

Digital transformation in government

Key trends for federal and state agencies

verizon

A woman in a light blue business suit and a man in a dark blue sweater and pants are walking through a server room. The woman is holding a tablet and smiling, while the man is gesturing with his hand. They are both wearing blue lanyards with ID badges. The server racks are visible on the left, and the floor has a grid pattern.



In the 21st century, citizens have seen a dramatic shift in how they interact with their government.

As the power of the internet and mobile devices drove greater online consumerism and new services over the last few decades, government agencies consistently lagged behind the private sector when it came to delivering compelling digital experiences.

Though public sector decision-makers were starting to push in recent years for IT modernization across government, it was the global pandemic that accelerated many of the developments we see today. Facing a workforce and populace that needed digital self-service solutions almost overnight, government agencies broke away from standard operating procedures to rapidly adopt and deploy modern technologies.

The momentum from the pandemic-fueled IT modernization surge has not abated. The desire across government to not just modernize legacy networks, hardware and software, but to digitally transform

operations has remained strong.

According to a General Dynamics Information Technology (GDIT) survey, two-thirds of defense, civilian, and intelligence agencies are reported as being moderately to extremely ready to embrace emerging technologies. The survey also found that one in three agencies identify increased security and enhanced productivity as the biggest motivations to adopt these technologies.

But what are some of the key digital transformation trends in government that are shaping the future of public services and mission readiness? How are government agencies reacting to the increased demand for better customer experiences, or the importance of better data management, accelerated cloud migration, enhanced workforce productivity and threats to network security?

Here are some of the key trends driving digital transformation in government.

Increased demand for digital services and better experiences



While the COVID-19 pandemic certainly hastened the push for digital services, the first big spark for innovation came when the 21st Century Integrated Digital Experience Act (IDEA) was signed into law in December 2018. 21st Century IDEA, which has received new guidance from the Biden administration (See “Delivering A Digital-First Public Experience” from the Office of Management and Budget), created a framework for modernizing government websites, digitizing documents and improving the customer experience.

Representative Ro Khanna, the bill’s sponsor explained, “Government exists to serve citizens, and this bill ensures government leverages available technology to provide cohesive, user-friendly online service that people around this country expect and deserve.”

In 2021, the Biden administration added to the advancements in digital services with the Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government, which declared, “Government must be held accountable for designing and delivering services with a focus on the actual experience of the people whom it is meant to serve. Government must also work to deliver services more equitably and effectively, especially for those who have been historically underserved.”

Despite notable progress over the past five years, there is still considerable work ahead to fully meet citizen needs. Deloitte’s 2023 digital citizen survey found that satisfaction with digital government services in the United States lags private sector services by nearly 40 percent.

“Government must be held accountable for designing and delivering services with a focus on the actual experience of the people whom it is meant to serve. Government must also work to deliver services more equitably and effectively, especially for those who have been historically underserved.”



Unlocking insights with data mining and enhanced strategies

Federal agencies are grappling with the management of an ever-growing influx of data, presenting dual challenges: determining the data to retain and devising efficient methodologies for analysis. To address this, President Biden's May 2021 Executive Order on Improving the Nation's Cybersecurity tasked the Office of Management and Budget (OMB) with outlining logging requirements for agencies. While the OMB has provided valuable guidance, individual agencies must still formulate their own tailored logging strategies that align with their mission.

Effectively harnessing this data necessitates collaboration with skilled data miners. The U.S. Government Accountability Office (GAO) employs data mining as a crucial component of audits and investigations. As evidenced in the GAO's 2023 Data Mining Results and Challenges for Government Program Audits and Investigations report - data mining yields

tangible insights into breakdowns in internal controls, facilitating the development and implementation of recommendations for enhanced controls to mitigate fraud, waste, and abuse.

The report concludes, "We are just beginning to make full use of data mining strategies. With the right mix of technology, human capital expertise, and data security measures, we believe that data mining will prove to be an important tool to help us to continue to improve the efficiency and effectiveness of our audit and investigative work for the Congress."

Accelerating movement to the cloud

While each agency is at a different stage of its cloud journey, movement to the cloud has had a huge impact in advancing the federal government toward digital modernization and enhanced efficiency.

The acceleration of cloud adoption is evident in diverse initiatives, such as the digitization of records, where agencies can receive valuable resources from the National Archives.

Moreover, cloud technology's influence extends to communication strategies, as evidenced by the implementation of cloud-based call centers equipped with advanced chatbots driven by natural language processing. This integration has the potential to refine customer service interactions, streamline responses, and elevate overall engagement.



Agencies are also actively engaged in data center and cloud optimization programs, fostering a more agile and cost-effective computing environment. The National Oceanic and Atmospheric Administration (NOAA), for example, has a program called the NOAA Open Data Dissemination (NODD). Zachary Goldstein, CIO of NOAA, explained in a Federal Executive Forum on Cloud Optimization in Government that “for effectively no cost we disseminate enormous amounts of information to the public and to industry to build on our data in the cloud.”

These programs and others enable collaboration and a faster adaptation to new technologies, which will continue to have a positive impact.

In the same Federal Executive Forum with Goldstein, Mark Lucas, Director of Cloud Computing Operations, Department of Homeland Security, said that the key is for agencies to remain focused on the “pursuit of industry and academic knowledge being created in cloud environments.” With this focus, Lucas proclaimed, “the government will be able to deliver services faster to the American public and with less human intervention, and of course with reduced errors, which translates to better and more accurate information for the public.”



Modernizing employees to increase efficiency and effectiveness

A pivotal focus of digital transformation also lies in modernizing employees to unleash their full potential and drive superior performance. Embracing collaborative tools stands as a cornerstone of this endeavor. As an agency's workforce becomes more distributed, efficient communication and seamless collaboration become paramount. Leveraging cutting-edge collaboration platforms facilitates real-time information sharing, enhances project management, and accelerates decision-making processes. These tools empower teams to work harmoniously across diverse locations, fostering a cohesive work environment.

In tandem, effective training, reskilling, and upskilling initiatives underscore the commitment to nurturing the best and brightest engineering talent. In a Federal Executive Forum on IT Modernization, Patrick Newbold, Assistant Deputy Commissioner and Deputy CIO of

the Social Security Administration, noted that, "digital modernization is a whole agency approach. If you're going to upgrade or replace technologies, we just don't want to do it to do it, [we] want to also look at processes and policies that better support business." Recognizing that the technological landscape evolves at a rapid pace, government agencies are dedicating resources to continuous learning. By offering tailored training programs and opportunities for engineers to acquire new skills, agencies position themselves at the forefront of innovation, cultivating a workforce well-equipped to tackle complex challenges.

Taking advantage of increased EIS funding



Harnessing the opportunities presented by increased funding, agencies across the government spectrum are strategically embracing the Enterprise Infrastructure Solutions (EIS) contract. This comprehensive solutions-based contract vehicle is fundamentally reshaping the way government entities approach their communications and IT services. Through EIS funding, the Department of State is spearheading the modernization of its global communications infrastructure, aiming to provide cutting-edge IT services to U.S. embassies worldwide. This initiative seeks to bolster diplomatic efforts through enhanced connectivity and real-time information exchange, fostering more agile and effective international engagement.

The Federal Bureau of Investigation (FBI) is also taking advantage of the funds awarded by the EIS contract, leveraging its capabilities to modernize and expand its network infrastructure. With a focus on data and voice solutions, the FBI seeks to amplify its operational efficiency, communication efficacy and information sharing capabilities. Simultaneously, the Department of Defense (DoD) is leveraging EIS to undergo a comprehensive modernization of its IT communications infrastructure. In a rapidly evolving security landscape, the DoD's commitment to embracing advanced communication technologies enhances its mission

readiness and responsiveness. The EIS initiative serves as a catalyst for these agencies, fueling their journey toward heightened connectivity, data-driven decision-making, and streamlined collaboration, ultimately fortifying their roles in national security and diplomacy.

Working toward Zero Trust

In preparation for the federal Zero Trust architecture strategy deadline of the end of FY 2024, agencies are putting in place practices and infrastructure. The Zero Trust concept rests on the foundational principle of distrust in any entity, both internal and external, seeking access to sensitive networks and data. Embracing Zero Trust entails treating every user, device, and network component as potentially compromised, mandating stringent identity verification and access validation before granting entry.

To operationalize Zero Trust effectively, the Secure Access Service Edge (SASE) framework emerges as a critical enabler. SASE converges security and networking services into a unified cloud-based architecture, simplifying the complex task of safeguarding dispersed networks and remote users. This innovative approach is particularly salient as government agencies increasingly embrace remote work and distributed operations. By replacing legacy VPNs with SASE, agencies can dismantle traditional network perimeters in favor of user-centric security, establishing a protective shield around each user, device, and application, regardless of their location. SASE empowers government entities to achieve a consistent and comprehensive security posture while optimizing network performance, scalability, and cost-efficiency, thereby aligning seamlessly with the Zero Trust ethos and federal requirement to deliver enhanced protection in the digital age.

Conclusion

In the dynamic landscape of government digitization, the acceleration towards enhanced digital services has been ignited by demands for convenience and efficiency. The transformative impacts of this shift have been underscored by the rapid adoption of digital self-service platforms, catalyzed by the COVID-19 pandemic. Amid this transformative era, agencies exhibit readiness to embrace emerging technologies, a drive propelled by motivations like heightened security and productivity.

To surmount these challenges and seize new opportunities, agencies are steering digital transformation efforts, leveraging data mining, cloud computing, employee modernization, and the Zero Trust security paradigm. This paper has delved into the diverse facets of current trends, illuminating the path forward for a more efficient, secure, and responsive government in the digital age.

To learn more about how Verizon can help your agency with its digital transformation journey, visit us at: [verizon.com/smartgovernment/](https://www.verizon.com/smartgovernment/)

See where your organization is in its digital transformation journey. Take our assessment at: [verizon.com/publicsectorassessment/](https://www.verizon.com/publicsectorassessment/)