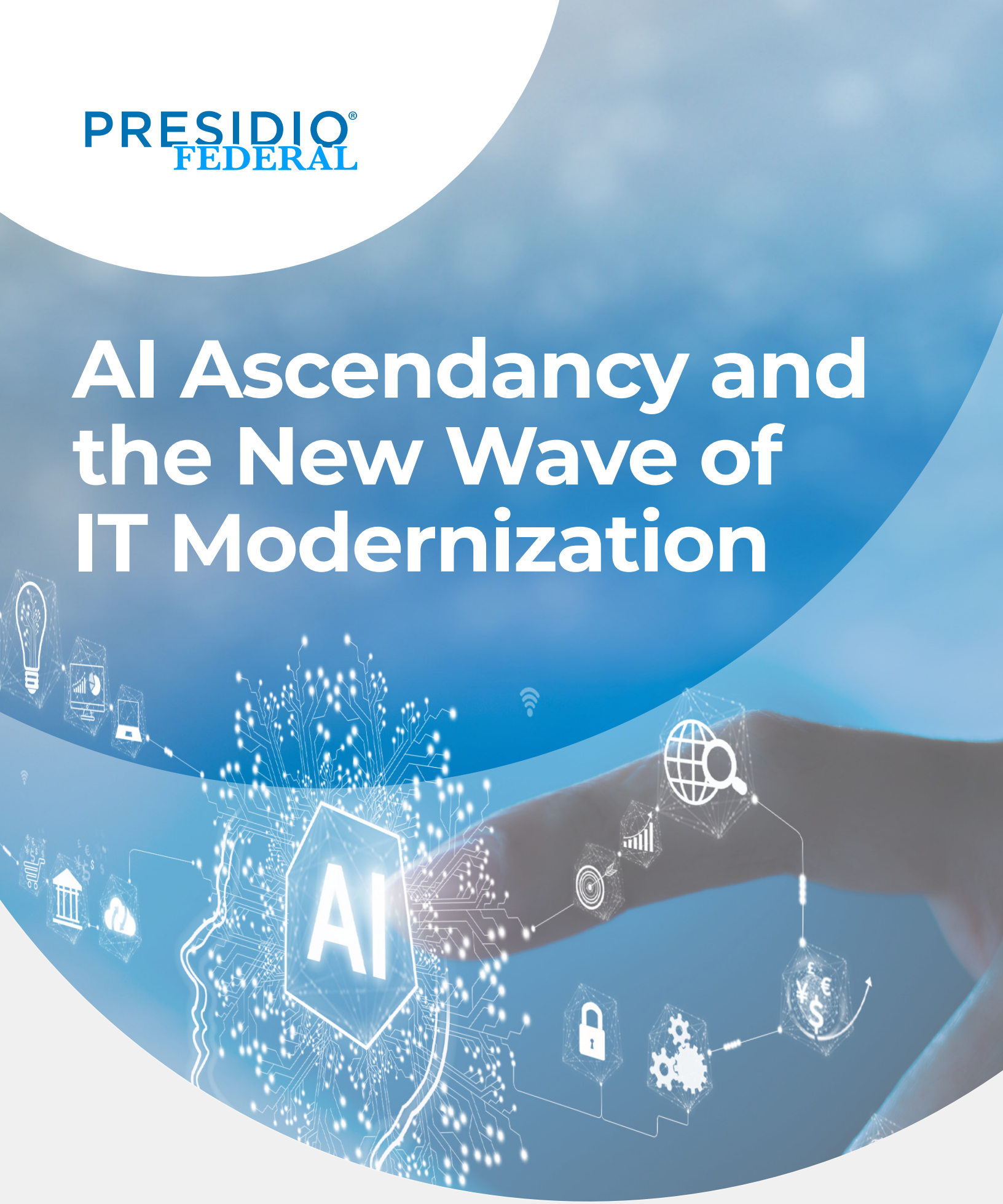
PRESIDIO® FEDERAL

AI Ascendancy and the New Wave of IT Modernization



WHITE PAPER | JUNE 2024

The landscape of IT modernization within the government is evolving at an unprecedented pace. As the number of executive orders, government mandates, new acronyms and powerful new tools continues to soar, defining an achievable path forward can pose challenges for federal agencies who are simultaneously focused on other modernization priorities, like cloud migration and cybersecurity.

Artificial intelligence and machine learning (AI/ML) are now a central part of government transformation strategies. These technologies, with their unparalleled ability to take in and make sense of vast amounts of data, have the potential to redefine federal agency operations – and, with these opportunities, pose new challenges in procurement, adaptation, and implementation. From customer experience (CX) to streamlining IT operations, agencies are expected to improve on all fronts, using secure and trustworthy tools, including emerging technology. This constantly changing environment underscores the need for a strategic approach to IT modernization within the government.

So what are the steps? What can agencies do to manage these competing and complex priorities within IT modernization? And what role might artificial intelligence play?

Step One

Use AI and automation to bolster, not replace, existing modernization goals.

Moving goalposts has been a consistent problem facing federal agencies as they work to bring their IT into the modern era. As technology morphs and changes rapidly, it can seem impossible to match pace with slow budget or procurement processes. The velocity of changes within AI/ML technologies has been particularly high, with systems that served a purpose six months ago already going out of date.

But reframing AI integration as a tool, rather than a goal, can help agencies modernize more effectively. AI/ML systems, with their unparalleled ability to collate and analyze vast amounts of data, can help agencies achieve both their technological and business goals even as they themselves mature. Using these tools in tandem can allow agencies to drive great efficiencies, improve modernization outcomes, and make the most of their data.

The Internal Revenue Service thinks of AI as "night vision goggles," according to commissioner Danny Werfel, that help it see through the enormous amount of complex data that the agency deals with every day. The IRS has two AI use cases on the horizon that will help alleviate some of the agency's challenges – virtual chatbots, helping taxpayers to navigate tax season, and AI tools that IRS agents can use to identify tax fraud. While privacy and data security concerns remain paramount, the agency sees AI as a game-changing tool that can empower both their employees and the public to engage effectively with the IRS's mission.

Step Two

To invest in mission outcomes, invest in employees.

With so many simultaneous mandates, the federal workforce is navigating a challenging landscape. IT modernization, enhancing customer experience, and the push to integrate AI can place strong emphasis on acquiring or developing new technology. But the heart of the federal government, and drivers of its mission, is not its tech – it is its employees. Prioritizing the upskilling and empowerment of current employees not only accelerates progress towards internal and external goals, but fosters a deeper understanding of the organization's needs. Empowered employees can more accurately identify gaps or areas that require external investment or partnership, as well as where additional hiring support is needed. Using technology not as a replacement for people, but as a tool to strengthen and amplify their skills, is the best way to ensure that IT modernization efforts translate into tangible benefits for the agency, its employees, and the public they serve.

United States Citizen & Immigration Services (USCIS) has used AI-powered chatbot Emma to answer frequently-asked questions in both English and Spanish since 2012. Now the agency is leaning into generative AI to enhance officer training. The agency will generate "dynamic, personalized training materials" that aim to support officers' ability to retrain crucial information, make better and more accurate decisions, and reduce the need for retraining over time.

Step Three

Anchor modernization in security.

This year will see high expectations of IT modernization for federal agencies. As the 2024 deadline for zero trust implementation looms, and expectations of AI implementation in government rise, it is more important than ever to move securely while moving swiftly. AI implementation, while a potential threat-hunting game changer, presents security challenges of its own around data and ensuring trustworthiness of the systems. Zero trust security models are closely tied with AI implementation and tech modernization overall, and are crucial in securing against the growing risks posed by new and unprecedented cybersecurity threats.

Security has always been an important component of IT modernization, but adapting and implementing technology at speed is itself a line of defense. A new category of threats is emerging, fueled by advanced AI tools capable of perpetrating fraud and probing cybersecurity defenses with unprecedented precision and speed. AI-driven threats can pose significant challenges to traditional security measures, including automated social engineering, phishing, and rapid exploitation of vulnerabilities.

And rooting modernization strategies in security is not simply about procuring the shiniest new system or software. An overwhelming majority of cybersecurity breaches are due to human error. Agencies must therefore think carefully about how to make employees partners in modernization, not simply recipients of it. Employees must be trained and equipped to identify and respond to cybersecurity threats effectively. This, combined with full zero trust adoption and thoughtful implementation of new technologies, is the key to enabling agencies to achieve their goals while safeguarding their operations against evolving threats and maintaining public trust.

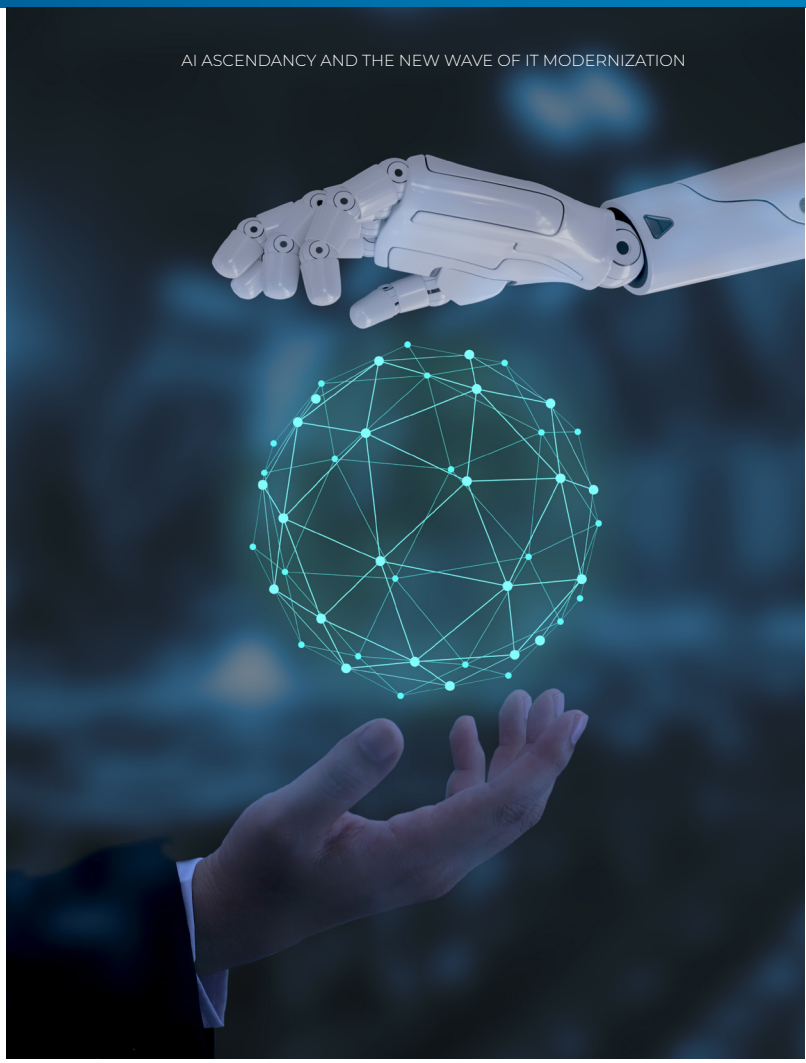
The Joint Cyber Defense Collaborative (JCDC), a group established to drive unified cybersecurity efforts across public and private partners, aim to help keep cybersecurity at the forefront of all modernization efforts across a number of sectors. Their 2024 priorities offer assistance and guidance in defending against persistent threats, raising the cybersecurity baseline, and anticipating risks posed by emerging technologies like AI. Striking the balance between innovation and security can be difficult, and the 2024 priorities aim to help make progress towards a world where technology is secure by design.

Step Four

Don't lose sight of the point of modernization.

Among the noise of new tools and capabilities, and of the need to stay on the forefront of innovation, IT modernization is about giving federal employees the right technologies to support their mission-critical work. Choosing investments wisely, based on relevance to an agency's mission and utility to its employees, is the best way to harness the full potential of technological innovation. Ultimately, modernization is meant to support the mission of government – providing services and improving the lives of the American people.

Veterans Affairs has long been at the forefront of innovative modernization for the good of those it serves. The agency expanded its telehealth services to provide digital care to veterans even in the most remote areas, including for mental health, serving 2.4 million veterans in FY23. Now, its groundbreaking electronic health records (EHR) system aims to create interoperable healthcare service for veterans. The EHR will house all medical records across a veterans' entire care, from their time in the service to records with the VA to local healthcare providers. The VA is also using AI to improve its healthcare services, including analyzing medical data, offering personalized care recommendations, and managing resources more effectively. These modernization goals were made to ensure that all veterans are receiving the highest quality of care, wherever they are.



Modernizing for the Future

IT modernization is an ongoing process, and with AI emerging as a powerful force, knowing where to go next can be a challenge. But by keeping major priorities in place – security, efficiency, and empowering the people both serving and served by government – agencies will be able to face the next chapter of their modernization journeys armed with the tools, the confidence, and the clarity they need.

About Government Business Council

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision-makers from across government to produce intelligence-based research analysis.

For more information, email us at research@govexec.com or visit our website.

Industry Perspective
A brief guide to driving IT modernization

As federal agencies turn the page and focus on the next chapter of their modernization journey, trusted partners will play a vital role in meeting key goals and expectations set forth by agency leadership and Congress.

"IT modernization offers the promise of speed, agility, personalization, simplification, and efficiency," said Thad Anderson, general manager for Presidio Federal. "But it also comes with the need for greater governance and guardrails."

Federal agencies facing resource constraints and increasing requirements can look to trusted partners like Presidio Federal to help effectively drive government modernization efforts and bridge the gap between legacy technologies and cutting-edge cloud-based services.

But what should federal leaders look for in potential partners? Jon S Kim, vice president of solutions and services for Presidio Federal, emphasizes the importance of selecting a partner that exhibits a "deep understanding of the unique challenges and regulatory requirements that federal agencies face." Moreover, this potential partner "should also have a proven track record of successfully implementing and supporting modernization projects throughout the federal space."

Digital transformation is more than just upgrading IT infrastructure. As agencies seek partners to help them effectively and efficiently modernize, they must also prepare internal leaders for the impact of modernization in three key areas:

1. Systems and network architecture
2. Operations and application delivery
3. The federal workforce

Preparing For Contemporary Service Delivery

The modern digital landscape is rapidly changing. As technology evolves, systems and network architectures must evolve to meet emerging requirements. As more employees work from home, for example, networks must evolve to accommodate remote data access. Enabling remote access to data and application services for large portions of the workforce, once a rare occurrence, is quickly becoming standard.

As agencies shift toward this more distributed model and the risks it introduces, IT modernization must be grounded in robust security governance. Enhancing security controls and training the federal workforce is critical to protecting data and networks from adversaries. However, protecting data is often easier said than done.

In the security operations center (SOC), federal employees protect and defend against threat actors, but handling such a significant volume of potential security threats can quickly become overwhelming. In a recent report published by IDC, approximately 23% of all security alerts are "ignored or not investigated" for organizations with over 5,000 employees. Robotic process automation (RPA) and generative AI could help SOC analysts better defend networks by connecting and creating a single, interoperable security platform.

Ultimately, IT modernization should focus on creating these "efficiencies of scale." Modernization should be focused on driving results for the end-user, as opposed to purchasing technology for technology's sake.

"The end user's experience is critical," Kim said. "It's not just about making things more efficient or buying more technology, users need to see the improvement themselves. At the end of the day, it should help streamline and optimize IT operations and help free up resources to focus on other strategic initiatives."

So, what should leaders do to prepare for digital transformation? While partnering with trusted private sector leaders can help expedite modernization, Anderson and Kim both emphasize that a successful modernization strategy is comprehensive, tailor-made and designed to align with an agency's mission, vision and goals. Beyond alignment, leaders should be on the lookout for plans that:

- Define how the federal workforce will receive training on new and emerging technologies and the benefits it will bring
- Emphasize phased implementation over single instance deployments
- Include strict governance and security requirements
- Clearly explain an agency's end goals and how the agency will get there, as well as the role of the partner and any shared responsibilities in this journey

Digital transformation doesn't have to be difficult. Trusted partners can help federal agencies accelerate modernization and build modern, contemporary agencies designed to meet the needs of citizens today and tomorrow.

"The pace at which technology changes is daunting," Anderson said, "but it's our job as partners to help the federal government navigate this change."

Click to discover how Presidio Federal partners strategically with federal agencies to support their digital transformation journeys.

Sources

"Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." White House. December 13th, 2021, Washington, D.C.
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

Konkel, Frank. "IRS commissioner indicates AI will play growing role in future tax collection." Government Executive. April 19, 2024.
https://www.govexec.com/management/2024/04/irs-commissioner-indicates-ai-will-play-growing-role-future-tax-collection/395867/

"Meet Emma, Our Virtual Assistant." U.S. Citizenship and Immigration Services. May 20, 2024.
https://www.uscis.gov/tools/meet-emma-our-virtual-assistant

Young, Shalanda D. "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." January 26, 2022.
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

"Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." White House. October 30, 2023.
https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

"Top Cybersecurity Threats in 2024." Forrester. April 5, 2024.
https://www.forrester.com/report/top-cybersecurity-threats-in-2024/RES180754

"Why Do People Make Mistakes That Compromise Cybersecurity?" Tessian. January, 2020.
https://www.tessian.com/resources/psychology-of-human-error-2022/

"2024 JCDC Priorities." Cybersecurity and Infrastructure Security Agency.
https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities

"Transforming Health Care for Veterans, Revolutionizing Health Care for All." Veterans Administration.
https://digital.va.gov/ehr-modernization/