GovCIO MEDIA & RESEARCH

SPRING 2023

DeepDives

Tools for IT Modernization

INSIDE:

SPONSORED BY

FORTINET FEDERAL®

GovCIO MEDIA & RESEARCH

From the writer's desk

Sarah Sybert, Senior Researcher

Turning Federal Modernization Plans into Action

As technology continues to evolve, government is looking to take advantage of new IT solutions to reduce administrative burdens, provide the public with user-focused interfaces, improve access to benefits and services and deliver a seamless customer experience, all the while driving cost efficiencies.

While the technology exists to make these concepts a reality, federal agencies face challenges with antiquated IT systems and lengthy procurement methods, leading to slow integrations and turnarounds.

Federal CIOs and tech leads are developing new pathways to speed up the modernization timeline and turn plans into action. The Technology Modernization Fund (TMF) is one tool in the federal modernization toolbox that is helping agencies retire legacy systems and deploy secure and efficient technology.

It's a long and winding road, but improving the tools and frameworks government has to implement modernization is a start.

Table of Contents

Sarah Sybert, Senior Researcher

Anastasia Obis, Staff Writer/ Researcher

Army to Invest Half a Billion Dollars in Critical Infrastructure

The Technology Modernization Fund will support the Army's Infrastructure Cyber Protection project, which will protect and modernize the Army's critical Infrastructure.

BY ANASTASIA OBIS

As cyber attacks become more sophisticated and bad actors shift their focus from informational to operational environments, sector leaders rush to address the growing threats to U.S. critical infrastructure. After more than two years of extensive studies and assessment, the Department of the Army is forging ahead with its Army Critical Infrastructure Cyber Protection (ACICP) project aimed to protect the department's critical infrastructure from cyberattacks. The service will invest about half a billion dollars in the project over the next five years with help from the Technology Modernization Fund (TMF).

The Army operates 23 depots, arsenals and ammunition plants across the United States to carry out a variety of missions, including repairing Humvees and tanks, manufacturing highly specialized equipment and serving as transportation sites, to name a few.

"These are all one-of-a-kind manufacturing equipment and facilities that don't exist anywhere in the world. There's only one in the world, and that's how sophisticated and niche they are," Raj Iyer, former Army CIO, said in an interview with GovCIO Media & Research.

As industrial equipment and machinery grow more sophisticated and interconnected, they track a wide range of data through sensors, including humidity levels on the floor, vibration or location of the machinery and equipment, power consumption and predictive maintenance.

The Army's assessment of its 23 industrial base facilities, directed by Congress through the National Defense Authorization Act several years ago, revealed some critical vulnerabilities that, if not addressed immediately, could pose a grave danger to national security.

"What we found was not that we were completely surprised by it, but quite

Photo Credit: Mark Cleghorn / DVIDS

Raj Iyer

Former CIO, U.S. Army

frankly, there was a lack of cybersecurity controls to the same extent that we would have on our traditional IT equipment," Iyer said. "This OT was not at the same level of cyber protection as the IT, but yet what we knew was if our adversary was able to come through any of these endpoints, whether it's OT or IT, because now they have access and entry into the network, they can actually go anywhere on the Army network. This created a huge awareness for us in the Army about how severe some of the risks were."

To fund the initiative, the Army turned to the TMF, established by Congress to address immediate security gaps and support the federal government's IT modernization efforts. Due to the budget cycles, if the Army wanted to address something immediate this year, it would have had to budget the fix back in 2019.

"The Army set money aside for the project in the 2024 budget, but prior to that it funded the work through the TMF, Iyer said.

The Army also wanted an avenue where it could address the problem in partnership with other agencies working toward securing the country's critical infrastructure.

"If we go out and try to solve it on our own … we are always very narrowly focused," Iyer said. "We felt it was important enough that we work with all the other agencies, we get the best practices and things that they are seeing, but also us being able to share with them. This is where I work with Clare Martorana, the White House CIO, the DOD CIO John Sherman, the Federal CIO Council where I sit as the CIO. And we hatched this plan to get after TMF funding."

To protect the operational technology at its organic industrial bases, the Army will use the security operations center-as-a-service (SOCaaS) model. The SOCaaS is an innovative approach where a third-party vendor fully maintains SOCs on a subscription basis.

This solution will allow Army IT leaders to ensure they are censoring all of their networks by tracking network traffic and identifying anomalous behavior in real time through analytics and artificial intelligence (AI). It will also allow red

team assessments to identify who can penetrate the networks, what attack vectors bad actors can use and potential vulnerabilities.

The Army is moving toward the SOCaaS model because it provides more flexibility and allows the Army to keep pace with ever-developing technology instead of running the risk of buying technology that becomes obsolete in several years.

“When we looked at how we were going to protect all this operational technology, the first thing we realized was the expertise in house didn’t exist. Even in our traditional IT, it’s taken us years. It was very clear that, at least initially, we needed an approach where we had to rely on industry to help us,” Iyer said. “The other piece, too, was we wanted to make sure that even though we are going to the industry, we needed whoever we brought in to help, teach us how to fish, right? They have to teach us and train us how to do this so we can become self-sufficient.”

The first transfer for the Army’s Critical Infrastructure project from TMF is currently in progress, with a total investment of $15,575,246. According to the initial assessment, the Army has about 500,000 devices across the industrial bases in need of security. The number is a rough estimate due to challenges associated with identifying the exact number of devices across all sites.

“Quite frankly, I don’t even know if it’s 500,000. We think it’s about 500,000, but it might be 700,000, might be a million — only because we have never actually cataloged every one of these things,” Iyer said.

Additional funding is needed, but the TMF investment will “stop the bleeding” and allow the Army good cybersecurity overwatch until full funding kicks in starting next year. The Army allocated about $100 million a year for this effort over the next five years.

“We are talking significant amounts of money, about half a billion dollars over the next five years, to actually go back, remediate everything, fix them up, but also modernize because what we believe is we have a lot of this old control

Photo Credit: Gorodenkoff/Shutterstock

system operation technology from the 1980s and 90s that are not secure — and we can never really protect them because of the old technology," Iyer said.

As for the 2023 goals, the Army's priority is remediating some of the extremely critical vulnerabilities at one of the 23 sites found during the initial assessment. The effort is classified, but it will serve as a pilot to allow the Army to understand how the SOCaaS model works, what changes need to be made to the architecture and distribution, what skill sets or training are needed, and how to work with vendors.

The ultimate goal is to modernize the Army's industrial bases as opposed to merely patching vulnerabilities.

"This is where we're also tying this effort into the Army's digital modernization plan. Army Materiel Command and Army have a plan in place to modernize the entire industrial base," Iyer said.

In working with the TMF, the Army received good feedback from the board of directors, who expect the Army to brief them quarterly on the progress made with the project. Through this process, the Department of Energy (DOE) has become the Army's closest partner.

"As the project moves further into the execution phase, the PMO will ensure that the project meets its goals by working with the project team to overcome any obstacles that may crop up. Successful implementation of this project will accelerate crucial protections at the Army's organic industrial bases and provide valuable insight to other agencies who face similar cybersecurity challenges. The project is anticipated to be complete in fiscal year 2027," a GSA spokesperson said.

Photo Credit: Baiploo/Shutterstock

“We are talking significant amounts of money, about half a billion dollars over the next five years, to actually go back, remediate everything, fix them up, but also modernize because what we believe is we have a lot of this old control system operation technology from the 1980s and 90s that are not secure and we can never really protect them because of the old technology.”

— Raj Iyer, Former CIO, U.S. Army

GovCIO MEDIA & RESEARCH

DeepDives

How the TMF Works

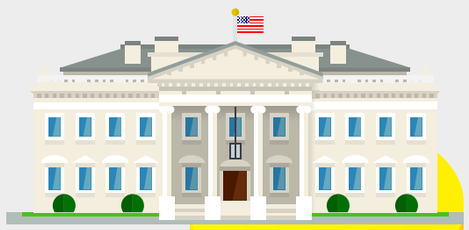
The TMF investment program gives agencies resources to improve service delivery to the American public, secure IT systems and data, and use taxpayer dollars more efficiently.

1

The TMF has received $175 million through the annual budget process and $1 billion through the American Rescue Plan to fund modernization projects.

2

The TMF is overseen by the Technology Modernization Board. Agencies submit IT-related project proposals for the board to review. Agencies submit modernization proposals to the board through a two-phased process.



6

The TMF has a flexible payback model, allowing for payback terms of up to five years.

5

Projects recommended for funding by the board receive incremental funding contingent on the successful execution of milestones.

3

PHASE ONE:
Agencies submit Initial Project Proposals (IPP) as a “pre-screen” to maximize the number of projects the board can review.

4

PHASE TWO:
If the board approves an IPP, the project team submits their Full Project Proposal (FPP) to the board. The FPP provides a full proposal description, project milestones and funding schedule.

Source:
The Technology Modernization Fund

PARTNER INTERVIEW

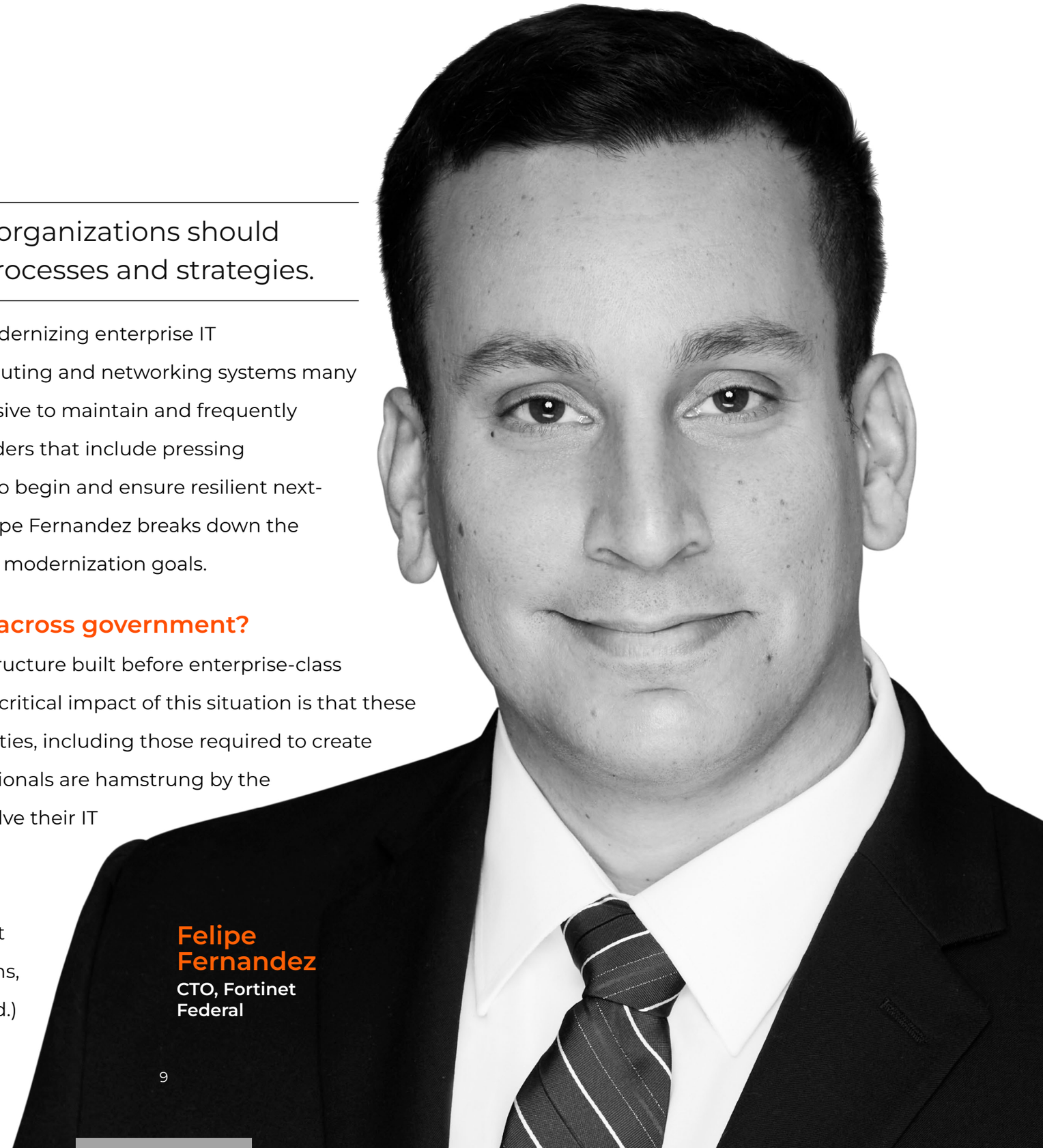
FORTINET FEDERAL®

GovCIO MEDIA & RESEARCH

Modernizing with Security in Mind

To effectively modernize aging IT infrastructure, organizations should prioritize agile and trusted cybersecurity tools, processes and strategies.

Government organizations have renewed their focus on modernizing enterprise IT infrastructures with security top of mind. The legacy computing and networking systems many rely on to support essential missions are unreliable, expensive to maintain and frequently incompatible with the latest technologies. With recent executive orders that include pressing requirements to implement zero trust architectures, knowing how to begin and ensure resilient next-generation cybersecurity can be daunting. Fortinet Federal CTO Felipe Fernandez breaks down the challenges, benefits and best practices necessary to meet agency IT modernization goals.



Felipe Fernandez
CTO, Fortinet Federal

Where are the critical areas for IT modernization across government?

Fernandez Federal agencies continue to support aging infrastructure built before enterprise-class computing systems were designed with security in mind. The most critical impact of this situation is that these systems cannot incorporate the best, modern cybersecurity capabilities, including those required to create resilient zero trust architectures. Consequently, government professionals are hamstrung by the inability to leverage the latest tools to help manage, defend and evolve their IT systems as requirements, missions and regulations dictate.

Today's challenge centers on when and how to modernize the infrastructure in a manner that doesn't impact the mission, does not compromise critical applications and services supporting U.S. citizens, and continues to make progress toward zero trust architecture. (ctd.)

“Aging IT infrastructure is a significant problem, but it is not too difficult to solve thanks to the innovations industry leaders have developed to refresh capabilities, provide better connectivity and ensure resilient operations. Regardless of the modernization approach, it is essential that the chosen technologies be tightly integrated with agile and trusted cybersecurity tools, processes and strategies.”

— Felipe Fernandez, CTO, Fortinet Federal

Aging IT infrastructure is a significant problem, but it is not too difficult to solve thanks to the innovations industry leaders have developed to refresh capabilities, provide better connectivity and ensure resilient operations. Regardless of the modernization approach, it is essential that the chosen technologies be tightly integrated with agile and trusted cybersecurity tools, processes and strategies.

How is your organization leveraging policies and guidelines from government to inform the development of your tools and services?

Fernandez Fortinet Federal regularly meets with federal agencies, including NIST, CISA and the Defense Department to ensure we understand their objectives, emerging guidance and concerns. Armed with this information, we can align our solutions with evolving agency requirements. Overall, Fortinet Federal strongly advocates for modernized IT infrastructures that are simplified — fewer tools that do more.

The primary method to meet these objectives is through product agility that encourages cybersecurity staff to accept the transition to modernized security architectures with flexible and adaptive solutions. Agencies can rely on standards-based methods for incorporating and ingesting data, normalized data inputs for rapid incorporation into zero trust architectures, resilient threat intelligence capabilities, and standards-driven methods for deploying network modernization capabilities. All these capabilities should be integrated into a highly portable platform that is not constrained by domain, enclave or location.

(ctd.)

How can IT modernization programs improve government agency security postures through migration to cloud alternatives?

Fernandez Innovative delivery models for cloud applications and services, delivered as a platform with all of its integrated capabilities, allow agencies to rapidly adopt hosted cybersecurity capabilities. Evolving “work from anywhere” approaches have continued to accelerate the migration to cloud-based applications and services from existing IT environments, which minimizes enterprise risk with enhanced hybrid cloud security. The latest cloud security management tools and solutions provide the federal workforce with the visibility, control and protection it needs to implement trusted cloud infrastructures that meet federal security requirements.

How is your organization delivering solutions to support federal modernization initiatives?

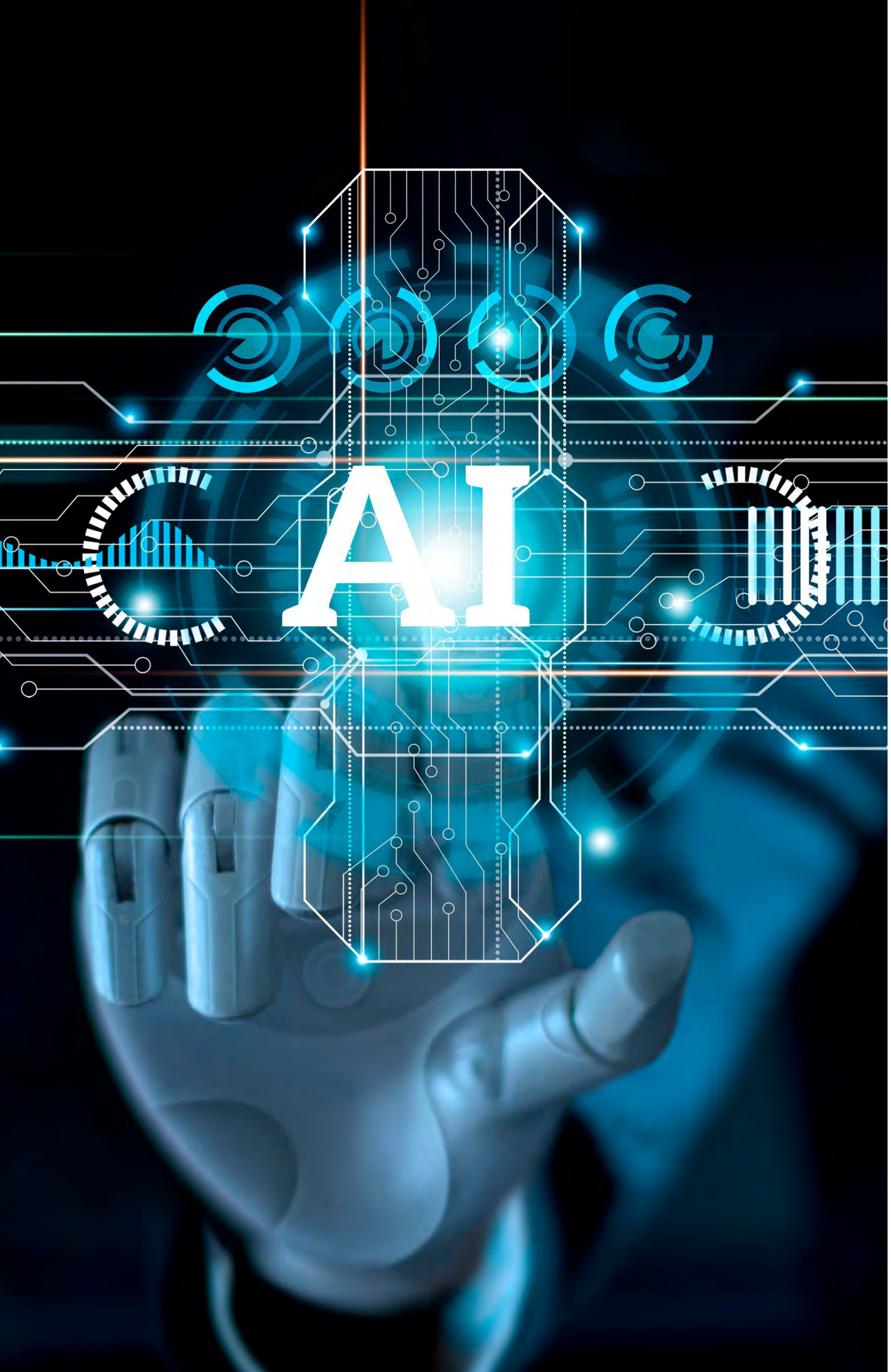
Fernandez Fortinet Federal delivers simplified, integrated security solutions that work seamlessly with third-party vendor products and legacy systems. This integrated approach eases the difficulty of modernization transition while maintaining the operational capability and integrity of mission-essential systems. Further, this deployment strategy enables large-scale transition for high impact through rapid deployment.

For example, Fortinet Federal has supported one ambitious federal civilian agency transformation initiative that in six months completed a 7,000-site upgrade. This success was due to a single platform delivering multiple capabilities that were implemented quickly. With the current tools and expertise, agencies can modernize multiple sites effectively with minimal operational disruption.

Fortinet Federal maintains partnerships with skilled implementation teams to ensure new cyber technologies meet agency modernization expectations.

(ctd.)

Photo Credit: sdecoret/Shutterstock



What are the top IT security tools and priorities you'll focus on in 2023 to help agencies create trusted, modern enterprise IT environments?

Fernandez The first priority is to keep abreast of the IT modernization and cybersecurity priorities so we can adapt technologies and solutions accordingly.

Second, Fortinet Federal is committed to helping agencies overcome the cybersecurity skills gap challenges by making clear the opportunities to leverage technologies to fill the gaps. Current technologies can be configured to automate tedious and repetitive tasks that currently burden cybersecurity professionals. AI-enabled tools are available to help agency staff to learn the capabilities they need to tailor applications to best meet their missions.

Organizations no longer can procure an amalgamation of diverse products and expect them to work in harmony without intervention. For example, when it comes to zero trust architecture implementation, there are plenty of actions left to agencies to incorporate. Fortinet Federal leverages replicable experiences and purpose-built solutions to ease IT modernization — whatever the architecture, mission or timeline.

At Fortinet Federal, we want to make sure there are zero excuses to not modernize and not incorporate innovative cybersecurity solutions — to enhance agency, department and national cybersecurity postures everywhere.

Photo Credit: PopTika/Shutterstock

FORTINET FEDERAL®

Modernize Networks for Security, Simplicity, and Scalability.

Everywhere You Need It.

LEARN MORE

The Future of Federal Case Management Modernization

EEOC, NARA and VA are accelerating case management modernization to prepare for the digital future.

BY SARAH SYBERT

Legacy systems and paper-based processes have been the foundation of federal case management, but agencies are looking to modernize these frameworks to move to a new, digital model to improve efficiency, reduce errors and quickly deliver services to citizens.

"As with many agencies, the National Archives and Records Administration (NARA) has incurred technical debt over the years, and it has become harder to maintain some legacy systems due to the high cost of maintenance agreements and upgrades," NARA CIO Sheena Burrell told GovCIO Media & Research.

Agencies also faced new challenges from the COVID-19 pandemic due to closed facilities and reliance on paper-based processes, which created new delays and backlogs. For instance, the backlog at the Military Personnel Records Center grew to exceed 500,000 requests following the onset of the pandemic.

"These unanswered requests are from U.S. veterans and their family members for copies of military service records they need to access benefits earned through military service," Burrell said. "Other mission areas for NARA had an additional backlog of nearly 230,000 requests from the Veterans Benefits Administration (VBA) for historical claims folders needed to support veterans' claims for benefits with the VA."

VBA's Joshua Jacobs, nominee to be under secretary for benefits, noted that the recently signed PACT Act will cause claims backlogs to rise as veterans become eligible for new benefits from their time in service. VBA is focusing on

workload management to balance both new and existing claims to optimize the speed at which veterans receive care.

"We will likely see challenges with timeliness because of just the sheer size of the volume. What we're going to do is work to prioritize the claims that are most timely," Jacobs said in August during a seminar at DAV's National Convention in Orlando. "I think it's probably going to take several years for us to try to get back to normal once we expect all these claims coming in." (ctd.)

Photo Credit: Stock-Asso/Shutterstock

Sheena Burrell

CIO, NARA

A joint memo between NARA and Office of Management and Budget (OMB), M-19-21, has been a major catalyst to case management modernization. A subsequent memo, M-23-07, extended the deadline requiring agencies to move toward fully digital records to June 30, 2024. While Laurence Brewer, NARA's chief records officer, said this date could be pushed back because of delays from the pandemic, the end goal is to reach a "paperless government" soon.

To do this, agencies are turning to digitization, automation and inter-government investment programs like the Technology Modernization Fund (TMF).

How does TMF play a role in digitization?

TMF gives civilian agencies the ability to invest in IT modernization projects through incremental funding and technical expertise. The goal is to provide agencies with additional ways to deliver services to the citizen more quickly, better secure sensitive systems and data, and use taxpayer dollars more efficiently.

In May 2022, NARA received over $9 million to upgrade two of its legacy systems to cloud-based platforms: the Archives and Records Centers Information System (ARCIS) and the Case Management and Reporting System (CMRS). These systems were developed in the early 2000s, and the software requires extensive customization, which is labor intensive and not cost-effective to maintain, Burrell noted.

The investment will allow veterans and their families to electronically request and receive their records, while improving responsiveness as the agency transitions toward digital recordkeeping. It will also allow NARA staff to fulfill records requests remotely, fully digitally and securely.

"One benefit of replacing our legacy case management system with a cloud-based platform is cost, a move to a more flexible platform is more cost effective to maintain," Burrell said. "We will also provide for a more flexible system that will meet the high standards and requirements for cybersecurity of a mission-critical HVA system." (ctd.)

The Equal Employment Opportunity Commission (EEOC) also received TMF funding in 2019 to modernize its Charge and Case Management System project. The agency launched a new system it calls the Agency Records Center (ARC).

Before ARC, EEOC's charge and case management program ran on an outdated and slow backbone system that relied heavily on proprietary technologies and required the use of precise alphanumeric codes, rather than plain language, to record case information.

"ARC provides many benefits to internal EEOC productivity, provides better customer service for employers and employees, as well as our state agency partners," an EEOC spokesperson told GovCIO Media & Research. "One example of improved productivity is replacing the manual entry of action codes with plain language, event-driven transactions. ARC's implementation replaced a system with a steep learning curve for staff, who required a burdensome binder to lookup action codes."

Where automation comes into play

Automation holds great potential when it comes to case management to streamline workflows, increase efficiency and reduce operational costs. Without automation, case workers and claims adjudicators rely on manual, outdated and inefficient tools to delegate, drive action, follow-up, resolve issues and deliver services to citizens.

"Modernizing [ARCIS and CMRS] would provide for faster case processing, automation, modern features, and capabilities such as HSPD-12 two-factor authentication and integration with NARA's Identity Provider and Email Tool Suite," Burrell said. "Modernization would also allow for automated field-level auditing as well as planned, future deployments of data encryption at rest and in transit and data loss prevention."

To reduce backlogs and provide new ways for technicians to securely access records remotely, NARA is creating a virtual desktop interface (VDI) that will

Photo Credit: metamorworks/ Shutterstock

enable access to records within the cloud. Through a partnership with the Department of Veterans Affairs, which presently has over 300,000 digitized military records stored in the cloud as well as 1.5 million records stored in other systems, the National Personnel Records Center (NPRC) technician will be able to access the digitized records from a remote location for processing.

"Implementing an intelligent automation processing solution is key to NARA's VDI tool and the goal of reducing the growing backlog of requests," Burrell said.

Burrell said that NARA also plans to implement an intelligent automation processing solution, which will assist in streamlining operations and expediting processing of Certificate of Release or Discharge from Active Duty (DD214) requests. The solution will determine the type of records that are being requested, search for responsive records from our repository of digitized military personnel records and create a draft response package for an employee to review before sending for digital delivery.

"Automating manual tasks of searching for responsive records and preparing responses will substantially reduce the time to process a veteran's record request, if the records have been digitized," Burrell added.

For EEOC, the agency automated several charge management processes within ARC, which will improve data quality and reporting. Automation will also make other advanced technologies easier to integrate in the future.

ARC's modernization and automation has enabled EEOC staff to spend less time on data entry and has improved data quality and reporting mechanisms to better monitor work, assess progress on key goals and identify areas that need additional resources.

"Due to the limitations of the legacy platform, our state partners … previously used non-digital methods to share information, further taxing their limited resources and our own. With the deployment of ARC … [state partners] enjoy the same automation benefits as the EEOC and have a common platform with the EEOC for sharing information," the EEOC spokesperson said.

As VA continues to modernize its claims management processes, Jacobs said his unit will rely on a "people, process, technology" approach to reduce workforce burden and streamline claims following the PACT Act's passing.

The agency is also looking to optimize processes, focusing on unnecessary evidence gathering and ways to cut down the amount of time that it takes for the evidence cycle, as well as integrating automation to improve technology

Photo Credit: SOMKID THONGDEE/Shutterstock

and data use to drive a more efficient process that delivers benefits to the veteran more quickly.

"We shouldn't have to require [veterans] to go fill out additional paperwork, bring those papers in. We shouldn't have to go through big piles of paper, piece by piece. We should let the machines do that. Make sure that machines do well what they do, and then humans do well what humans do," VA Secretary Denis McDonough told GovCIO Media & Research. "Those are the three things we've done: hired people, we've improved the process itself, and we're automating the process."

Modernization adds up to improved customer experience

Automating case and claims management processes will help streamline delivery of benefits and services to citizens as well as boost customer experience. Burrell explained that NARA is modernizing public-facing digital services by:

- Incorporating modern user experience methods and measuring tools
- Enhancing customer self-help capability through AI/ML features
- Improving user access by supporting all common access methods regardless of end-user device
- Addressing present performance and service shortfalls like core functions and delivery services

"Putting the requestor at the center of the system interface design is the key to NARA's modernization plan," Burrell said.

Before the pandemic, NPRC offered limited opportunities for the public to request records electronically, but the process was complicated, and most requests were still fulfilled on paper. During the pandemic, the NPRC expanded its digital services to the public by improving the web interface and expanding digital delivery of responsive records.

"The current system is a barrier to fully electronic processing of records requests at large volumes," Burrell noted. "NARA will replace the legacy platform and public-facing website with a modern customer relationship management platform and bring a user-centered design approach to addressing obstacles to users' needs."

EEOC noted that these modernization efforts have improved the quality of its services. While citizens previously had 24/7 access to their cases, ARC significantly improved the granularity and quality of data available to constituents.

"This applies to both individuals who filed a charge of discrimination and

Photo Credit: PopTika/Shutterstock

companies responding to these allegations," the EEOC spokesperson said. "The parties can now access their case information, add documents, address matters related to the case, and check the case status whenever it is convenient for them."

What's on the horizon?

Moving forward, agencies will focus their modernization strategies around digitization standards, data transparency and innovative tools that help sift through massive amounts of case and claims data.

"Like other agencies, NARA is looking to improve our cybersecurity efforts as they relate to the mandates around zero trust architecture," Burrell said. "We plan to do more in this area as well as digitization and automation."

Burrell noted that as more information moves to a digital format, NARA will prioritize cybersecurity. She explained that the agency's legacy platform is so highly configured that it relies on dedicated specialists to monitor, patch and customize to keep it aligned with NARA's overall cybersecurity plan and standards.

"By replacing it with a FedRAMP-approved cloud-based software-as-a-service (SaaS) platform, the modernized systems will benefit from dedicated monitoring and patching by the cloud provider, which will lower NARA's overall risk and harden its cybersecurity posture," Burrell said.

For VA, the agency is looking to hire more staff to accommodate additional claims. McDonough estimated the agency would an additional 2,000 new employees within VBA at the end of 2022. VA CIO Kurt DelBene also told GovCIO Media & Research that the agency will continue to bolster automated capabilities to alleviate workforce burdens and deliver veteran benefits faster.

"The goal, first and foremost, is to automate the collection of data that allows the claims agent to be more effective in his or her job," DelBene said.

"By replacing it with a FedRAMP-approved cloud-based software-as-a-service (SaaS) platform, the modernized systems will benefit from dedicated monitoring and patching by the cloud provider, which will lower NARA's overall risk and harden its cybersecurity posture."

— Sheena Burrell, CIO, NARA