HOW AGENCIES ARE MODERNIZING MODERNIZATION



govloop

IT modernization has always had an image problem. While the goal is to deliver faster, more efficient systems and services, the modernization process is often seen as being too slow and cumbersome, making it difficult to keep up with the latest innovations in the private sector.

That is a big concern of federal IT leaders, according to the recent EY Center for Modernization survey of public-sector officials. The survey found:

- **64%** of federal respondents said they were worried their infrastructure could not handle emerging tech.
- **69%** were also worried about having enough funding to modernize their infrastructure.
- **42%** were concerned about outdated hardware.
- **35%** were concerned about outdated software.

But agencies in federal, state and local government are trying new approaches to modernization, even as they face familiar obstacles. Here's a look at what's going on.

AI LOOMS LARGE IN MODERNIZATION LANDSCAPE

Artificial intelligence (AI) is expected to play a big role in modernization plans going forward, especially with the emergence of agentic AI. AI agents are trained to carry out specific tasks with minimal oversight. For example, an agent designed to monitor network performance might have the ability not only to identify a potential problem quickly, but also to determine the best way to resolve the issue.

We are still in the early days of agentic AI, but here are some ways that the technology could change modernization strategies.

Better self-service applications.

Unlike the current generation of AI-based chatbots, which largely are limited to providing information, AI agents will take a much more active role in helping customers, often resolving their requests without any human intervention, according to Gartner.

More complex automations.

While AI agents typically are designed to carry out specific tasks, orchestration tools or platforms will make it possible to coordinate the work of multiple agents to create a fully automated workflow. For example, according to a recent article in Harvard Business Review, an HR process might involve individual agents specializing in information retrieval, analysis, workflow generation and employee assistance, while another agent would coordinate their work.

More efficient project plans.

In a recent article, McKinsey analysts said that going forward, any large-scale IT project that does not involve AI "should be treated with skepticism." Augmenting the workforce with AI agents often can reduce costs and accelerate delivery, especially when used in large numbers.

Higher-level planning.

To take full advantage of this new approach to automation, organizational leaders must rethink their larger operating model, according to Forrester. "This includes rethinking workflows, governance, and engagement strategies that go beyond simple process efficiency," Forrester analysts wrote in a recent blog. The goal, they said, is to "architect the autonomous enterprise."

GSA TO REVAMP FEDRAMP

The U.S. General Services Administration (GSA) aims to take an innovative approach to its cloud security compliance program in hopes of giving agencies quicker access to new cloud solutions.

Over the years, industry vendors have complained that the FedRAMP authorizations are too costly and take too long. The problem, say GSA officials, is that the program relies on overly complex, manual processes.

The new initiative, dubbed FedRAMP 20x, would reduce unnecessary paperwork and automate large parts of the process, relying on cloud-native technologies.

"We're not just modernizing a process; we're reimagining how federal cloud security can work and providing agencies the ability to determine their own risk posture," said Thomas Shedd, Technology Transformation Services Director and Deputy Commissioner of the Federal Acquisition Service, in a statement.

In another change, GSA will no longer require vendors to find an agency sponsor for low-impact cloud solutions. The agency plans to revamp the security requirements to make them easier to implement. The goal is to provide FedRAMP authorization in weeks for most products, the agency said, instead of months or even years, as often has been the case.

STATES BET BIG ON CONSOLIDATION

In their efforts to improve the delivery of services to agencies, many state chief information officers (CIOs) are consolidating/centralizing different aspects of IT operations, according to a recent survey by the National Association of State CIOs. Top areas include:

- **90%** — Consolidating infrastructure
- **69%** — Consolidating services
- **64%** — Centralizing IT project management/oversight
- **60%** — Centralizing tech procurement in CIO organization
- **48%** — Consolidating IT personnel in central office

GAO: MAKE YOUR WORKFORCE CLOUD SAVVY

Given the importance of cloud to federal IT strategies, the Government Accountability Office is encouraging agencies to consider adopting practices that have proven successful in the private sector. In a recent report, GAO shared six best practices for preparing the workforce to take advantage of the cloud:

- ☑ **Identify skill gaps:** Identify workforce skill gaps resulting from the adoption of cloud computing solutions.
- ☑ **Retain and recruit:** Evaluate retention and recruiting strategies to address skill gaps resulting from the adoption of cloud computing solutions.
- ☑ **Provide resources:** Ensure that appropriate resources to operate systems in a cloud environment are available to the workforce.
- ☑ **Communicate consistently:** Ensure the workforce has dedicated opportunities to communicate with leadership before, during, and after migrating to a cloud environment.
- ☑ **Outsource selectively:** Outsource selectively when internal workforce is limited, to maximize cloud utilization and security.
- ☑ **Shift culture:** Ensure that internal controls and culture are in line with adopting cloud computing solutions.

Building a Network for AI Cybersecurity

Watch the interview



Artificial intelligence (AI) is already making work easier in countless ways, and it has the potential to transform how agencies function. In the cybersecurity realm, it can detect threats and take action faster and more accurately than ever before. But making the most of AI requires a high-performance network infrastructure that legacy systems can't provide.

Upgrading network infrastructure is more than just fixing what's broken. Done right, it can integrate AI so agencies get its full benefits, help them address new and growing security challenges, and automate more functions. But modernization isn't easy. Technologies such as Cisco's networking as a service (NaaS) can help.

In this video interview, Kevin Manwiller, Operations Director for National Security at Cisco Systems, discusses how AI can transform agency security and the network structure that's needed to support it. Topics include:

- Why agencies need AI to counter the current, and future, threat landscape
- What network capabilities best support AI cybersecurity
- How AI agents will change security response

"If you have the greatest AI tool in the world, but the network is lagging behind it and not providing the type of performance it needs, the AI tool is going to be viewed as a failure. Without the right modern network, AI actually can become a liability, instead of an asset."

Kevin Manwiller
Cisco Systems

ABOUT CISCO

Cisco is the worldwide technology leader that securely connects everything to make anything possible. Its purpose is to power an inclusive future for all by helping Cisco customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals.

LEARN MORE

How to Bring Greater Efficiency to Network and Cyber Operations



Network and security modernization initiatives have taken on new importance in recent months. With return-to-office mandates, agencies are concerned about the ability of their legacy infrastructure to handle the surge in bandwidth requirements. At the same time, as the threat landscape continues to evolve, agencies also are looking to adopt advanced cyber capabilities, such as defense-in-depth, micro-segmentation and zero trust.

Increasingly, agencies recognize they need to take what's known as a converged approach, integrating their network and cyber infrastructure in a common platform. This approach also helps improve the efficiency of IT operations, said Bill Lemons, Director of Systems Engineering at Fortinet Federal.

In this video interview, Lemons discusses best practices in shifting to a converged approach. Topics include:

- Closing the knowledge gap that hinders cybersecurity efforts
- Reducing the total lifecycle costs associated with managing infrastructure
- Incorporating new and emerging technologies into the IT environment

"You can create a consolidated environment that provides the full breadth of required services but with highly efficient management."

Bill Lemons
Fortinet Federal

ABOUT FORTINET FEDERAL

Fortinet Federal, Inc., a wholly owned subsidiary of Fortinet, Inc., is dedicated to delivering trusted cybersecurity and IT modernization solutions to U.S. Federal government agencies. Fortinet Federal provides the public sector with a comprehensive cybersecurity platform that combines advanced threat protection, secure access, and integrated cloud and network security to anchor any agency Zero Trust architecture. Trust Fortinet Federal to safeguard your agency operations and mission-critical assets.

LEARN MORE

FORTINET FEDERAL®

ABOUT GOVLOOP

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop



govloop