NTT DATA Services

POINT OF VIEW | PUBLIC SECTOR

Reigniting Modernization

Why modernizing government is an imperative, not a choice

MARCH 2019

NTT DATA

> 70% of government agencies' major IT spend goes to operating and maintaining legacy systems.[4]

Modernization in government hasn't been without its challenges. Agency chief information officers (CIOs) work hard to balance the mounting technical debt and lack of cost transparency while trying to make sense of the emerging technology landscape. Today's CIOs ultimately have to balance priorities, using limited budgets and resources — effectively doing more with less.

When looking at the current state of the federal IT landscape, 28 federal IT systems are at least 25 years old, and 11 are 35 (or more) years old. In 2018, the IRS' most important system — the 60-year-old Individual Master File — went down on Tax Day, affecting most of the agency's public apps and prompting the acting commissioner to extend tax season an additional day.[1] The system is in dire need of an upgrade. Veterans Affairs has spent close to $2 billion over the last 10 years trying to implement an electronic health records system only to scrap past efforts.[2] The Census Bureau is having trouble getting its new technology programs ready for the 2020 decennial count.[3] And these are just a few examples of the challenges currently impacting federal agencies.

These examples are a symptom of agencies experiencing enormous disruption from the surge in the complexity of the IT landscape and huge technical debt. Old systems of record must coexist with new systems of engagement and process unexpected formats, sizes and sources of data. Information exchange has progressed beyond the web and intranets; many transactions occur on mobile devices and/or in the cloud. Employees, partners and citizens demand more and better ways to engage with the government. The latest entrant to this complex mix is the internet of things (IoT), which is becoming a prominent channel for information exchange, business intelligence and citizen engagement. Additionally, more information is being exchanged via open application programming interfaces (APIs). This "API-ification" of enterprise IT is leading to new, largely unanswered questions for enterprise-wide strategy, rationalization and standardization.

Public expectations are changing faster than ever. We're now amid the Fourth Industrial Revolution — Digitalization. With this comes various geopolitical, societal, economic and technological shifts. Experiences and interactions in the commercial environment now drive citizen and employee expectations — due to companies such as Uber, Airbnb, Venmo and Amazon. As millennials become the dominant consumer of government services, influencing the sociopolitical landscape, economics and technology innovations, government needs to up its game to meet the expectations of a more sophisticated and informed user. A shift is happening.

On December 12, 2017, President Donald Trump signed the Modernizing Government Technology (MGT) Act into the last part of the 2018 National Defense Authorization Act. The law creates working capital funds for IT projects for federal agencies and a central modernization fund housed by the General Services Administration. Key themes include:

- Upgrading legacy systems
- Moving to cloud email
- Emphasizing shared services
- Using artificial intelligence (AI) to detect malicious activity across networks

Under the MGT Act, when an agency upgrades its technology infrastructure and saves money, those savings can be used to fund future projects.

> **"Our goal is to lead a sweeping transformation of the federal government's technology that will deliver dramatically better services for citizens. Government needs to catch up with the technology revolution."[7]**
>
> **—President Donald Trump, speaking with the American Technology Council, June 2017**

There's a viable need to create greater transparency and more citizen-centric services. Citizens are demanding the delivery of information anywhere, anytime and on any platform or device. The need to modernize government spans the aisle, crossing political parties as a critical objective.

Modernization isn't a choice, it's a necessity. According to Teo Chee Hean, Deputy Prime Minister of Singapore, "The emergence of new Infocom technologies calls for fundamental rethinking and transformational shifts in the way we look at egovernment. Governments must take on the roles of a facilitator and enabler — to collaborate with the public, private and people sectors in creating new solutions, new businesses and new wealth."[6]

Planning for a new wave of modernization

Governments need to change, evolve and embrace inevitable shifts or continue to face budget challenges and low citizen satisfaction scores. To effectively shift, government agencies need to take a fresh and holistic approach to planning. However, is the public sector ready to embrace and institutionalize emerging technologies into its existing enterprise blueprints — not only in silos but also through a well-thought-out strategy that brings together a confluence of key emerging trends in a creative and meaningful way? To do so, governments need to capitalize on the moment now to reignite modernization.

For maximum effectiveness, and using a phased and carefully planned approach, this new wave of modernization should focus on six key areas — customer experience, data and intelligence, intelligent automation, IoT, cybersecurity and IT optimization.

> **"I want us to ask ourselves every day, how are we using technology to make a real difference in people's lives."[5]**
>
> **—Former President Barack Obama, Digital Government Strategy Initiative**

Data & Intelligence

Whether protecting the homeland or predicting the possibility and magnitude of a crime in a "smart city," public sector agencies have an opportunity to harness the massive amounts of data at their disposal to create an unprecedented level of insight. A growing amount of data and digital knowledge now fuels innovative use cases across government agencies. Treating data as a strategic asset and securing it with the same rigor, will be key to an agency's ability to grow. Agencies need to take advantage of 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 humans focus on actions versus analysis. But before embarking on these tasks, federal agencies should look holistically at their overall data governance, as well as at the data architecture of their current state. Agencies need to understand where they are to effectively transition toward, or embrace, the emerging technology areas for maximum benefit. It's also important to look at data and intelligence in the context of the other key focus areas.

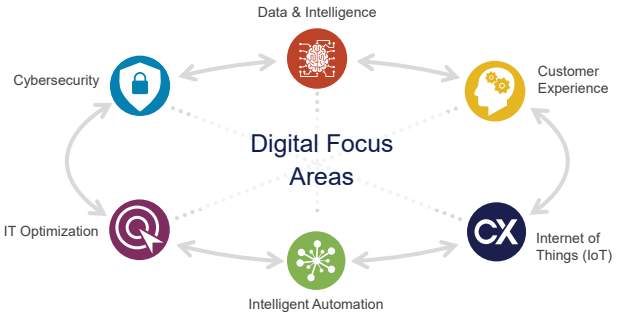

Figure 1: Modernization initiatives should focus on six key areas

Intelligent Automation

Closely related to data and intelligence, automation should consider all other focus areas before executing a strategy. Effective automation quickly consumes relevant data, efficiently finds patterns and matches those patterns to automation models, such as autonomics, robotic process automation (RPA) and virtual cognitive agents. Like private sector organizations, government agencies need to evaluate automation strategies across both IT end-user services, such as the service desk, field services, IT asset management and infrastructure monitoring, and the corresponding domain-centric business processes. Government agencies also need to identify and document business processes to create the operational efficiencies that automation tools can provide. The other key challenges to overcome include the need to rationalize infrastructure and applications, remove redundancies (through application rationalization initiatives), and simplify processes and technology landscapes to take advantage of automation. For example, capturing and monitoring events to eliminate duplication, suppressing false positives and invoking self-healing activities. For both data center and end-user services, devices should be commissioned, managed and decommissioned across compute platforms in an autonomous way. Automation isn't just about savings, it also has a direct impact on the citizen experience.

Customer Experience

For agencies to execute their missions successfully, they must engage the customers they serve — citizens. Many argue that public sector agencies don't need to create engaging experiences, because they don't compete with other companies and aren't out to make a profit. But through the sustained engagement of citizens, agencies can create a successful customer experience. By introducing self-service and omnichannel solutions, agencies will be able to not only improve efficiency but also save taxpayer money. A good, immersive experience is built on a foundation of understanding citizens' needs and delivering consistently across channels and touchpoints. And the experience must be emotionally engaging.

Government plays a role in our daily lives. Now more than ever, the services delivered need to be transparent, easy to use, engaging and extremely relevant. Each customer experience should combine form (desirability), fit (relevance) and function (usability), as these three elements are critical to engaging the citizenry. A beautiful site or application can be useful, but if it's not relevant, citizens will lose interest very quickly. On the other hand, if the site or application is conceptually very good but not at all functional, the experience is over in one click.

Internet of Things

From millions of users to billions of devices, IoT is moving toward the internet of everything (IoE). While the first wave of the internet mainly connected people with each other, the next wave of the internet connects devices and more. By increasing computing capabilities, government services and operations can become more intelligent, moving from simple automation to full autonomy where applicable. Government agencies should consider the following technologies as part of any IoT initiatives:

- Sensors (temp, proximity, image, light)
- Near-field communication (NFC) and radio frequency identification (RFID)
- Low power networks
- Event stream or signal processing
- Device-level cybersecurity

61% of federal IT officials said the government's aging IT infrastructure impedes its ability to comply with federal cybersecurity mandates.[8]

For government agencies, IoT also adds a new (and complex) layer of challenges around scalability, privacy and security. It's imperative that IoT planning considers the impact and integration of each focus area — especially cybersecurity.

IT Optimization

Government agencies continue to look at optimizing their IT landscape, but they also need to think about strategies that enable rapid responses to marketplace dynamics while balancing cost and risks — ensuring the effective allocation of taxpayer money. Agencies are considering a move to multi-cloud/hybrid-cloud environments. This next phase of modernization will require this paradigm in conjunction with on-demand, workload-centric provisioning, supported by microservices architectures in a DevOps environment with some carefully planned services-based architecture and orchestration strategy.

Cybersecurity

Government agencies and commercial organizations alike need to address compounding problems related to data breaches, phishing, ransomware and hacks by securing their perimeters, which many have started to do. More important, they must secure the data, which is the real treasure. Hackers and others intent on causing harm want to obtain data to sell, hold for ransom and manipulate. Agencies need a holistic assessment of their cybersecurity posture.

Cybersecurity can't be an afterthought. Assess all architecture layers to ensure appropriate controls are in place as applicable. Data-level security is paramount, and all data needs to be protected with more urgency. Agencies should go a step further and track real-time user behavior analytics and pervasive AI to learn threat and risk behavior patterns and to optimize outputs and alerts accordingly. Appropriate data protection can address most, if not all, of today's hacks and breaches.

Another critical success factor in an agency's overall security posture is a carefully thought out, robust, federated identity management program that crosses operational divisions. When planning and modernizing, agencies need to combine that program with a more granular, attribute-based access management strategy, and then tie both into previous stages — for example, having a good understanding of the data, data flow, data ownership and control, and appropriate levels of security based on automation levels and strategies. Government agencies need to go a step further and adopt, and even strengthen, biometrics-based access, establish real-time risk monitoring and threat remediation techniques, and find appropriate and effective uses of emerging distributed-ledger technology (blockchain) in a private/permissioned model.

Key focus areas in action

The confluence and intelligent combination (as applicable) of these six focus areas is really what will reignite the next wave of modernization in government and move it away from the many silos that decades of technological layers have added to IT organizations.

Some examples of where the confluence of these six focus areas have seen positive results (albeit in early stages) include:

- Adoption of agile development and DevOps, which has increased the speed of delivery of new applications and enhancements at agencies, such as the U.S. Citizenship and Immigration Services and the Patent and Trademark Office.
- Adoption of advanced analytics solutions, which provides higher value use of an agency's information in delivering new and more efficient IT services, like reducing fraud at the Social Security Administration.
- Adoption of cloud solutions, both for commodity services such as email and for specialized hosting and shared services, which is reducing the capital investment requirements of the involved agencies, such as at the Federal Communications Commission. As of 2017, half of state and local agencies had integrated cloud into their strategies due to the benefits of cloud-driven IT modernization, such as regular upgrades, mobility for caseworkers and citizens, and easier to use services.
- Adoption of modern mobile applications at the Transportation Security Administration, which enables a more efficient travel experience.

Conclusion

Modernizing government is no longer a choice, it's an imperative. The challenges are daunting and many, but soon the risks of not modernizing will cripple many aspects of our government. Modernizing requires careful planning, because many legacy systems must be kept operational as new systems are put into service. At the same time, the government and its agencies must carefully consider new and future technologies to ensure systems meet the needs of the citizenry now and well into the future.

About the author

Shamlan Siddiqi, Chief Technology Officer, Public Sector, NTT DATA

Shamlan is a results-oriented leader with an extensive track record developing and leading the implementation of innovative solutions and strategies, and building and motivating high-performance teams. Previously, Shamlan successfully led the Digital Experience practice in both top-line and bottom-line growth year over year and against the annual operations plan. He is a published author and accomplished speaker, and he holds a master's degree from George Washington University.

Let's get started

NTT DATA Services makes modernization painless by:

- Applying in-depth commercial experience to government solutions
- Investing in innovation for forward-reaching solutions
- Partnering with industry-leading experts to help you build and realize your mission

Contact Shamlan Siddiqi or visit our website to discover your future enterprise with NTT DATA.

Sources

1. Aaron Boyd and Frank Konkel. “IRS’ 60-Year-Old IT System Failed on Tax Day Due to New Hardware.” Nextgov. April 19, 2018. https://www.nextgov.com/it-modernization/2018/04/irs-60-year-old-it-system-failed-tax-day-due-new-hardware/147598/
2. Alice Lipowicz. “DOD unhappy with electronic records upgrade.” Defense Systems. October 6, 2010. https://defensesystems.com/articles/2010/10/06/defense-dod-ahlta-ehr-electronic-health-record.aspx
3. U.S. Government Accountability Office. “2020 Decennial Census.” https://www.gao.gov/highrisk/2020_decennial_census/why_did_study#t=1
4. Ben Berliner. “Legacy systems O&M still dominates FY17 IT spending.” FCW. June 9, 2017. https://fcw.com/articles/2017/06/09/snapshot-it-spend-berliner.aspx
5. President Barack Obama. Digital Government Strategy Initiative. https://open.obamawhitehouse.archives.gov/
6. Teo Chee Hean, Deputy Prime Minister of Singapore. “The Future of e-Government - The Singapore Perspective.” Information Policy. June 29, 2011. https://www.i-policy.org/2011/06/the-future-of-e-government-the-singapore-perspective.html
7. David Shepardson. “Tech CEOs meet with Trump on government overhaul.” Reuters. June 19, 2017. https://it.reuters.com/article/companyNews/idUKKBN19A16I?symbol=FB.O
8. Morgan Chalfant. “Nearly half of federal IT managers report breach in last six months: research.” The Hill. May 3, 2017. https://thehill.com/policy/cybersecurity/331815-nearly-half-of-federal-it-managers-report-breach-in-last-six-months

Visit nttdataservices.com to learn more.

NTT DATA Services partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. As a division of NTT DATA Corporation, a top 10 global IT services and consulting provider, we wrap deep industry expertise around a comprehensive portfolio of infrastructure, applications and business process services.

NTT DATA
Trusted Global Innovator