The Future of Federal IT Modernization and Digital Transformation

Starting in 2021, the President-elect Biden Administration (hereafter “Administration”) and 117th Congress (hereafter “Congress”) will have an unprecedented opportunity to make transformational change in Federal technology and cybersecurity operations, governance, and performance. As the government continues its shift towards a more prevalent digital culture and modern workflows (which the onset of COVID-19 dramatically accelerated), the time will be especially ripe to make long overdue and important changes to law and policy that can better equip agencies to harness commercial innovation, embrace new technology capabilities, improve digital service delivery for citizens, and ensure smarter and more effective spending for IT and cybersecurity outcomes.

The Alliance for Digital Innovation (ADI) believes that government exists to competently and capably serve its citizens – and that technology is a key driver behind this relationship. But, too often government has been beholden to outdated ways of thinking, afraid of embracing change, and too accepting of wasteful processes and policies that effectively enrich incumbents at the expense of the American taxpayer. ADI is laser-focused on abolishing the cult of legacy: legacy systems, legacy processes, and legacy mindsets.

ADI exists to accelerate change by driving government’s adoption of innovative commercial technology to empower the mission and ensuring that the public sector more effectively buys and uses technology as a catalyst to improve the lives of the American people. We believe that government’s continuing reliance on outdated, insecure legacy technology fundamentally obstructs creation of a modern, secure digital government capable of delivering critically needed services to the American taxpayer.

To this end, ADI has developed a set of legislative and policy proposals that we believe can unite both parties and both the Legislative and Executive branches of government. These efforts will empower Federal agencies to thoughtfully and effectively leverage innovative commercial technology and cybersecurity capabilities, reduce wasteful spending on outdated technology and infrastructure, and ensure today’s government builds a robust, yet agile, foundation for long term digital transformation.
ADI’s recommendations fall into three key pillars that, working together, will unlock and accelerate IT modernization, increase the ability of the government to harness innovative technology solutions, improve collaboration and coordination among a more highly skilled workforce, and ensure that Federal agencies remain resilient and secure. Our key pillars and recommendations are:

**Pillar 1: Fix the Way the Government Acquires and Uses Technology Solutions**

1. Reform and Rewrite a New Legislative Foundation for Federal IT
2. Adopt Enterprise-wide Commercial Capabilities
3. Expand Innovative Acquisition Authorities
4. Address Outdated Funding Models for IT Projects

**Pillar 2: Secure Federal Networks, Data, and Information**

1. Scale Secure Telework
2. Update FISMA
3. Move from Check-the-Box Compliance to Risk-Based Decision Making

**Pillar 3: Create a Strong Foundation for the Future of IT Modernization**

1. Modernize Federal Technology Service Delivery
2. Empower the Federal Technology Workforce
3. Improve Performance of Federal IT Spending

Our recommendations for the Administration and Congress are both practical and powerful. These common sense, bipartisan priorities can dramatically accelerate IT modernization, enabling the government to more effectively, securely deliver the high-quality, high impact digital services that citizens deserve.
Pillar 1: Fix the Way the Government Acquires and Uses Technology Solutions

1. **Reform and Rewrite a New Legislative Foundation for Federal IT.** The Federal government’s response to the COVID-19 pandemic has shown what is possible when exigent circumstances arise and immediate challenges require innovative thinking and new technology operating models. Going forward, agencies should build on the bright spots that have surfaced during this difficult time and powerfully embrace disruption in all aspects of the technology, security, and IT acquisition. To ensure this change is lasting, the 117th Congress should pursue legislation that would repeal numerous outdated Federal IT laws (such as Clinger-Cohen and the E-Government Act of 2002) and in their place create a new, comprehensive foundation for Federal IT operations, management, acquisition, and oversight. Such IT reform legislation should address several key areas:

   a. Creating new authorities to enhance and support the ability of agencies to pilot, scale, and acquire new and emerging commercial capabilities to meet mission outcomes by repealing outdated paradigms that lead to costly, wasteful IT projects and unsupportable legacy maintenance tails;

   b. Providing a new, modern IT budgeting, acquisition, and appropriations framework to ensure greater accountability for IT spending within and across agencies, and to provide agencies greater flexibility in their IT funding to facilitate more modern, agile acquisitions;

   c. Updating existing IT policies by reforming the authorities of the Office of Management and Budget (OMB) for technology policy, oversight, funding, and performance;

   d. Codifying the roles of the CIO Council and formalizing the responsibilities of Agency Chief Information Officers (CIOs), Chief Technology Officers (CTOs), Chief Data Officers (CDOs), and Chief Information Security Officers (CISOs) to provide more clarity around those key functions and how they support an agency’s overall technology, data, IT, and cybersecurity priorities; and

   e. Updating critical privacy, information management, and digital service delivery authorities to ensure agencies are focused and able to effectively support improved service delivery to agency customers and citizens, rather than remaining beholden to formulaic and outdated technology management and governance processes.

2. **Adopt Enterprise-wide Commercial Capabilities.** As part of the continued COVID-19 response and recovery efforts, the Administration should make significant investments in promising applications of emerging commercial technology to build on the successes in IT modernization over the previous year. The workplace of the future has been irrevocably altered by the pandemic, highlighting government’s need to establish sustainable, remote collaboration. Enhanced use of artificial intelligence, machine learning, robotic process automation, and other cutting-edge capabilities can spur innovation and improve service delivery outcomes within and across agencies. Both government and industry have identified numerous examples where new capabilities or innovative IT services have enabled agencies to function more effectively and improve the delivery of digital services to citizens.

   Now is the time to develop and support a comprehensive plan to scale those solutions, fund them appropriately, and maximize the impact of these critical investments. The White House and OMB should immediately develop a coordinated, government-wide strategy for how agencies can fund and acquire these key capabilities and showcase how these new technologies can spur greater interoperability and collaboration across the Federal enterprise. Such a plan will involve...
a dramatic shift away from individual agency (and sub-agency) risk management frameworks and move the Executive Branch towards a more automated, repeatable, reciprocal process to authorize new systems and software for faster adoption within and across agencies. OMB should consider changes to Circular A-130, updating the 10-year old guidance on how agencies adopt secure cloud authorizations under the Federal Risk Authorization Management Program (FedRAMP), and enforce stronger reliance on continuous monitoring to improve both the speed and security of these new capabilities and ensure important capabilities get into the hands of mission owners quickly and securely.

In addition, Congress and the Administration should explore a path forward to true adoption and sufficient resourcing of commercial shared services. Improving the way all Federal agencies manage common processes (such as financial management, grants management, human resources management, etc.) starts with centralizing the expertise and authority to centrally oversee and manage these functions, including identifying robust and effective market solutions that agencies can adopt. Importantly, Congress must be willing to support any robust, actionable Administration plan to comprehensively deploy shared services by providing sufficient resources and direction – both to those lead agencies that will help standardize solution sets for government-wide adoption and to customer agencies that will need to move away from legacy providers and adopt modern commercial capabilities.

3. **Expand Innovative Acquisition Authorities.** It is vital that the Administration support the consistent training and upskilling of the Federal acquisition workforce to ensure they understand and can leverage agile acquisition authorities to more effectively pilot and scale commercial innovation within their agencies. In addition, agencies should leverage key government-wide playbooks such as the 18F Guide to De-Risking Government Technology Projects and the Digital Services Playbook to better define, scope, and acquire technology products and services in a modern, effective manner.

Agencies should continue leveraging existing authorities such as Other Transaction Authorities (OTAs) and Commercial Solutions Offerings (CSOs) – and Congress should consider an expansion of these rapid acquisition authorities to additional agencies. ADI has already developed a proposal called RAPIT (Rapid Acquisition Procedures for IT) that would provide for OTAs and CSOs at all civilian agencies. The proposal would provide for necessary pilots, reporting, and oversight – but also encourage agencies to scale such programs if administered wisely and showcasing promising results.

Procurement must keep pace with the speed of innovation happening in the private sector. Without robust, timely insights into the dynamic changes in the commercial technology, the government risks always buying yesterday’s solutions for today’s challenges. Therefore, the Administration should work to update and reform the ways in which agencies access and understand developments in the market research portion of their acquisition process. Additionally, OMB should pursue policy changes that push agencies to adopt a commercial-first framework for technology procurements, eschewing the outdated and cumbersome requirements approach still too common across agency acquisitions.
4. **Address Outdated Funding Models for IT Projects.** Critical technology projects, including those that seeks to replace legacy systems and processes with newer, modern capabilities, simply do not align well with traditional budget cycles. Even the most creative and well-executed plans struggle unduly because of inconsistent appropriations processes. To drive true digital transformation, agencies need multi-year or no-year dollars.

The model adopted within the Technology Modernization Fund (TMF), which provides no year dollars, agile acquisitions, and constant oversight and project management able to identify new challenges or embrace new opportunities, creates a virtuous cycle. The Administration’s first budget should support, and Congress should provide, the full $3 billion dollars originally requested for the TMF.

Beyond the TMF, it is past time that agency CIOs have more budgetary and project management control over their agency’s entire IT portfolio. These leaders should also be able to, carefully and with sufficient oversight, fund and acquire new and emerging IT solutions without fear of subverting current appropriations law. Congress should provide agencies with the authorities necessary to establish IT Working Capital Funds (as envisioned under the Modernizing Government Technology Act) and, absent legislative action, OMB should work with agencies to implement the TMF model within existing agency working capital funds or other multi-year funds, and help centralize agency IT projects under CIOs, to enhance the effectiveness and outcomes of IT dollars.

---

**Pillar 2: Secure Federal Networks, Data, and Information**

1. **Scale Secure Telework.** The government’s comprehensive and overwhelming response to the COVID-19 pandemic, especially the shift to nearly total telework and remote collaboration, highlighted numerous challenges and opportunities for agencies as they continue this “new normal” operating model. Even when the threat of the virus recedes, it is likely that government agencies will retain a significant telework posture for the foreseeable future. Now is the time to build a robust, secure, and collaborative operating environment for agencies that empowers the workforce and enhances collaboration and mission outcomes in a distributed environment.

Within the first 100 days, the Administration should develop a robust telework strategy that enables agencies and their workforces to safely and securely perform their mission responsibilities. As such, it is imperative that both industry and government work collaboratively together to build a secure telework ecosystem that supports the technology and cybersecurity capabilities necessary for agencies to deliver vital programs and services, keep the workforce safe, and ensure agencies operate in state-of-the-art environments that rely on sophisticated digital workflows and commercial tools that support the mission. The plan should also enable agencies to manage their data assets and identity credentialing and access capabilities in modern, distributed operating models. It should also provide innovative solutions for those agencies that handle vital national security portfolios to share and collaborate on classified and sensitive information without – potentially – having to be physically located in a secure government facility.

The future of Federal “work” will continue to be distributed – the previous assumptions have changed for good. The Administration can embrace the future by moving away from network-centric models of infrastructure and security to zero trust paradigms and software-defined networking will reinforce and propel these recent shifts to remote operations and ensure that the government can safely and ably perform its mission in a decentralized, but networked, world.
2. **Update FISMA.** The *Federal Information Security Modernization Act* (FISMA) was passed in 2014 to improve Federal cybersecurity. Unfortunately, FISMA has devolved into a check-box compliance regime for agencies fueled by overlapping and duplicative directions from OMB and the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security (DHS), manual and onerous reporting requirements, and uneven implementation that frustrates both agencies and industry.

Updating the way agencies are held responsible for risk management, overhauling the burdensome and formulaic cybersecurity audit cycle, and further refining the roles and responsibilities of OMB, DHS, the National Institute of Standards and Technology (NIST), and Federal agencies with respect to cybersecurity policy, budgeting, and program implementation is a critical priority. Congress should craft FISMA reform legislation that focuses on driving smarter, data-driven cybersecurity improvements within and across agencies, increasing the operational leadership of CISA to protect Federal networks, and empowering agencies to modernize their IT systems, network architectures, and cybersecurity policies to reduce complexity and enhance their awareness and ability to respond to emerging threats.

Additionally, any FISMA reforms should also enhance and expand the authorities of Federal agencies to recruit, compensate, retrain, and train the cybersecurity workforce. These reforms should extend beyond the traditional “security engineer” or “information security specialist” position descriptions normally associated with Federal cybersecurity roles and encompass other skill sets with are necessary to ensure effective technology delivery and information security roles, such as program management, acquisition, and IT governance.

3. **Move from Check-the-Box Compliance to Risk-Based Decision Making.** The current budget processes and models used by the Federal government are vestiges of a previous age – they simply focusing on “cost, schedule, and performance” for IT investment oversight. This outdated way of managing IT has been, for quite some time, woefully inadequate. No modern commercial enterprise reports on spending by “investments” – they have smarter, more relevant categories of spending and performance aligned to the mission and objective of the organization. The government can and should do better. It is time to eliminate the decades-old capital planning and investment control spending model.

As an immediate priority, the Administration should direct OMB to better align their technology oversight regime to identify relevant spending categories and data elements across agency enterprises and cross-reference that data against agency appropriations. Today’s capital planning and investment control IT spending model is irrelevant and the Administration should pursue new, useful data-driven IT spending paradigms that can effectively tie agency appropriations to key spending activities – and, most importantly, to performance and outcomes. In addition, OMB should further develop and implement a robust cybersecurity risk management model that highlights the numerous risks faced by agencies, and ensures cybersecurity spending addresses the most pressing risks. These processes should enable greater visibility and analysis of IT and cybersecurity spending by Congress, OMB, and agency CIOs and CISOs – the latter of which should be given increased authority and accountability for these classes of spend and be empowered to make informed, risk-based decisions.
Lastly, any pertinent improvements to risk-based budgeting and decision making will have to support agency efforts to secure American supply chains. While both industry and government agree that improving supply chain resiliency is a critical national security imperative, too often these efforts have been dispersed and poorly coordinated. The Administration should consider working under existing legislative and interagency authorities to develop a “smart supply chain” plan that centralizes and increases coordination across the various supply chain and risk management agencies to help government and industry deter the threats from nefarious nation-state actors, secure vital government data and information, and protect the valuable intellectual property of our nation’s leading companies.

**Pillar 3: Create a Strong Foundation for the Future of IT Modernization**

1. **Modernize Federal Technology Service Delivery.** While much effort has gone into, and some unqualified successes have come from, the establishment of entities such as the U.S. Digital Service, the Presidential Innovation Fellows, and GSA’s Technology Transformation Services, there is still far too much confusion and far too little understanding of why these offices exist, how they do (or do not) coordinate to support government-wide modernization efforts, or how they partner successfully with industry to drive digital service delivery and improve outcomes in agencies. These offices have been a force for good in Federal technology over the past several years and a new Administration would benefit from the development of a comprehensive assessment of these groups – and use their evaluation to reorganize these digital service teams to deliver long-term, sustainable successes into the future.

The Administration and Congress should work together on a large-scale reimaging of these Federal technology delivery units that would seek to centralize and elevate programs that combine the top technology, product, and acquisition experts that can support both individual agency and enterprise-wide modernization efforts. Rather than the recent exercises in creating one-off offices or independent programs within agencies that seek to address pieces of this puzzle, the Administration should develop a comprehensive reorganization plan that truly supports the modernization efforts necessary to move the U.S. government into a 21st century environment. Any plan should address critical issues around roles and responsibilities, resourcing (both in budget and in the ability to attract, hire, and retain a highly-skilled digital services workforce), accountability, and key priorities for improve Federal digital service delivery.

2. **Empower the Federal Technology Workforce.** The response to COVID-19 is revolutionizing the way Federal agencies execute their missions how their current (and future) workforces perform their roles in constantly evolving physical and digital environments. To continue this progress, the Administration should develop a comprehensive technology workforce strategic plan that supports the IT skills and abilities of all Federal employees. In addition to constant and consistent upskilling of the core Federal IT workforce (to ensure they are educated, aware, and able to leverage modern commercial solutions to drive mission outcomes) or exercising novel authorities to hire more qualified tech talent, the Administration should immediately work on developing a Federal technology workforce strategy. Specifically, the strategy should:

   a. Establish a robust, hands-on training regimen that enables the Federal workforce to more effectively acquire and leverage more modern software and applications through agile acquisition approaches - which will increase agency productivity and enable more effective mission outcomes;
b. Help contracting personnel conduct more effective market research by providing better data and market intelligence to ensure that technical representatives and contracting officers have the tools they need to rigorously and effectively review commercial technology products and services as part of the acquisition process;

c. Create special pathways to enable human capital exchanges between the public and private sector, for limited terms, to increase the skills, training, and competencies of both Federal agencies and industry partners;

d. Expand and scale the SME-QA pilots to include new and emerging technology and cybersecurity positions within the government and use their skills-based, peer-reviewed hiring model to more quickly and effectively identify talent to fill roles across multiple agencies; and

e. Improve agility, competency, and technical acumen across senior managerial positions to ensure that senior executives understand the impact of technology on their workforce and have the competency to communicate, collaborate, and build strong teams, even in a distributed telework environment.

A more skilled, informed, and technology-forward workforce will enable agencies to use cutting-edge capabilities that will drive stronger outcomes for agency programs and improve digital service delivery for both citizens and internal customers. A plan that includes the elements above (along with other creative focus areas) will reimagine the future of technology capabilities within all Federal jobs and, collectively implemented, empower agencies to scale innovative solutions that meet mission needs.

3. **Improve Performance of Federal IT Spending.** Overall annual IT spending in the government continues to increase, and is currently determined to be around $95 billion. Of that amount, **roughly 80% still goes to maintaining outdated legacy systems.** Every 1% shift away from Operations and Maintenance (O&M) spending and towards Development, Modernization, and Enhancement (DME) would free up hundreds of millions of dollars for agencies to allocate to the acquisition, adoption, and use of modern commercial capabilities, enhanced digital workflows, and stronger collaboration within and between agencies. As one example, the Administration and Congress should work together to create incentives for agencies to allocate some portion of every O&M contract to include modernization efforts, and to keep and savings from eliminating legacy systems and repurpose such savings towards acquiring additional innovative technology solutions.

In addition, Congress should work to ensure that awareness and accountability for IT modernization is a part of every Department head’s responsibilities, especially as they move through the confirmation process and yearly budget justification cycles on the Hill. Members could leverage recommendations in ADI’s *Lost Opportunities* report and include key IT modernization questions during agency budget hearings to get senior leadership on the record about their plans for prioritizing IT modernization and to hold them accountable for results. Congress should require OMB to better detail IT spending (such as tying it to appropriations line items or across various funds within agencies) to ensure greater transparency and traceability for all relevant technology spending.

IT spending data must be tied to agency mission responsibilities and highlight how agency IT does (or does not) effectively support mission service delivery, perhaps by better incorporating the IT Dashboard into the President’s Management Agenda and leveraging its information, along with other useful performance data, to better understand the spending – and effectiveness – of agency IT systems and programs.
Conclusion

Going forward, it is clear that major changes need implementation to reflect the hard lessons of 2020. The current pandemic has accelerated long-pending operational and policy reforms essential to creation and delivery of a modern digital government.

The next Administration and Congress have the opportunity to support bipartisan reforms across both the Executive and Legislative branches to drive important outcomes in Federal IT modernization and digital transformation. Now is the time to embrace the opportunities and address the challenges that the government technology ecosystem has experienced over the past year and use these upcoming months to make overdue, but critical updates to Federal technology, security, and acquisition policy.

To find out more about ADI and how they are supporting the drive for effective IT modernization in government, please visit alliance4digitalinnovation.org