

Federal IT

Trends **in** 2023 Outlook **for** 2024



INSIDE:

DOD zero trust.....	3
Data-sharing strategies	8
VA EHR reset.....	15
The promise of AI	19

SPONSORED BY



From the editor's desk



Amy Kluber, Editor-in-Chief

Setting the Stage

For starters, the end of the public health emergency closed the chapter of the COVID-19 pandemic and opened a new one for agencies to begin enacting on lessons learned. One of those being the CDC's two-year plan to overhaul how the nation responds to public health emergencies — because, yes, there will be another one. A key part of that is through leveraging data to inform this level of decision-making.

The industry also saw a long-anticipated executive order directing agencies to develop artificial intelligence responsibly. Leaders have called for a better national approach to AI development especially amid concerns that it can be biased and hurt more than it can help. But

agencies see AI's promise. Inside, we dive into how the ways government is using it for health care and also to alleviate burdens on the workforce.

There are also coordinated efforts to address a quickly changing threat landscape that still places zero trust at the forefront of these cybersecurity discussions. More on that inside as well.

In my five years covering this industry, a new year always looks better and better for the tech that will solve some of the biggest national challenges. In the words of Federal CIO Clare Martorana, "We can do it, and technology is what is getting us there." ✨

Table of Contents



Anastasia Obis
Staff Writer/
Researcher



Jayla Whitfield
Staff Writer/
Researcher



Jordan McDonald
Staff Writer/
Researcher



Nikki Henderson
Staff Writer/
Researcher



ARTICLE

Tech Developments at DOD to Watch in 2024

Zero trust, AI and hybrid cloud were on the minds of defense tech leaders this year.

BY ANASTASIA OBIS



ARTICLE

Data Sharing and AI Top Federal Health Agency Priorities in 2024

Government is on a mission to address health disparities and close gaps through technology.

BY JAYLA WHITFIELD



PARTNER INTERVIEW

The Outlook for Zero Trust

Developments in the threat landscape are leading to renewed focus in cybersecurity strategies.

Danny Connelly, Chief Information Security Officer, Zscaler



ARTICLE

VA Prepares for EHR, AI Priorities in 2024

The agency saw some largescale digital developments this year around EHR modernization and increased health care demands.

BY JORDAN MCDONALD



ARTICLE

The Outlook for Federal AI Development in 2024

Agencies will see more benefits as well as challenges with the adoption of AI into 2024 and beyond.

BY NIKKI HENDERSON

Tech Developments at DOD to Watch in 2024

Zero trust, AI and hybrid cloud were on the minds of defense tech leaders this year.

BY ANASTASIA OBIS

The Defense Department's technology portfolio is among the largest in the world. Zero trust, artificial intelligence and hybrid cloud dominated tech conversations and will support ongoing priorities as the agency embarks on a new year. These efforts are part of broader technology initiatives to connect the military services and operate jointly across domains — all of which underpin the newly renamed Combined Joint All-Domain Command Control (CJADC2) concept.



“We came out with our zero-trust strategy, which was a really big deal ... it was the first time the DOD expressed what they wanted in zero trust and described the level we needed to achieve. And one year after the strategy, it was a requirement to actually submit an implementation plan,” Randy Resnick, director of the office, told GovCIO Media & Research at AFCEA TechNet Indo-Pacific in November. “This is a really big change for everybody, ... but what I saw when I reviewed it, I was very pleased with the content. ... It’s a

big move from the cyber perspective.”

A rapid shift to artificial intelligence and cloud-based technologies, remote work and technical debt are only some of the factors contributing to an increased security threat environment for DOD. To address the constantly evolving cybersecurity challenges, military service branches have until fiscal year 2027 to achieve target level zero-trust readiness.

Since military services and components are delivering their implementation plans with different solutions to meet their specific mission

Services Weigh Zero Trust Implementation

One year after the release of the Defense Department's five-year zero-trust strategy and execution roadmap in 2022, service branches began submitting their zero-trust implementation plans for review.

The Zero Trust Portfolio Management Office has just received more than 40 implementation plans from military services and defense agencies. The office is expected to finish evaluating those submissions in before the end of 2023.

needs, Resnick's challenge is to ensure that everyone is synchronized throughout the process.

"We wanted the components to choose how to get the target level. But some of them are doing it in different ways, and the hard part for our portfolio offices is to keep track of all of this. So it's about actual procurement in the actual implementation," Resnick said.

By the end of fiscal year 2024, Resnick's office expects services and components to start buying solutions.

"Once we approve, we are expecting them to make procurements happen. And that's when they're going to start engaging heavily with the vendors. Contracts are going to be established. ... That's when really the hardware, software hits the ground, and applications, users and data start moving," Resnick said.

The Pentagon is also required to brief Congress in January 2024 on how the department plans to achieve zero trust target level readiness by 2027.

During this transition, the Defense Information Systems Agency (DISA) is helping military services to move away from the legacy castle-and-moat cybersecurity approach through its Thunderdome initiative.

DISA's Thunderdome program led to a \$1.86 billion contract with Booz Allen Hamilton to move from prototype to production. Some service branches and components will partner with DISA in the coming year to evaluate whether Thunderdome is a viable option for them to protect networks.

Artificial Intelligence Dominates

To advance modernization efforts with AI adoption, the Pentagon established the Chief Digital and Artificial Intelligence Office (CDAO) in 2022. In November, the office released its new AI strategy focusing on agile AI implementation across the enterprise.

The new strategy followed the White House's long-awaited artificial

**“[In 2024],
contracts are
going to be
established. ...
That’s when really
the hardware,
software hits the
ground and
applications,
users and data
start moving.”**

**— Randy Resnick, Director,
Zero Trust Portfolio Management
Office, Defense Department**



intelligence executive order that seeks to reduce and manage national security risks posed by the technology.

The strategy is meant to provide a foundation and unified approach for data, analytics and AI adoption across all military services, assembling an educated workforce to incorporate commercial tools and advancing research of the nascent technology.

“Our integration of data, analytics and AI technologies is nested within broader U.S. government policy, the network of private sector and academic partners that promote innovation, and a global ecosystem. We need a systematic, agile approach to data, analytics and AI adoption that is repeatable by all DOD Components,” according to the strategy.

For fiscal year 2024, the Pentagon requested \$1.8 billion for artificial intelligence, a \$600 million increase from \$1.2 billion the department requested for the previous year.

As the Pentagon is scaling up its use of artificial intelligence, the need for the department to do so responsibly and ethically is critical.

In November, the CDAO released the Responsible Artificial Intelligence

(RAI) Toolkit, a key deliverable of its Responsible AI Strategy and Implementation Pathways released in 2022. The toolkit is meant to provide a centralized process for identifying and enhancing the alignment of the department’s AI projects and the AI ethical principles.

“We reach for the opportunity that AI provides us with what we need to reach with the other hand and manage the risks that will come with the application of that disruptive technology,” Coast Guard Vice Adm. Kevin Lunday said at the 2023 Sea-Air-Space conference at National Harbor, Maryland, earlier this year.

With the release of the artificial intelligence executive order, the White House wants DOD to address gaps in AI talent, assess ways AI can increase biosecurity risks and complete an operational pilot project to deploy AI capabilities, including large language models.

“If the White House and executive branch achieve even half of the provisions, it will be a vital step forward to safeguard AI,” Heather Frase, senior fellow of AI assessment at Georgetown University’s Center for Security and Emerging Technology, told GovCIO Media and Research.



Randy Resnick

Director, Zero Trust
Portfolio Management
Office, Defense
Department

Hybrid Cloud and Edge Computing Advance

Pentagon CIO John Sherman's August memo mandated the services to use the Joint Warfighting Cloud Capability (JWCC) contract to purchase cloud capabilities and services across all classification levels moving forward.

DOD's \$9 billion multi-vendor cloud contract marks a new era for the DOD cloud efforts. It was launched after its failed predecessor, JEDI, was awarded to Amazon, Google, Microsoft and Oracle in December 2022.

While the JWCC is not the "end all be all" of the DOD cloud, this work is critical to provide cloud capabilities at the secret and top-secret classification levels, as well as extending the cloud to the edge environments to provide a more resilient infrastructure outside the contiguous United States.

"How do we extend what today is primarily a CONUS-based cloud infrastructure with a few edge nodes that the military departments have been bringing out themselves, and how do we move the enterprise out to the edge out to the battle space to provide a more resilient infrastructure, more responsive infrastructure, and give us data processing and AI capabilities directly within theater? That's that a big step that we're working on," Rob Vietmeyer, DOD's chief software officer, told GovCIO Media and Research.

DISA, the agency leading the procurement effort, announced in October that DOD awarded 13 different cloud task orders that are worth over \$200 million under the JWCC contract. Some of the task orders service the department's CJADC2 initiative. More than a dozen orders are also in the works.

The program plan is a three-year base contract with two one-year options, which means that the work will possibly be conducted through 2028. At the end of the five-year procurement period, the Pentagon will launch "a full and open competition for a future multi-cloud acquisition."

5G Connectivity

The Pentagon recently said it will shift 5G-related efforts from the Undersecretary of Defense (USD) for Research and Engineering's FutureG and 5G Office to the CIO. The shift marks a key time when there is a growing need for the expansion of 5G pilot programs that will advance implementation for the wireless capability.

The FutureG & 5G Office focused its efforts on three areas to advance the Pentagon's modernization efforts:

- The "accelerate" portion of the initiative focuses on advancing the Defense Department's adoption of 5G.
- The "operate through" part concentrates on ensuring the secure use of 5G.
- The "innovate" area of the initiative works on investing in NextG technologies.

Since 2020, the Pentagon invested \$600 million in 5G development at nine military test sites around the continental U.S. Two of the test sites, Naval Base San Diego in California and Marine Corps Logistics Base Albany in Georgia, have been working on 5G-enabled smart warehouses.

Sherman said his office wants to expand the existing programs, possibly add more 5G installations, including an open radio access network (O-RAN).

"The technology has really matured to a point where it's ... almost imperative for DOD to work with this and to understand how we can interact with what we call the 'global information infrastructure.' This is the worldwide connectivity of everything. How do we not participate and how do we not utilize what's been produced out there in the commercial world?" Dr. Tom Rondeau, principal director for FutureG & 5G at the Pentagon's Office of the Undersecretary of Defense for Research and Engineering, told GovCIO Media and Research. 🌟



Data Sharing and AI Top Federal Health Agency Priorities in 2024

Government is on a mission to address health disparities and close gaps through technology.

BY JAYLA WHITFIELD

The public health sector faced a challenging but optimistic reality this year as it grappled with the end of the pandemic-induced public health emergency and set in motion many technological advancements that will continue to shape the conversation in 2024.

Some of the biggest developments included a reorganization at the Centers for Disease Control and Prevention in how it is modernizing data reporting to prepare for the next pandemic. Other health agencies are leveraging artificial intelligence and new approaches to cybersecurity in the face of a changing health care landscape.

Data Sharing and Coordination

CDC’s two-year data initiative, CDC Moving Forward, aims to improve capturing and distributing data throughout the public health ecosystem.

“There’s such a great opportunity in public health — a need to advance the way that we exchange data,” said Dr. Jennifer Layden, director of the new Office of Public Health Data, Surveillance, and Technology (OPHDST), at the Health IT Summit in September.

The initiative has made significant advancement in automated electronic



case reporting, which CDC plans to integrate into disease surveillance systems for more than 30 jurisdictions by the end of 2023.

“We are in this transformational moment to build the better data, the better

**“There’s
such a great
opportunity in
public health —
a need to
advance the
way that we
exchange
data.”**

**— Dr. Jennifer Layden, Director,
Office of Public Health Data,
Surveillance, and Technology
(OPHDST), Centers for Disease
Control and Prevention**

analytics for that better response,” said Dylan George, director of operations for the CDC’s Center for Forecasting and Outbreak Analytics, at a panel during the HIMSS conference in April.

Other data modernization efforts include those to develop better standards and policies for interoperability.

This year the Office of the National Coordinator for Health IT (ONC) advanced two key frameworks: the Trusted Exchange Framework and Common Agreement (TEFCA) and expanded the United States Core Data for Interoperability (USCDI). Both are providing a model for the health IT community to develop common agreements and operating structures to share data especially for electronic health records.

Artificial Intelligence for Health IT

In a government-wide movement, health agencies are also amping up AI research and development. AI is showing promise for its positive impact on the workforce who can use it to offload routine, traditionally manual tasks and support clinical decision-making such as better detecting cancer.

“I’ve never seen quicker and more thoughtful uptake of an emerging technology in the government than I am seeing right now with AI,” said Sanja Basaric, former AI program lead at the Department of Health and Human Services who now serves the Defense Department’s Chief Digital and AI Office, at the September 21 Health IT Summit.

These capabilities can also support the public in an equitable way, meeting patients where they are and unlocking critical access to these services. Much of this work comes down to the data.

Biden’s October artificial intelligence executive order gave HHS a 90-day deadline to establish an AI task force. In addition, the order gives the agency 180 days to assess whether AI technologies in the health sector can sustain quality levels.



Dr. Jennifer Layden

Director, Office of Public Health Data, Surveillance, and Technology (OPHDST), Centers for Disease Control and Prevention

Addressing Cybersecurity Risks

In March, HHS released a cybersecurity implementation guide aimed at helping health care organizations prevent breaches and address cybersecurity risks during a time when fraud and data security threats increased.

“Cyber incidents pose risks to patient data, intellectual property, scientific or laboratory research, medical manufacturing, and ultimately the ability of health care organizations to safely serve their patients,” HHS Deputy Secretary Andrea Palm said in a statement in March.

The agency also has been working toward broader zero-trust goals. An HHS task force, for example, released guidance in June that includes zero-trust resources for health facilities to secure networks and protect technology.

Digital Services for Health Equity

Ensuring health equity and access to health care services is a core principle of health agencies and an area where technology can make a difference.

The Centers for Medicare and Medicaid Services’ digital services chief is on a mission to modernizing systems and services so that they better serve the public.

“It is imperative that we give people information they can find quickly and in accessible plain language. For health care, that also means that our services are easy to use for people using screen readers and with low vision, cognitive disabilities, low bandwidth and non-English speakers,” CMS Chief Digital Strategy Officer Andrea Fletcher told GovCIO Media & Research.

Other health leaders say addressing and identifying bias is one key to the issue. There’s also factors around care access especially in rural areas where capabilities like telehealth can help further close the gap. ✨



The Outlook for Zero Trust

Developments in the threat landscape are leading to renewed focus in cybersecurity strategies.

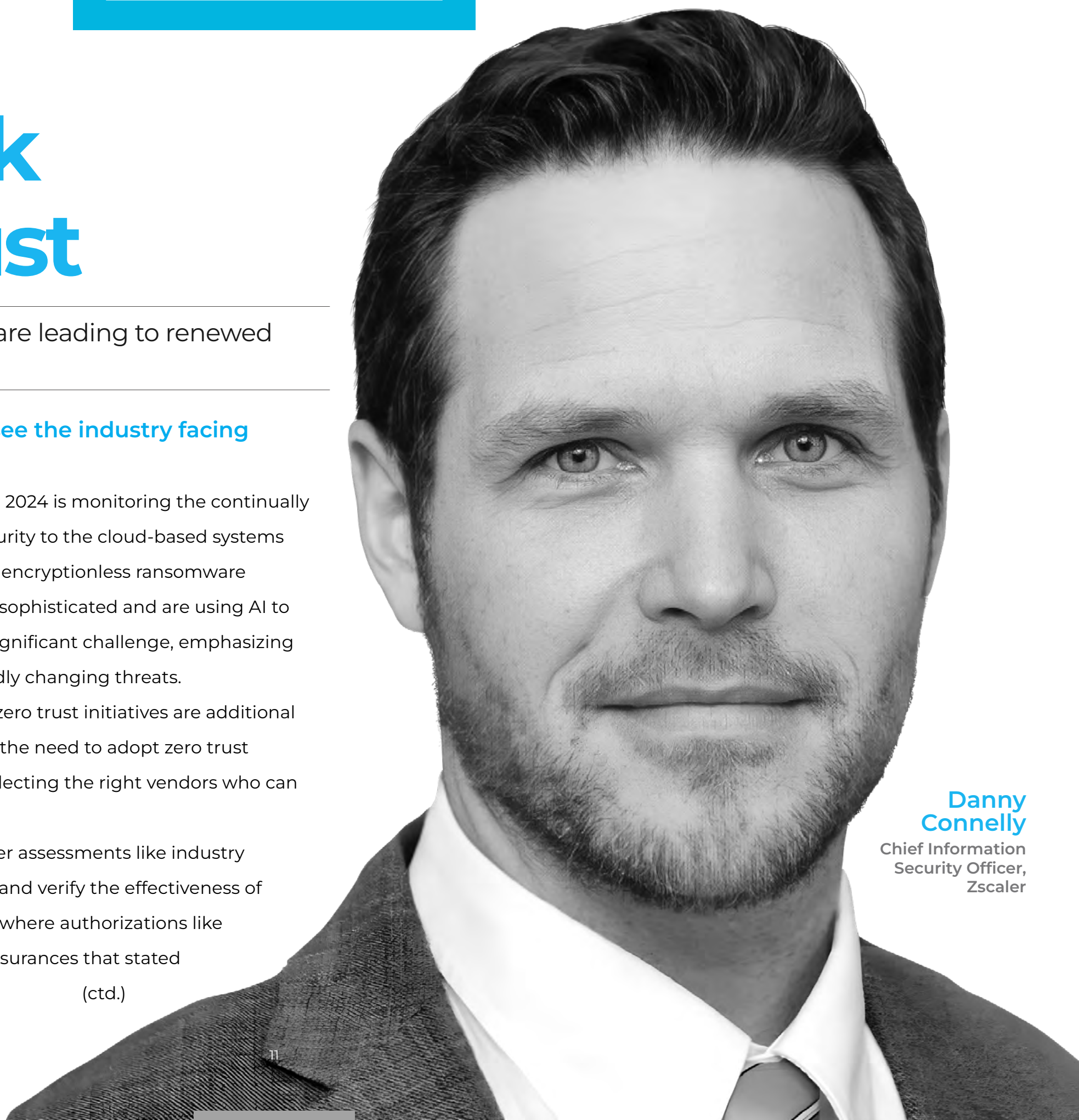
 **What are some of the challenges you see the industry facing next year?**

Connelly One of the most notable challenges for 2024 is monitoring the continually evolving threat landscape, and adding even more security to the cloud-based systems that will support the 2024 elections. The recent rise of encryptionless ransomware attacks has shown that attackers are becoming more sophisticated and are using AI to optimize their attacks. These evolving tactics pose a significant challenge, emphasizing the need for agencies to adapt and stay ahead of rapidly changing threats.

Shifting security to the cloud and implementing zero trust initiatives are additional challenges. Amid the call for heightened security and the need to adopt zero trust principles, federal agencies face the difficult task of selecting the right vendors who can truly deliver on zero trust promises.

It is crucial for federal agencies to go beyond paper assessments like industry reports or vendors' claims. They must thoroughly test and verify the effectiveness of solutions through proof of concepts and pilots. This is where authorizations like FedRAMP and DoD Impact Level can give agencies assurances that stated capabilities can actually be delivered.

(ctd.)



Danny Connelly
Chief Information Security Officer,
Zscaler

“Having a dual focus on security and innovation will lead to a more secure and resilient federal IT landscape as agencies truly embody the concept of ‘never trust, always verify.’”

**— Danny Connelly
Chief Information Security Officer,
Zscaler**

Additionally, agencies continue to grapple with the persistent issue of general malware and phishing attacks. While organizations sift through various vendor solutions, they must simultaneously address these ongoing threats to their security.

 **What are some of the biggest federal IT developments this year that you see transforming operations heading into 2024?**

Connelly One of the more significant developments has been the increased implementation of zero trust initiatives. Agencies have made concerted efforts to establish formalized zero trust programs, such as appointing dedicated zero trust leads or creating working groups.


These individuals or teams are taking the lead in driving the adoption of zero trust technologies and principles within their respective agencies. This represents a crucial step toward the widespread adoption of zero trust practices across the federal government.

By embracing zero trust principles, agencies can significantly enhance their security posture by continuously verifying device, identity, posture and threat.

Additionally, artificial intelligence and machine learning are reshaping IT operations. Organizations are leveraging generative AI and predictive analytics to be more proactive in detecting and mitigating threats. Behavioral analysis also stands out as a critical tool in empowering organizations to detect potential breaches and providing valuable insights to strengthen cyber defenses.


The increased focus on zero trust initiatives and advancements in AI/ML will continue to shape federal IT operations, as seen in the new federal guidance that has come out around emerging issues such as AI and DevSecOps. Having a dual focus on security and innovation will lead to a more secure and resilient federal IT landscape as agencies truly embody the concept of “never trust, always verify.” (ctd.)



 **In what areas do you see shifts in the economy impacting how agencies will prioritize technology?**

Connelly Although agencies are not immediately affected by economic downturns, they grapple with perennial budget constraints. Operating on a two-year budget cycle adds to the pressure, demanding foresight into desired solutions and associated costs. Agencies have to meticulously plan not just for immediate needs, but also for sustained integration of solutions into future budgets. Agencies have to figure out what solutions are going to work for them and then get funding.

On top of that, the evolving technology landscape presents a double-edged sword for many agencies. While they actively adopt new tools and technologies to fortify their security stacks, the unintended consequence is a proliferation of solutions that need to be managed, maintained and financed.

Recognizing this, agencies then face a consolidation phase while looking at ways to streamline and optimize their environments. Organizations like Zscaler can create a positive financial impact for government agencies by optimizing technology costs and eliminating legacy applications, reducing operational complexity and freeing up valuable technical resources. 



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

VA Prepares for EHR, AI Priorities in 2024

The agency saw some largescale digital developments this year around EHR modernization and increased health care demands.

BY JORDAN MCDONALD

The Department of Veterans Affairs saw key IT developments this year that included updates around PACT Act implementation, electronic health records modernization and other key concepts such as zero trust.

Now as the agency heads into the new year, it faces continued progress toward these initiatives especially as it relaunches its EHR modernization effort, continues its push for hiring claims processors and other technology talent amid a shifting hybrid workforce, and other administration targets especially around artificial intelligence development.



Hiring, Digital Services Meet Health Care Demands

The VA said it set all-time records in a number of categories when it came to delivering care to veterans in 2023. More than 116 million health care appointments were delivered to veterans, surpassing the previous record by more than 3 million appointments.

A big part of that number were made possible through innovations like telehealth and digital services like the Health and Benefits App, which celebrated its 1 million downloads milestone this year. VA also said in October it will be transitioning the My HealthVet portal to VA.gov so that users can manage all of VA health care in the same place.

In sum, more than 1.5 million veterans saw more than \$163 billion in earned benefits in 2023, including \$150 billion in compensation and pension benefits. The

VA also processed nearly 2 million veteran and survivor claims, an increase of 15.9% over the previous record. The VA also set new records for engagement, as over 2.4 million veterans applied for earned benefits, a 39% increase from 2022.

Backlog in claims originating from the pandemic spurred more demand for claims processors and automation as well as address the influx of hundreds of thousands of PACT Act-related claims. Since the PACT Act's passage, 76.7% of the 710,000+ PACT Act-related claims have been approved.

All of this was done by a workforce that expanded to more than 400,000 employees at the Veterans Health Administration and more than 32,000 employees at the Veterans Benefits Administration. VA across the board plans to hire nearly 52,000 employees per year over the next four years.

EHR Program Reshuffles

The VA froze its electronic health record modernization program in April 2023 and paused future rollouts as leadership conducted an assessment and realignment of the program.

The freeze followed an “assess and address” period, during which the agency drafted a report about needed changes to mitigate existing issues with accuracy, enterprise standardization and reliability of data in the new EHR.

“We’ve heard from veterans and VA clinicians that the new electronic health record is not meeting expectations — and we’re holding Oracle Cerner and ourselves accountable to get this right,” VA Secretary Denis McDonough said in a press release at the time of the freeze. “This reset period will allow us to focus on fixing what’s wrong, listening to those we serve, and laying the foundation for a modern electronic health record that delivers for veterans and clinicians.”

The Oracle-Cerner EHR program is likely to pick back up in the new year. In September, Tanya Bradsher was confirmed as the agency’s deputy secretary — whose role is to oversee the program. Bradsher embarked on a listening tour of the five sites using the new record as she builds a robust plan for it in 2024.

“Right now, with the reset, we are taking a hard look. We’re working with our clinicians and making sure that we are up and running,” Bradsher said of her listening tour. “This is a wonderful opportunity for me to learn from our clinicians and to bring back not just what I’m being told sitting in meetings and on Teams, but to actually see it on the ground, see how it’s working, see if it’s up.”

The next rollout is scheduled concurrently with the Defense Department’s

“We’re working with our clinicians and making sure that we are up and running. ... This is a wonderful opportunity ... to actually see the [EHR] on the ground, see how it’s working.”

— Tanya Bradsher, Deputy Secretary, Department of Veterans Affairs

Tanya Bradsher

Deputy Secretary,
Department of
Veterans Affairs



rollout of MHS Genesis at the Lovell Federal Health Care Center in North Chicago.

Sites that have not taken on Oracle-Cerner have continued to use the VA's legacy system Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS) to deliver health care.

VLM Doubles in Size

The digital Veteran's Legacy Memorial saw its largest expansion this year since its creation in 2019. The platform grew from 4.8 million records in May to 9.8 million by Veterans Day.

The nearly 10 million records were pulled from databases from VA cemeteries, DOD-managed cemeteries including Arlington Cemetery, 13 of the 14 National Park Service cemeteries and from the more than 4,000 veterans laid to rest in 87 countries.

"This particular effort of adding nearly 5 million additional pages was fairly complicated. We were tapping into a database that was new for us," James LaPaglia, digital services officer at the National Cemetery Administration, told GovCIO Media & Research. "Within that database, there were all kinds of variations of locations and addresses and cemetery names."

Approximately 80,000 new records came from state, tribal and territory cemeteries and new gravesites like Gettysburg and New York's Green-Wood Cemetery, were added to the database. All in all, over 73,000 tributes have been inputted into the database.



Modernization in 2024

Looking forward into 2024, some of the agency's largest priorities will center around building frameworks for AI and EHR modernization.

VHA's National Artificial Intelligence Institute was one of the major players behind the White House's Blueprint for an AI Bill of Rights, which outlined the need for agencies to develop AI that is fair and trustworthy. That was followed this year by Biden's executive order directing agencies on how to do so, as national interests in harnessing the technology for national security and maintaining a competitive edge globally grows.

The institute kickstarted an AI Tech Sprint to spur creation of AI-enabled tools to help reduce employee burnout.

According to the VA, these tools have helped decrease employee burnout

20% between 2022 and 2023.

"AI solutions can help us reduce the time that clinicians spend on non-clinical work, which will get our teams doing more of what they love most: caring for Veterans," Under Secretary for Health Shereef Elnahal said in a VA statement. "This effort will reduce burnout among our clinicians and improve Veteran health care at the same time."

The VA will also hold a competition to reward a \$1 million prize to winning teams that create solutions in two key areas:

- Speech-to-text solutions to be used for notetaking during medical appointments.
- Document processing for faster integration of non-VA medical records into a patient's VA record. 🌟

The Outlook for Federal AI Development in 2024

Agencies will see more benefits as well as challenges with the adoption of AI into 2024 and beyond.

BY NIKKI HENDERSON

Artificial intelligence development has made significant impacts across agencies in 2023. This led to a White House executive order directing agencies to develop and use it responsibly.

In the new year, agencies across the board will be working toward the various directives of this order to not only to improve service delivery, but also to prevent malicious actors from abusing and misusing the technology.

As a result, agencies have released several strategies and other implementation plans. Here is a look at how agencies are thinking about the technology and some of its benefits by missions.

AI and Cybersecurity

In November, CISA unveiled a new roadmap for AI adoption specifically for cybersecurity. The roadmap establishes a more secure way to develop and implement AI capabilities with five lines of effort:



- Responsibly use AI to support mission.
- Assure AI systems.
- Protect critical infrastructure from malicious use of AI.
- Collaborate and communicate on key AI efforts with the interagency, international partners, and the public.
- Expand AI expertise in the federal workforce. (ctd.)

“Artificial Intelligence holds immense promise in enhancing our nation’s cybersecurity, but as the most powerful technology of our lifetimes, it also presents enormous risks.”

**— Jen Easterly, Director,
Cybersecurity and Infrastructure
Security Agency**

“Artificial Intelligence holds immense promise in enhancing our nation’s cybersecurity, but as the most powerful technology of our lifetimes, it also presents enormous risks,” CISA Director Jen Easterly said in a statement. “Our Roadmap for AI, focused at the nexus of AI, cyber defense and critical infrastructure, sets forth an agency-wide plan to promote the beneficial uses of AI to enhance cybersecurity capabilities; ensure AI systems are protected from cyber-based threats; and deter the malicious use of AI capabilities to threaten the critical infrastructure Americans rely on every day.”

AI and Data Modeling

The National Oceanic and Atmospheric Administration (NOAA) is using AI to provide forecasters more accuracy in weather data and climate modeling, as well as helping simplify moving data across multiple systems.

For CTO Frank Indiviglio, AI’s benefits have great power for the agency.

“AI helps us focus the compute that we have on things we’re really concerned with like hurricane models, AI can help us focus most of the compute on the storm rather than outside of the storm. It can help reduce data movement and help us get better answers,” said Indiviglio in a GovCast interview.

Still, Indiviglio says adopting AI is challenging.

“It’s a new technology that you have to really get your arms around and truly understand it. You have to have data scientists and machine-learning experts to build around your science teams,” he said. “You have to help your workforce so you can get to a place where you can rapidly adopt these things and make them usable and make sure people trust them. “ (ctd.)

AI for Health Care

The executive order is also calling on health agencies to focus on safety concerns around the technology. Per the order, the Department of Health and Human Services (HHS) will create an AI task force that will be utilized across the health care ecosystem.

The safety program will collect reports, examine harmful AI-related health care practices and establish resources to design AI educational tools.

The Department of Veterans Affairs is exploring how AI can help VA make better, faster and more-informed decisions — improving veteran health outcomes and benefits decisions while eliminating redundant administrative tasks.

“AI solutions can also help us reduce the time that clinicians spend on non-clinical work, which will get our clinicians doing more of what they love most: caring for Veterans,” a VA spokesperson said in a statement to GovCIO Media & Research.

AI is also aiding the National Institutes of Health (NIH) in overcoming big data challenges and offering hope to the National Cancer Institute when it comes to improving research and treatment options.

The National Center for Advancing Translational Sciences (NCATS) at NIH is utilizing AI in its 2024 through 2029 Strategic plan to tackle big data and develop innovations that will reduce costly and time-consuming barriers in translational research.

The National Cancer Institute is exploring AI to screen for and treat cancer and sees the emerging technology supporting treatment for patients. NCI is also looking into how AI can help advance alternative treatments to chemotherapy.

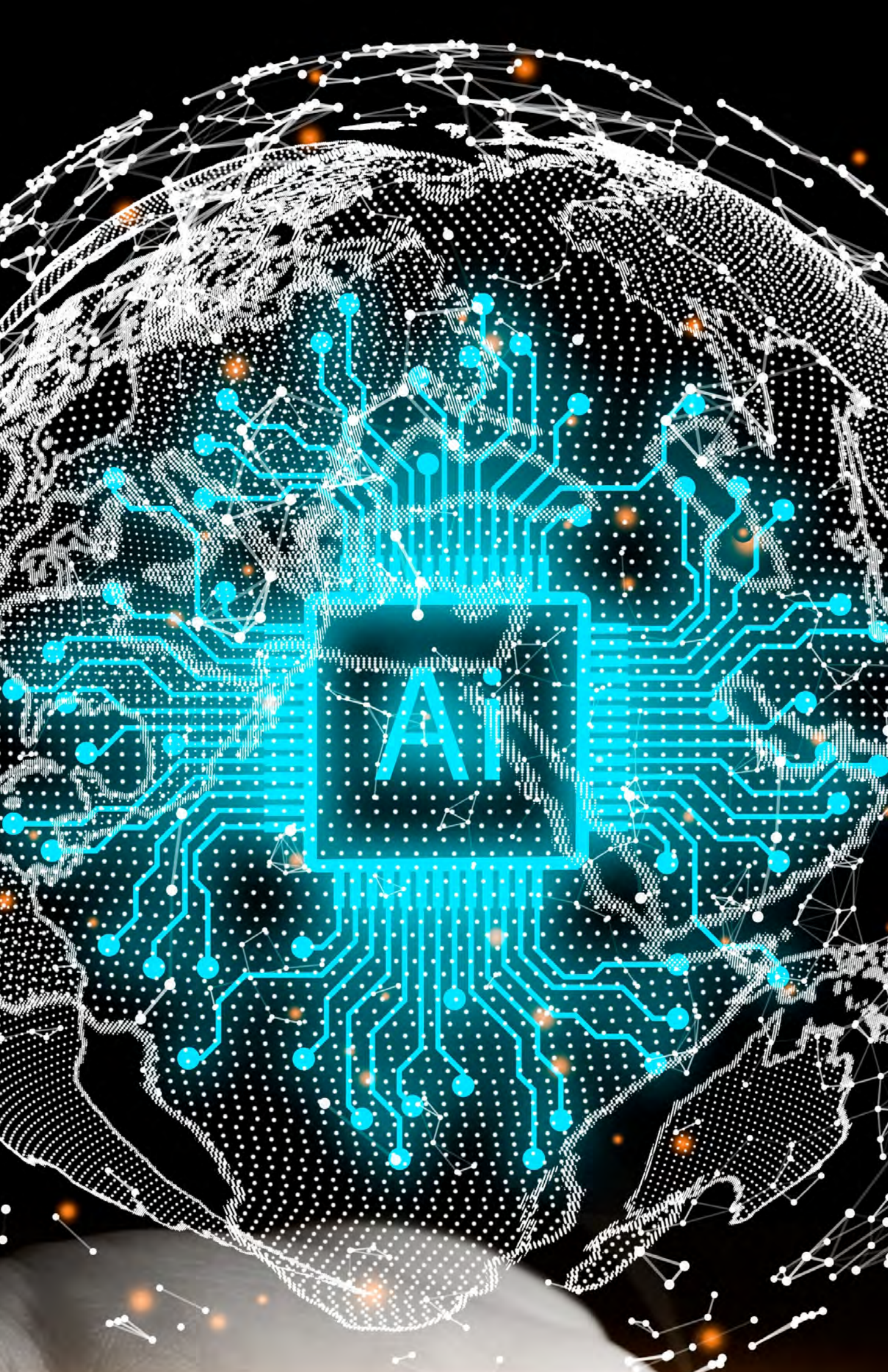
Federal leaders are also looking at AI’s impact on health equity.

The Office of the National Coordinator for Health Information Technology (ONC) is in the final stages of a proposed rule that would empower health care providers and ensure more transparency over algorithms used in clinical

Jen Easterly

Director, Cybersecurity
and Infrastructure
Security Agency





decision support. National Coordinator for Health IT Dr. Micky Tripathi said ONC is thinking more about health equity as a core design principle.

“One is starting with the data itself. You’ve got to have that data available in order to be able to identify where there might be communities that are getting different types of care,” said Tripathi.

AI Streamlines Workflows

USPTO Emerging Technology Director Jerry Ma said that AI’s role in the agency’s behind-the-scenes operational work has enabled the agency to deliver maximum value to the innovation community and stakeholders.

“AI has a central role to play in making sure that examiners are able to contend with that, which ultimately delivers value to our stakeholders because they receive benefits from stronger, higher quality and timelier patent and trademark brands,” Ma said.

According to Securities and Exchange Commission Chief Strategy and Innovation Officer Tanu Luke, AI is also providing the SEC with a better way to identify cybersecurity threats and fulfill requirements of the zero-trust mandate.

“We want to be mindful of more than just the immediate threats,” said Luke. “We want to look at how AI is going to help with identifying and proactively help with cybersecurity incidents in the future.”