development System (JCIDS), a requirements process criticized for taking nearly a year to approve a single document.

“JCIDS was focused on paperwork, not mission. It became a years-long bureaucratic anchor,” Hegeth said.

In its place, new forums will tie funding directly to top warfighting priorities and encourage experimentation and rapid prototyping.

Industry partners will be asked to deliver “85% solutions” quickly, with the Pentagon iterating improvements over time.

“An 85% solution in the hands of our armed forces today is infinitely better than an unachievable 100% solution endlessly undergoing testing,” Hegseth said.

The overhaul aims to stabilize demand signals, expand competition and rebuild the defense industrial base into what leaders described as a “new arsenal of freedom” capable of surging production at speed.

“[DOW] will only do business with industry partners that share our priority of speed and volume above all else and who are willing to surge American manufacturing at the speed of ingenuity to deliver rapidly and reliably for our warfighters,” Hegseth said.

Photo credit: Pfc. Jose Nunez, U.S. Army

The Year of Tech, Talent Reinvention at VA

The agency set the stage to modernize its electronic health record, implement emerging technology like artificial intelligence and streamline its workforce.

BY JORDAN MCDONALD

The first year of President Trump's second administration brought dramatic changes to the Department of Veterans Affairs as it navigated AI enhancements, workforce reductions and set the stage for an expansion of federal health record modernization deployments.

Preparing for EHR Deployment

The agency continued its work on modernizing the federal health record, with plans to deploy at select sites in 2026.

Dr. Neil Evans, acting program executive director for the Department of Veterans Affairs Electronic Health Record Modernization Integration Office, said at GovCIO Media & Research's Health IT Summit in September 2025 his office is deploying the EHR in waves throughout 2026, with a goal of full deployment in 2031.

"When we go live in a local market, and there's a period of time where a medical center that collaborates very closely with its neighboring medical center are on two different electronic health records, it introduces all kinds of complexity with regard to training … with regard to technical interfaces … during this period of transition. And so, there's a real opportunity, we realize, to say, 'Let's start to think more in a market-based fashion,'" Evans said.

Photo credit: Invision Events

Navigating Workforce Reforms

Reductions in force across the government also affected the VA, but leaders within the department said that emerging technology would aid in shoring up any lost personnel.

The agency lost nearly 17,000 employees between January and June 2025, with the agency expecting an additional 12,000 to have departed since Sept. 30, 2025.

Acting CIO Eddie Pool, who was acting CIO at the time, told GovCIO Media & Research in August 2025 the agency streamlined its workforce and prioritized "cyber dominance," to safeguard data and bolster veteran trust.

"It's process efficiency. We're streamlining a lot of our operations and leveraging automation in a whole new way. In doing so we're maximizing our efficiency and productivity with a much leaner and more capable workforce," Pool said at the time.

Overcoming a Historic Government Shutdown

The federal government faced the longest shutdown in history in fall 2025, but VA was mostly functional throughout the closure. The VA Human Capital Contingency Plan estimated that 97% of employees continued to work despite the shutdown.

VA Secretary Doug Collins told reporters in October 2025 that the shutdown had limited impact on veterans' health care services, but strained other parts of the agency's operations and workforce, such as the Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA), even though disability payments and burials continued.

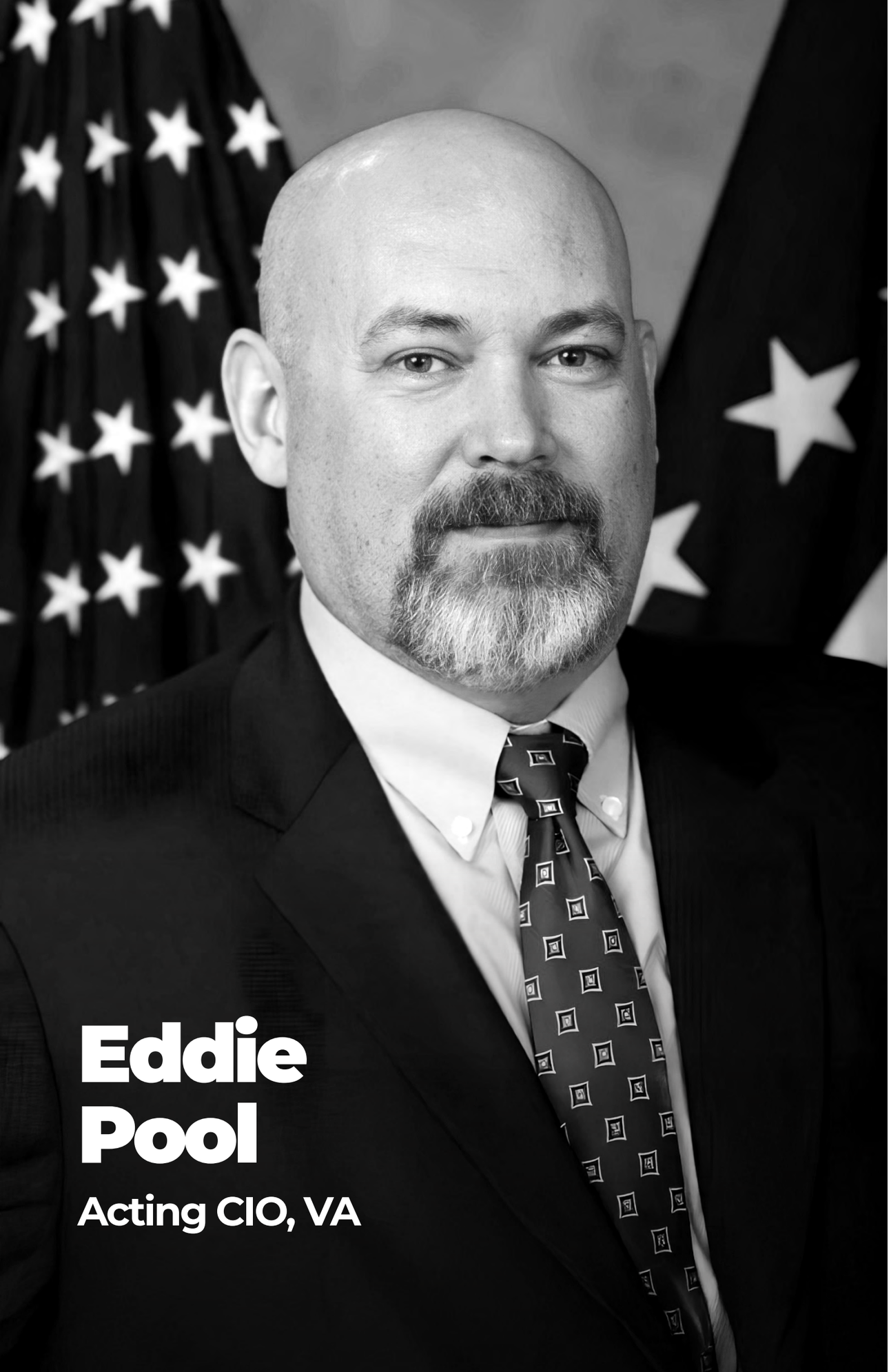
Advancing Artificial Intelligence

The agency also adopted significant AI use cases across the enterprise, with a goal of delivering "speed, quality, efficiency and accuracy," while "fundamentally transforming the delivery of health care and benefits for veterans," according to its updated AI strategy from October 2025.

The strategy focuses on five key areas of innovation and the adoption of "high-impact" use cases, which falls in line with Trump administration directives

"It's process efficiency. We're streamlining a lot of our operations and leveraging automation in a whole new way."

— Eddie Pool, Acting CIO, VA



to define, implement and then adopt minimum risk standards across government agencies.

"VA is taking a dual-track approach by enabling early AI experimentation while allowing those lessons to inform future standards," the strategy states. "As AI tools are validated and show worth, they will be incorporated into the EHR and many other information technology platforms through coordination between innovators and the teams managing those systems today."

Kimberly McManus, deputy chief AI officer and deputy CTO, said in a LinkedIn post, "[VA's] goal is to lead in effective, reliable and safe AI, delivering measurable improvements in speed, quality and efficiency for veterans."

One of the major use cases centers around ambient dictation, which takes notes of clinician-patient interactions and synthesizes them, saving clinicians hours of work they would otherwise spend reviewing and writing notes.

The VA announced in September 2025 it would launch the first pilots of its ambient listening program at 10 facilities nationwide by the end of the year.

Dr. Evan Carey, acting director of the National Artificial Intelligence Institute, told congressional leaders in September 2025 that the team would track criteria and evaluations focused on "user acceptance testing, veterans' perceptions of the tool as it's used in their ongoing trust in the care they receive, and just overall performance of the tool."

"We are measuring clinician burden and getting clinician feedback, both synchronously and through survey mechanisms to understand the impacts," Carey told leaders in September 2025.

PARTNER INTERVIEW

zscaler™

GovCIO MEDIA & RESEARCH

Effective AI Implementation Hinges on a Unified Strategy

Advances in policy, data and security drive government's AI implementation strategy.

Chad Tetreault
Public Sector CTO, AI Strategy and Governance, Zscaler

What is one of the biggest challenges in implementing AI?

Tetreault This year, the federal government has focused on building a strong foundation for artificial intelligence implementation. I see four key pillars that need attention.

First, there was initially policy guidance on generative AI, and policy drives everything government does.

The second pillar is cyber, as existing cyber tools must be continually updated to counter new AI-driven threats.

The third is data, with agencies putting major effort into improving data quality.

The fourth pillar is technology, and agencies are actively evaluating and adopting new tools to better leverage AI in mission and operational processes.

(ctd.)

What are some of the successes or use cases for technology you've seen helping?

Tetreault Policy guidance such as OMB Memoranda M-25-21 and M-25-20 have pushed agencies to take meaningful steps forward. These directives encouraged agencies to begin building their AI plans. For example, the State Department not only responded to the orders but also developed a new enterprise data and AI strategy to align with them. OMB under M-25-21 has also asked agencies to appoint chief AI officers and establish AI councils. Knowledge sharing is critical but difficult because each agency is focused on its own mission. Still, creating collaborative spaces can enable significant cross-agency learning.

Partnerships between government, academia, the scientific community and developers are also essential. While NIST is working hard to keep pace with rapid technological change and emerging risks, organizations such as MIT's AI Risk Initiative are publishing new insights almost daily.

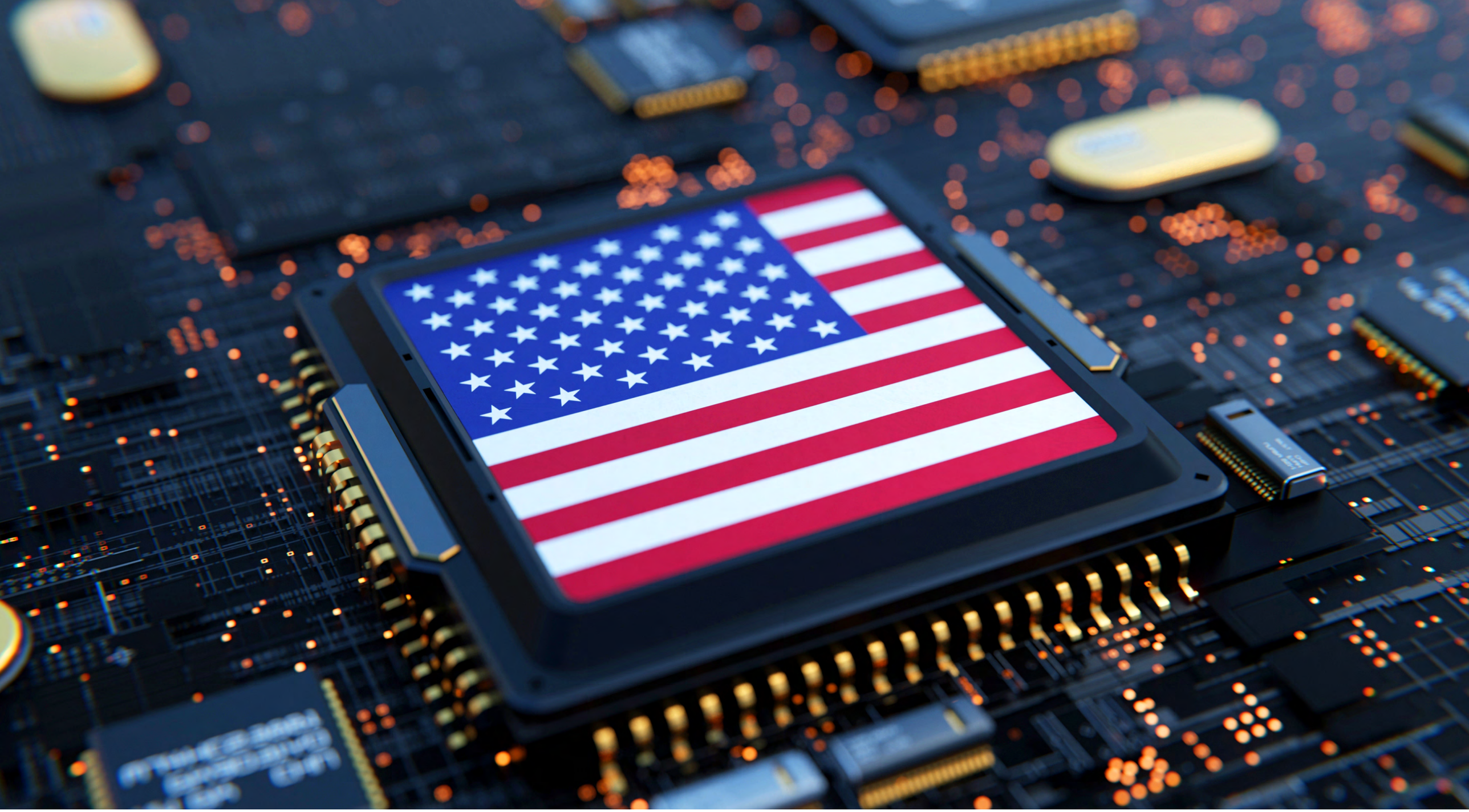
What do you look forward to over the next year?

Tetreault One of the biggest challenges in implementing AI for security is helping agency lawyers, policy teams and privacy officials understand how the technology works. AI systems must be explainable, with clear visibility into their actions. Thanks to recent advances, separate interfaces or chatbots can now break down an AI model's decision-making process, showing what it did, how it reached a conclusion and whether the underlying data was accurate.

Dynamic defense is another promising development. In recent years, the Defense Advanced Research Projects Agency introduced the concept of using

"AI brings a different approach to finding vulnerabilities and can operate around the clock."

— Chad Tetreault, Public Sector CTO, AI Strategy and Governance, Zscaler



AI to identify system vulnerabilities. Previously, agencies had to use red teams, which follow time-consuming and expensive processes. Active defense shifts AI red-teaming much earlier in the process. AI brings a different approach to finding vulnerabilities and can operate around the clock.

I'm hopeful that in the coming year we'll advance the question of how to approach AI implementation at a national scale. Both the federal government and several states are already making significant progress, implementing AI to support citizen services. The U.S. is in a race for technology dominance in AI development. Launching the Genesis Mission will serve "as the coordinated national effort to unleash a new age of AI accelerated innovation and discovery that can solve the most challenging problems of this century," according to the executive order.

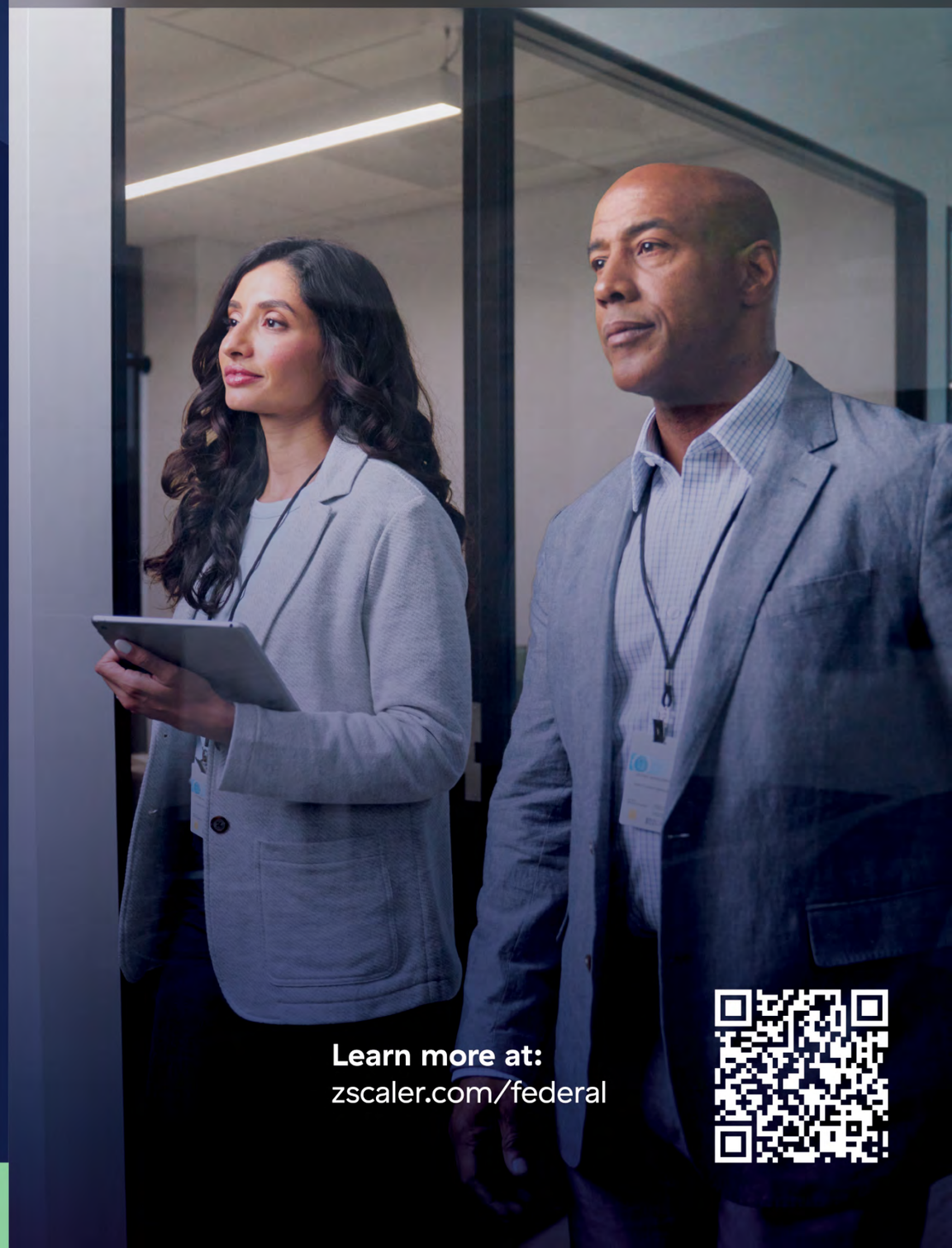
Photo Credit: Mahir Asadli/Shutterstock

zscaler™ | U.S. Government Solutions

GovRAMP FedRAMP™ IL5 PA CYBERSECURITY MATURITY MODEL CERTIFICATION

Zero Trust + AI for Government

- **Protect** users, branches, clouds and data
- **Reduce** IT cost and complexity
- **Improve** user experience and fortify the digital workforce
- **Securely** embrace public and private GenAI



Learn more at:
zscaler.com/federal

Q&A: HHS CDO Builds Trust Through Data Transparency

Kristen Honey breaks down the milestones, cultural shifts and lessons learned after HHS launched its Living Open Data Plan.

BY SILVIA OAKLAND

The Department of Health and Human Services in a push toward transparency released its Living Open Data Plan in July 2025 to guide improvements in data governance, public accessibility and agency-wide decision-making.

GovCIO Media & Research spoke with HHS Chief Data Officer Kristen Honey earlier this year about how the department is advancing an "open by default" mindset when it comes to data management.

How will you ensure the Living Open Data Plan remains dynamic rather than static?

Honey: Technology moves fast, so we wanted a format that could evolve with it. Rather than publishing a static PDF that sits on a website, we broke every chapter and appendix into modular GitHub components. The public can comment on them in real time, offer suggestions and signal where they see gaps or opportunities.

That public input becomes a demand signal to guide updates. We hope to refresh the plan at least a couple of times a year — and right now we're moving even faster. When we launched the plan in July, the deputy secretary committed to releasing an updated version within four months. Working openly, taking real-time feedback and iterating quickly are core to the model.

What did your process for developing the modular design entail?

Honey: During COVID, we saw how effective "living evidence guidelines" were, especially in places like Australia. Instead of waiting years for updates, experts revised clinical guidelines monthly as new science emerged. That modular, iterative model worked incredibly well during a fast-moving emergency.

HHS has a strong open data community. HealthData.gov sees nearly a

Photo Credit: Invision Events

million visits a month, with many longtime super users. We realized we could replicate that model here by tapping into the expertise of users inside and outside government. Open data fuels research, business models, student projects — it sparks innovation. So why not build a model that continuously incorporates that insight?

How does HHS want public and private partners to engage differently under this plan?

Honey: We're exploring ways to make open data engagement radically transparent. In the past, interagency open data groups sometimes held meetings that were open for the public to observe, not participate, but to see who the leaders were and how decisions were made. We want to bring more of that spirit back.

Partnerships exist on a spectrum. On one end, there are lightweight collaborations — like the Census Bureau's Opportunity Project tech sprints — where government provides data and stewardship, but the collaboration is informal. On the other end, there are formal public-private partnerships, like HHS' KidneyX Innovation Accelerator. We expect to pursue more of both.

Marrying government's authoritative role with the speed and experimentation of industry allows us to move faster. Industry users are often the ones pushing standards and applying data at the cutting edge. When we work together, we get the best of both worlds.

What are your plans to bolster user experience for HealthData.gov?

Honey: We're a very small team — fewer than six people — so we rely heavily on human-centered design and AI-enabled routing to make the user experience seamless.

The public shouldn't need to know which HHS division owns which dataset.

Photo Credit:
SeventyFour/Shutterstock

We want HealthData.gov to be a one-stop shop. When users reach out, we act like a concierge service: we help them find what they need, and on the backend, AI helps route inquiries to the right experts across the department.

The better the tech gets, the more high-touch we want to be. Automation should free us to respond faster and more personally.

How does “open by default” shift the culture at HHS?

Honey: At its core, “open by default” is a power shift. Traditional government structures rely on top-down, hierarchical information flows where offices act as gatekeepers. Open data flips that — information moves bi-directionally, silos break down and decision-making power moves closer to the front lines.

Other agencies have gone through similar transitions. The Pentagon, for example, had to radically rethink information flows during the shift away from 20th-century approaches to warfare. HHS is at a similar inflection point. By embracing transparency, we enable complex-systems thinking and more holistic understanding of health impacts across society.

Success in my role means empowering experts across the department — not centralizing power at headquarters.

CMS’ open-source work is a notable example of interagency collaboration. How does HHS plan to scale similar efforts?

Honey: CMS’ Open Source Program Office (OSPO) is a great model. Their team built tools to implement the SHARE IT Act within CMS, but they also designed them from day one to benefit all of HHS and even other federal agencies.

My office partners closely with OSPO. We’ve piloted using their open-source tools for open data, and early results are promising. Different divisions have different needs and mission spaces. Our role is to listen, provide optionality and act as the connective tissue that brings together metadata, standards and shared solutions. (ctd.)

Radical transparency has strong top-cover support across HHS, which helps every division move forward with confidence.

What do the first metadata standards establish, and how will they evolve?

Honey: Metadata standards will be a long-term effort, and they must involve not just federal leaders but also industry, academia and expert data users. We want a governance model that brings in these external voices without relying on federal advisory committees — something more agile and collaborative. Other agencies have done versions of this before, so we know it's possible.

For November, we'll focus on the modules where public feedback is highest. We also expect to release version 2.0 of both the Living Open Data Plan and the HHS Data Inventory, which catalogs public and nonpublic assets across the department.

Once those are out, we hope to set a regular cadence — likely at least twice a year — for updating the living plan. Governance, iterations and expanding the metadata catalog will be major priorities moving into 2026.

"Open data fuels research, business models, student projects — it sparks innovation."

— Kristen Honey, CDO, HHS