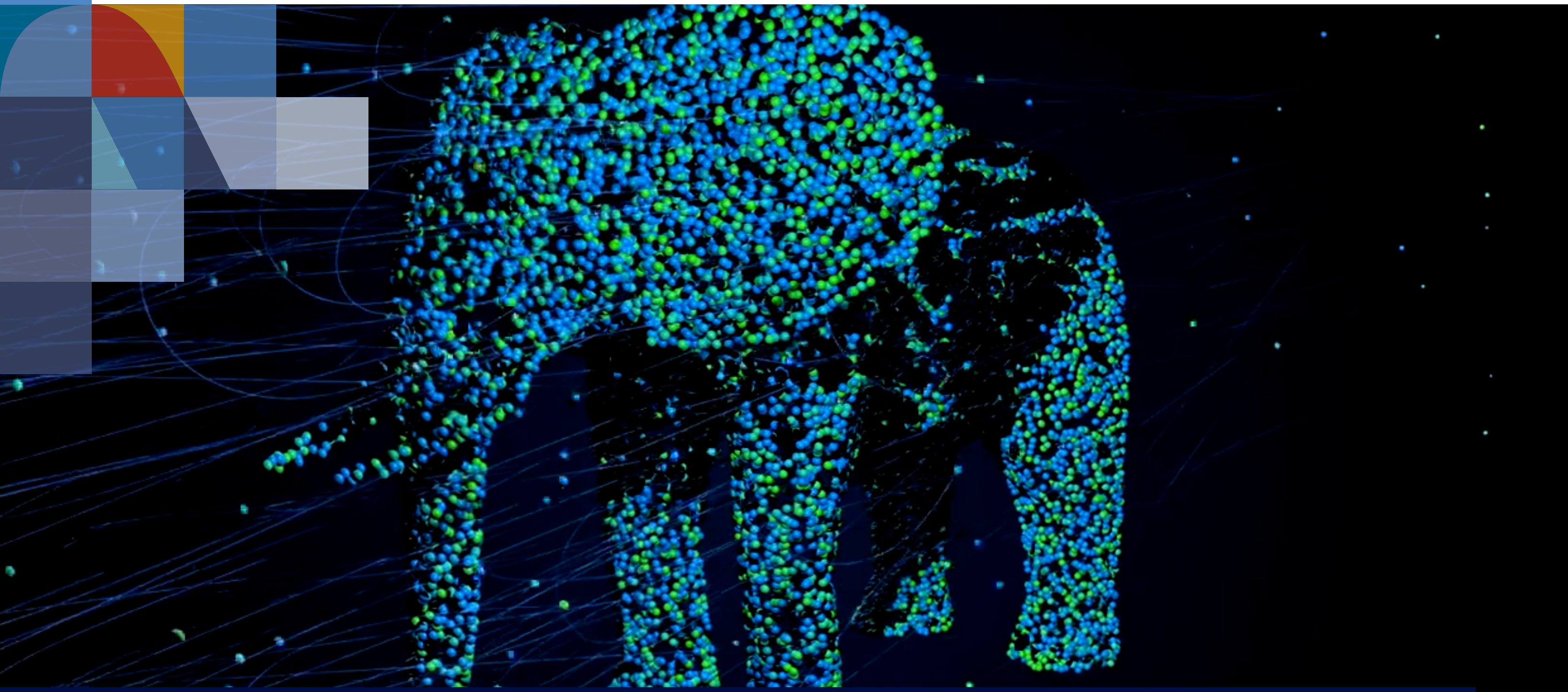

WHITE PAPER | PUBLIC SECTOR

Managing the IT Modernization Elephant

A bite-sized approach to digital modernization

Table of contents

There's an old saying, "How do you eat an elephant? One bite at a time." In some cases, the task of technology modernization is akin to eating an elephant. Government agencies are filled with legacy applications, many of which have been heavily customized over decades of operation. While moving to modern, cloud-based infrastructure and increasing cybersecurity are necessary, IT leaders often feel overwhelmed by the enormity of the task of modernizing legacy applications. It can be difficult to determine where to start when faced with such an extensive effort. This paper breaks down modernization into manageable initiatives so agencies can begin a modernization journey.

The Technology Modernization Fund emphasizes four special categories:[2]

- Modernizing high-priority systems
- Cybersecurity
- Public-facing digital services
- Cross-government collaboration/scalable services

Modernization starts with a vision

Decades of technical debt in government IT systems and disconnected processes hinder government agencies. It's left citizens unable to conduct business digitally with the government as they do with private industry. Operating on cost-intensive legacy systems reduces agency agility, creates cybersecurity vulnerabilities and limits citizens' ability to easily access services. COVID-19 catalyzed the need to efficiently deliver services online, highlighting the urgency for government agencies to modernize legacy applications and infrastructure. As cities locked down, operations within many government agencies came to a standstill, creating a significant backlog and preventing citizens from getting timely access to needed services.

Some agencies found success by capitalizing on changing workplace needs to drive forward digital modernization initiatives. For others, however, old barriers continue to keep government agencies from modernizing. Outdated procurement processes, funding, staff training, cybersecurity concerns, legacy applications, and lack of a clear return on investment or comprehensive strategy create hesitation about modernization initiatives. To help agencies overcome some of these barriers, the Technology Modernization Fund (TMF) and the American Rescue Plan allocate more than $1 billion to cover the costs of modernization projects.[1] Over the past several months, the TMF board has approved seven new projects totaling over $300 million in new funding. The White House recently proposed an additional $300 million in its 2023 budget request.[2] Now is the time to address previously back-burnered modernization issues.

For modernization to be more than just a buzzword, each agency must first assess its current IT infrastructure and clearly define how to measure successful modernization activities. For some agencies, that means becoming more agile; others will strive to harness their data for actionable insights. Many agencies are modernizing because of recent cyberattacks, seeking to improve cybersecurity, restore citizens' trust in government and make it easier to do business. The needs of each agency will differ, and a single project might not achieve all goals, so having a clear vision will help prioritize modernization initiatives. Agencies need to consider what aspects of their infrastructure can be modernized concurrently and which pieces will need to be modernized sequentially. Migrating to the cloud is often a first initiative because it can support several priorities, including cybersecurity, agility and cost reduction.

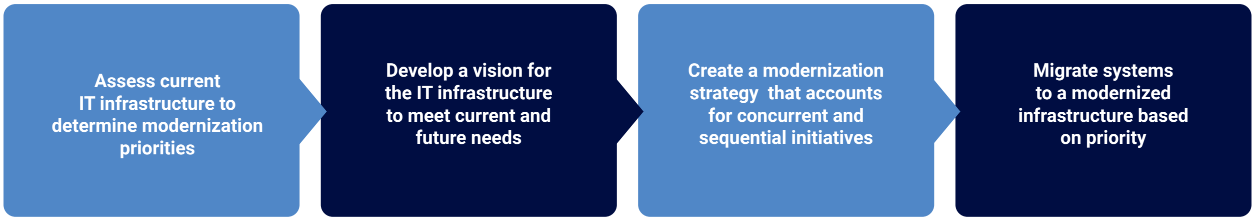
Assess current IT infrastructure to determine modernization priorities
Develop a vision for the IT infrastructure to meet current and future needs
Create a modernization strategy that accounts for concurrent and sequential initiatives
Migrate systems to a modernized infrastructure based on priority

Figure 1: Digital modernization can be broken down into manageable steps.

Increase agility and scalability by moving to secure cloud services

From the Obama Administration's 2010 announcement of Cloud First to the 2018 Trump initiative known as Cloud Smart and President Biden's Executive Order in Improving the Nation's Cybersecurity, the last three administrations have set goals for government agencies to move legacy applications to the cloud. Agencies have long known the benefits of moving workloads to the cloud, but many have been slow to embark on a cloud journey. During the pandemic, agencies running legacy on-premises systems couldn't adapt as easily as those with modern systems operating in the cloud. They couldn't rapidly pivot to meet increased citizen demands for online services. These challenges proved especially problematic for U.S. unemployment insurance systems; in many cases, the drastic increase in claims volume caused legacy systems to crash. Legacy unemployment systems couldn't monitor and log claims in real time, resulting in more than $87 billion in fraudulent claims.[1]

Achieve cloud security

It's important for agencies to adopt a proactive security approach with elements like zero trust architectures, DevSecOps processes for container scanning and a properly configured cloud access security broker tool. Ensuring information systems adhere to relevant NIST 800-53 controls based on their risk rating should be paired with continuous monitoring of the environment. These practices will ensure foundational rigor when moving workloads to the cloud while maintaining compliance to proper controls in public and/or private clouds.[3]

As agencies plan for the future, many are contemplating how to become more agile and scalable to maintain continuity. Washington Technology Solutions, the State of Washington's technology agency, realized several benefits when it transitioned a mainframe system to the cloud in 2020. The system can scale according to agencies' needs without the state having to make major new capital investments. A second site mirrors data on the cloud, providing redundancy in the event of a computer failure or natural disaster. The state also expects to see a cost savings of approximately $3 million annually.[4] While those organizations that have transitioned off the mainframe have seen success, many have only begun the journey. Of the 35 states surveyed in the recent biennial study, "A Fresh Look: Capitals in the Clouds," 89% still have a mainframe computer, and 71% haven't begun the process of moving applications off the mainframe.[5]

Once agencies determine they should move to the cloud, they need to evaluate what types of cloud models best suit their workloads and decide how to proactively address potential security and cost optimization issues. Re-hosting (also called lift and shift) is the quickest, easiest way to move existing applications into the cloud. Applications and data are redeployed like-for-like, retaining the existing source code and functionality. Lift and shift typically migrates on-premises applications to the cloud with little or no change. Re-hosting can happen quickly, with minimal disruption and planning. A lift-and-shift approach alleviates many concerns, including the need to reduce costs and increase application scalability. Often the best first step in modernization, lift and shift by no means represents a fully modernized cloud-native solution created to take full advantage of the features and functions required to meet the demands and challenges of government CIOs.

Re-architecting or re-engineering an application often involves a more advanced process of recoding some portion of an application to take advantage of cloud-native frameworks and functionality. This approach eliminates obsolete functionality or technology-specific source code while introducing architectural best practices, such as service-oriented architecture, an up-to-date security model, multi-lingual capabilities and underlying software architecture improvements that make a system easier to maintain. Although re-architecting requires the most upfront resources, it can offer the greatest cost efficiencies as agencies modify applications and infrastructure to fully leverage cloud benefits. Re-architected systems are also more adaptable to change; if needed, they can be enhanced more easily to address emerging business requirements at a lower cost and with less risk than older legacy systems.

In some cases, the decision to modernize and migrate a legacy application to the cloud may be driven by agency requirements such as improving the citizen experience or improving cybersecurity. Often, legacy monolithic applications prevent the achievement of these other priorities because the application itself can't process real-time data or effectively secure the data against modern cyberthreats.

Government agencies won't be able to modernize everything all at once. It's important for agencies to develop a cloud migration strategy and prioritize which systems to move first. They must also identify which applications can be re-hosted and which need to be re-architected. For some, there might be an interim step to re-host the application and start taking advantage of the cloud before modernizing the application. With a solid strategy, government agencies can benefit from the power and scalability of cloud computing by responding quickly to new demands for telework, scaling programs, optimizing applications and reducing costs.

Enable the productivity of a remote workforce

Prior to the pandemic, only 3% of federal employees teleworked daily, but that number jumped significantly during the peak of the pandemic when 59% of federal employees teleworked every day.[6] Agencies have the opportunity to apply lessons learned during this time to integrate telework and remote work into their strategic workforce plans. The U.S. Office of Personnel Management encourages agencies to use workplace options such as telework, remote work and flexible work schedules to support mission productivity and efficiency and to enhance employee satisfaction and wellbeing.[7]

The forced migration to remote work triggered by the pandemic has forever changed the employee experience and expectations. Goverment agencies now face the challenge of enhancing the productivity of their distributed workforce while optimizing operations and providing frictionless security. Agencies must deliver seamless and consistent user support across multiple channels and devices to give employees the flexibility they want to feel safe and engaged while maintaining the security and control the organization needs.

To meet the changing demands, agencies should develop strategies that leverage artificial intelligence (AI), collaboration, self-service, automation and analytics technologies. Agencies can augment IT services with convenient chatbots and mobile applications, offering self-service and self-help solutions that accelerate issue remediation and minimize business disruption.

This reduces friction and improves the user experience. Embracing a dynamic workplace makes government agencies more resilient during severe weather, natural disasters, public health emergencies and other disruptions.

Derive greater insights from data

Government agencies collect an incredible amount of data. Through modernization efforts, including an application programming interface-driven infrastructure, this data can be harnessed across business silos to achieve an unprecedented level of insight and then used to create programs and policies that help citizens and improve operational efficiency. However, if the data is outdated, inconsistent or incomplete, it hinders agencies' abilities to make critical decisions. Recognizing this, the Department of Justice (DOJ) launched a new initiative in 2022 to "make criminal justice data visible, digestible, actionable and transparent."[8] The DOJ released dashboards for every state that use the latest publicly available data to provide an overview of crime, incarceration, probation and post-release supervision population data and how often it's being reported, allowing officials to identify gaps in corrections reporting.

Many agencies also envision using technologies such as AI and automation to modernize their analytics capabilities. The National Technical Information Service uses AI to analyze massive amounts of data to model climate change and its effects and to develop better forecasts. As AI and associated machine learning tools improve, the level of uncertainty in these models decreases.[9]

Agencies should look holistically at their overall data governance, as well as at the data architecture of their current state. They need to capitalize on new trends within AI (specifically, machine and deep learning) to harness the power of data using pattern matching and classification. This helps better predict outcomes while also helping employees focus on actions versus analysis. Agencies that transform information into actionable intelligence make informed business decisions through predictive analytics. They can analyze massive data volumes and less structured forms of information to gain a greater understanding of their operations and impacts. Federal agencies can use continued innovations in data analysis, AI and automation to streamline operations while enhancing employee and citizen experiences.

Design interfaces with users at the forefront

According to Forrester's 2021 U.S. Federal Customer Experience Index, federal agencies' average score of 62.6 out of 100 still lags 10.7 points behind the private sector average, and the quality of federal customer experience varies widely for different demographic groups.[10] With experiences and interactions in the commercial environment now driving citizen and employee expectations, many agencies recognize the need to modernize systems to provide intuitive service delivery.

On December 13, 2021, President Biden issued the Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government, further amplifying the call to modernize systems and applications throughout government. The Executive Order tasks federal agencies with transforming service delivery to ensure citizens of all abilities can quickly, easily and conveniently access the services they need.[11]

An intuitive user experience can be the difference between effective dissemination of information and frustration and confusion. Improving the user experience of a website or application can involve visually redesigning the layout, improving accessibility, creating more interactive elements, and adding dashboarding and reporting tools. By introducing self-

> "In recent years, the annual paperwork burden imposed by executive departments and agencies (agencies) on the public has been in excess of 9 billion hours. That number is too high. Agencies must work with the Congress; the private sector and nonprofit organizations; State, local, Tribal and territorial governments; and other partners to design experiences with the Federal Government that effectively reduce administrative burdens, simplify both public-facing and internal processes to improve efficiency, and empower the Federal workforce to solve problems."[11]
>
> — Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government

service and omnichannel solutions, agencies will be able to not only improve efficiency but also save money. A good, immersive experience is built on a foundation of understanding citizens' needs and delivering consistently across channels and touchpoints.

In 2020, the National Institute of Allergy and Infectious Diseases (NIAID) worked with NTT DATA to apply human-centric design best practices to the design and development of the Vaccine Adjuvant Compendium (VAC). The VAC website provides an intuitive and searchable online database of vaccine adjuvants defined through the adjuvant studies NIAID supports. The public database helps foster collaborations between the adjuvant researchers who NIAID supports and the broader scientific community.[12]

Develop a comprehensive cybersecurity strategy

The digital shift to telework, coupled with aging systems and infrastructure, magnified threats and increased the need for security. Over the course of the pandemic, many agencies have grappled with sophisticated cyberattacks. In January 2022, Albuquerque Public Schools canceled classes for around 75,000 students due to a cyberattack. Four other school districts in New Mexico also suffered cyberattacks over the past two years.[13] Many agencies operate on legacy technology, making them more vulnerable to cyberattacks, and cybersecurity solutions designed for the threats of the past may not protect against current and future risks. For this reason, agencies have resolved to improve their cybersecurity posture and build cybersecurity into modernization initiatives.

To reduce the vulnerabilities in federal agencies, President Biden signed the Executive Order on Improving the Nation's Cybersecurity in May 2021. It requires federal agencies to modernize and implement more substantial cybersecurity standards, such as implementing a zero trust architecture. The executive order also expedites the federal government's adoption of secure cloud services, including software-as-a-service, platform-as-a-service and infrastructure-as-a-service capabilities.[14]

On January 19, 2022, President Biden issued a Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems that builds on the requirements established in the cybersecurity executive order. The memorandum sets new deadlines for defense and intelligence agencies to comply with cybersecurity requirements. Within 60 days of the memorandum, each agency that owns or operates a National Security System (NSS) must update existing agency plans to prioritize resources for cloud technology adoption and use and develop a plan to implement zero trust architecture. Agencies were given 90 days to develop a strategy for coordinating on cybersecurity incident response. Additionally, they have 180 days to implement multifactor authentication and encryption for NSS data.[15]

> "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises or hybrid. The scope of protection and security must include systems that process data (information technology) and those that run the vital machinery that ensures our safety (operational technology)."[14]
>
> — Executive Order on Improving the Nation's Cybersecurity

Both the executive order and the memorandum emphasize the urgency for agencies to modernize their IT systems to ensure cybersecurity. To reach the established objectives, agencies need to consider multiple variables when developing a comprehensive cybersecurity strategy. The percentage of remote workers, use of cloud apps and volume of sensitive or classified data must be taken into account. Securing systems through zero trust mindsets, DevSecOps, automated security controls and compliance, and advanced data and cloud security form the foundation of protection solutions. Using these modern approaches will help agencies simplify IT management and better protect their remote workforce and their data.

Conclusion

The benefits of modernization are known, and there's a pressing need for agencies to modernize. It's vital that agencies implement the latest cybersecurity measures and become more agile so they can meet changing citizen demands. Although each agency may have different modernization goals, many sources of funding are available to aid agencies in a variety of modernization initiatives. Now is the time to begin modernizing.

Like eating the proverbial elephant, modernization initiatives can be enormous undertakings. Agencies should reach out to a trusted IT partner for support. Partners with extensive experience in helping government agencies modernize their legacy infrastructure will be able to provide guidance on which initiatives to prioritize first and support the implementation of these initiatives. With a clear vision and a list of priorities, agencies can manage massive modernization initiatives one bite at a time.

About the authors

Noel Hara, Chief Technology Officer, Public Sector, NTT DATA

Noel is an experienced strategist who infuses technology solutions across the public sector to help solve the most challenging problems. As Chief Technology Officer of NTT DATA's public sector, he blends over two decades of experience in the public and private sector with an insatiable curiosity for technology and applications. Since the start of the global pandemic, Noel has been responsible for adapting the company's offering portfolio to support clients in their shift to remote working and learning while continuing to support citizens through the expansion of digital government.

Hannah Noah, Marketing Senior Analyst, Public Sector, NTT DATA

Hannah has experience supporting federal civilian agencies including the Department of Commerce, Department of Health and Human Services, Millennium Challenge Corporation, U.S. Agency for International Development and U.S. Trade and Development Agency. In her role at NTT DATA, she helps develop marketing and communications materials to support the Federal Health and Civilian team. Her marketing experience analyzing and writing for the healthcare, renewable energy and IT industries gives her a unique perspective on the challenges faced by public sector agencies.

Sources

1. Noel Hara. "5 Resolutions for a Happier New Year for Government CIOs." NTT DATA. January 6, 2022. https://us.nttdata.com/en/blog/2022/january/resolutions-for-government-cios#.Ye69HEy0K2N.linkedin

2. Tara Franzonello. "How to help agencies fund critical IT modernization projects." Washington Technology. January 21, 2022. https://www.washingtontechnology.com/opinion/2022/01/how-help-agencies-fund-critical-it-modernization-projects/361033/

3. "The Journey From Cloud First to Cloud Smart." NTT DATA. 2020. https://us.nttdata.com/en/-/media/assets/reports/federal_the-journey-from-cloud-first-to-cloud-smart-final.pdf

4. Bill Lucia. "A State Moves Its Mainframe System to the Cloud." Route Fifty. October 23, 2020. https://www.route-fifty.com/tech-data/2020/10/washington-state-transitions-mainframe-to-cloud-service/169532/

5. Phil Goldstein. "State Governments Face Hurdles on Cloud Migration, Letting Go of Mainframes." State Tech. November 17, 2021. https://statetechmagazine.com/article/2021/11/state-governments-face-hurdles-cloud-migration-letting-go-mainframes

6. "Government Wide Management Report." United States Office of Personnel Management. 2020. https://www.opm.gov/fevs/reports/governmentwide-reports/governmentwide-management-report/governmentwide-report/2020/2020-governmentwide-management-report.pdf

7. "2021 Guide to Telework and Remote Work in the Federal Government Leveraging Telework and Remote Work in the Federal Government to Better Meet Our Human Capital Needs and Improve Mission Delivery." United States Office of Personnel Management. November 2020. https://chcoc.gov/sites/default/files/Telework-Guide-2021_0.pdf

8. Shourjya Mookerjee. "Better data for improved criminal justice." GCN. January 28, 2022. https://gcn.com/data-analytics/2022/01/better-data-improved-criminal-justice/361344/

9. Patience Wait. "Using AI, ML Will Help the Government Tackle Climate Change, Experts Say." Nextgov. January 28, 2022. https://www.nextgov.com/cio-briefing/2022/01/using-ai-ml-will-help-government-tackle-climate-change-experts-say/361317/

10. Frank Konkel. "Federal Agencies Achieve Highest Customer Experience Scores Yet." Nextgov. December 16, 2021. https://www.nextgov.com/cio-briefing/2021/12/federal-agencies-achieve-highest-customer-experience-scores-yet/359898/

11. "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." The White House Briefing Room. December 13, 2021. 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/

12. The National Institutes of Health and National Institute of Allergy and Infectious Diseases. "Vaccine Adjuvant Compendium." https://vac.niaid.nih.gov/

13. "A cyberattack in Albuquerque forces schools to cancel classes." NPR. January 14, 2022. https://www.npr.org/2022/01/14/1072970219/cyber-attack-in-albuquerque-latest-to-target-public-schools

14. "Executive Order on Improving the Nation's Cybersecurity." The White House Briefing Room. May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

15. "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." The White House Briefing Room. January 19, 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

Visit **nttdataservices.com** to learn more.

NTT DATA Services is a recognized leader in IT and business services headquartered in Texas. A global division of NTT DATA — a part of NTT Group — we use consulting and deep industry expertise to help clients accelerate and sustain value throughout their digital journeys.

NTT DATA
Trusted Global Innovator