CHAPTER TWO

Going Digital

Daniel J. Chenok

Highlights

- Technology has played a critical role in the delivery of government programs and the conduct of government operations. The evolution toward a "digital government" has improved services, reduced costs, and enhanced security through efforts that have progressed over the past two decades.
- Digital government promotes the introduction of emerging technologies, agile development, a skilled workforce, and flexible investment strategies.
- Law, policy, strategy, organizational, and governance frameworks have laid the foundation for continued improvements in adopting commercial best practices to implement digital government.

GOING DIGITAL

By Daniel J. Chenok

The New York City Fire Department uses a computer-driven Risk-Based Inspection System that leverages digital technology to predict where fires might break out in different parts of the city. This system runs on an algorithm combining data from five agencies and uses artificial intelligence to develop a list of potential high-risk buildings, initially based on 60 indicators. The current version of this system is ten times more powerful than the first version launched in 2010. In 2015, the department started developing a third version to combine data from 17 agencies to predict potential suspect buildings based on 7,500 factors. This example shows how digital change has helped improve government amidst growing complexity.[1]

INTRODUCTION

Today's digital economy has evolved significantly since the eras of mechanical and analog electronic technology. This evolution began in the late 1950s with the advent of mainframe computing as a standard practice for leading businesses, accelerated in the late 1970s with the introduction of personal computers, and continues to the present day in the form of emerging technologies that include cloud computing and artificial intelligence. Beginning in the 1990s, the internet brought about a revolution in how citizens and businesses access, share, and retain information over open networks. These digital steps forward have led to significant changes in how information technology (IT) impacts society, the economy, and government.

What is Digital Government?

Just as the private sector has adapted digital technologies and ways of doing business to serve its customers, government has grown in its digital capacity over the past twenty years. The initial adoption of internet applications for government services two decades ago led agencies to incorporate these technologies in placing information on the web. Early agency websites were followed by the development of applications that enabled secure transactions for citizens and businesses—ranging from student loans to financial filings.

Digital Government Defined

Jane Fountain, Director of the National Center for Digital Government at the University of Massachusetts, Amherst and author of multiple IBM Center for The Business of Government publications, defines digital government as "governance affected by internet use and other information technologies (IT). Digital government is typically defined as the production and delivery of information and services inside government and between government and the public using a range of information and communication technologies. The public includes individuals, interest groups, and organizations, including nonprofit, nongovernmental organizations, firms, and consortia. The definition used here also includes e-democracy, that is, civic engagement and public deliberation using digital technologies."[2]

Today, governments can leverage open networks in the cloud, where individuals work together over the internet in a secure environment to communicate and develop new ideas and applications. Given advances such as artificial intelligence and the "internet of things," mechanisms exist to collect, distribute, and access vast amounts of data in various formats from many sources to help government leaders make decisions that deliver on missions and programs. Moreover, digital transformation has disrupted how government operates—how agencies do work, tackle problems, and meet expectations. Key examples of digital information include:

- Digital government places the user experience front and center. It has ushered in new ways to improve how citizens interact with government, leveraging cross-disciplinary approaches such as design thinking—a structured, interactive method to facilitate innovation among stakeholders. It also affects the government employee experience in ways that can improve service to the citizen; employees who use mobile devices to perform their roles across the country can serve their communities more rapidly, productively, and efficiently.
- Digital processes change the skills needed in today's government workforce—technologies like artificial intelligence (AI) and advanced robotics enable automation of manual tasks. These technologies require new expertise and new ways of working to deliver mission outcomes that meet or exceed user expectations.
- Digital technologies have facilitated the application of virtual and augmented reality in government. Federal agencies have begun working with virtual reality, such as NASA for data visualization and the Department of Veterans Affairs to treat post-traumatic stress disorder.

The U.S. Federal Chief Information Officer (CIO) Council's 2016 *State of Federal IT Report*, prepared under the direction of federal CIO Tony Scott,

found that digital technologies now significantly impact every federal agency and employee.[3] The adoption of emerging technologies has begun to improve internal collaboration, human resources and procurement operations, resulting in a shift away from legacy systems and a push towards transparency and open data. This evolution has been amplified by the impact of technology to improve government collaboration with external partners—agency leaders can now leverage new innovations, like blockchain to work with business partners in a network that provides speed and security for their digital interactions.

Organization of Chapter: The Evolution of Digital Government

Progress in this arena has moved through three major phases along the journey of the past 20 years, as shown in the chart "Evolution of Digital Government: 1998-2018."

- **Early action:** As the position of agency-level chief information officers was authorized under a landmark IT management statute in 1996 (the Clinger-Cohen Act), the growing importance of IT in implementing agency missions led CIOs to develop business cases that showed return on IT investments in the form of mission achievement and cost management. The mission-critical nature of IT also pointed agencies to start integrating security and privacy into planning and implementation. At the same time, the internet first entered wide use in the public sector as agencies took their large volume of written public information and made it widely available on the web. Early cross-government applications, such as the FirstGov web portal, introduced the notion that government could use technology at a wide scale to improve citizen service.
- **Expansion:** The advent of e-government was accelerated by a U.S. federal initiative that established citizen-facing IT projects, shared services for back-office operations and cross-agency architectural standards to drive significant progress. This acceleration was codified in the E-Government Act of 2002, which authorized a presidentially appointed government-wide leader of IT under whose direction agencies continued to advance IT policy and programs, and drive IT security and privacy. Such activity led to the use of open data and open government as ways to continue integrating innovation with citizen service and program outcomes, fueled by enabling technologies like cloud and mobile computing.
- **Institutionalization:** Agency IT progress pointed to the need for strategy, policy, and law to support an updated framework for bringing new talent into government, while strengthening the authorities of CIOs working as leaders of technological change with other mission and mission-support executives to drive outcomes. The highly visible challenges and resolution efforts associated with the roll-out of healthcare.gov in 2013 led the Office of Management and Budget (OMB) and the General Services Administration (GSA) to drive commercial best practice into government through "digital services" teams, innovation officers, and chief technol-

ogy officers. Congress stepped forward with two statutes that advanced governance and funding frameworks. The government has continued to move forward through several 2018 Cross-Agency Priority goals, placing IT modernization as Goal 1 in the President's Management Agenda in a way that is closely linked to data strategy as Goal 2 and workforce improvement as Goal 3. The tie between IT, data, and workforce is especially important given the large volume and variety of digital data now available to agency teams, who can leverage analytics technologies to derive insights from the data that enable them to improve citizen service and performance (see Chapter Three and Chapter Four for more detail).

Evolution of Digital Government: 1998-2018

1998

Early Action: Digital Government 1.0 – Moving Information Online

– Web Portals and FirstGov
– Business Cases for IT Investment
– Security, Privacy, and Accessibility

2001

2001

Expansion: Digital Government 2.0 – Establishing Law, Policy, and Organizational Structures

– E-Government Strategy, Statute
– IT Security and Privacy
– Agile
– Open Data, Open Government
– Emerging Technologies (Mobile and Cloud)

2012

2012

Institutionalization: Digital Government 3.0 – Driving Strategy, Services, and Modernization

– Digital Services
– IT Modernization
– Emerging Technologies (AI, Blockchain, IOT)

2018

To continue advancing digital government, agencies must invest in modern technologies that support secure and scalable applications. Identifying and prioritizing efforts for investment, integrating these priorities into agency and federal budget planning cycles, and applying appropriate measures to track the success of key efforts will drive progress. Critical to effective investment in digital modernization is understanding the existing barriers to capturing savings over time from those investments, and identifying means to overcome these barriers. Investing in emerging technologies that can help government will inform where and how private sector entities may most effectively support digital transformation to improve performance and reduce cost.

The remainder of this chapter presents more detail about these three phases. The chapter concludes with lessons learned and observations about what's on the horizon as government relies on emerging technologies to drive continued performance improvement.

EARLY ACTION: DIGITAL GOVERNMENT 1.0—MOVING INFORMATION ONLINE TO SUPPORT THE MISSION

Policy Foundations

The roots of digital government actually took hold well before 1998. Toward the end of the Carter administration, with the increased use of IT systems to collect federal information and deliver services, Congress focused on improving oversight of federal IT, and ultimately enacted the Paperwork Reduction Act of 1980 (see the box highlighting key the statutory milestones that drove the early years of digital government). OMB then worked with senior agency IT officials to oversee information management for well over a decade, reviewing implementation challenges with major IT systems—including "Presidential Priority Systems" in the 1980s and "SWAT" teams in the early 1990s. With the advent of the internet in the mid 1990s, government agencies followed a private sector trend and began to create CIOs to manage information as a strategic asset in the context of rapidly evolving technologies. Key national IT issues that arose in the 1990s remain on the agenda for digital government today, including the government's approach to the internet, electronic commerce, encryption, and website policies. During this time frame, the National Performance Review led numerous experiments and pilot programs to adapt commercial innovation in these areas for government.

Statutory Foundations of Digital Government

1974: The Privacy Act[4] established a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by federal agencies.

1980: The Paperwork Reduction Act[5] gave OMB authority over agency IT and information policy and management, using the term "information resources management" (IRM) to describe such activity.

1987: The Computer Security Act[6] was intended to improve the security and privacy of sensitive information in federal computer systems and to establish minimally acceptable security practices for such systems. It required the creation of computer security plans, and appropriate training of system users or owners where the systems would display, process or store sensitive information.

1996: The Clinger Cohen Act[7] authorized a CIO at each agency who had responsibility for IT leadership, and led to an Executive Order that created the Federal CIO Council.

First Digital Steps

Web Portals

By 1998, most agencies in government had created websites that enabled internet access for citizens and business. As agencies expanded the amount of information on the web, it became apparent that the public would have an easier time understanding and accessing government data by establishing a "portal" that would tie together different websites within and across agencies, following private sector advances in the use of portals to link common information for consumers. State governments made early progress on portals, as discussed in the 2001 report by Jon and Diana Burley Gant and Craig Johnson*, State Web Portals: Delivering and Financing E-Service*—portals allowed states "to use the internet and web-based technologies to extend government services online, allow citizens to interact more directly with government, employ customer-centric services, and transform the provision of traditional government services."[8]

FirstGov

As 2000 approached, federal agencies had created over 30,000 different sites, with loose coordination from OMB for policy and GSA which led a federal webmasters working group. GSA developed an early experiment to pilot a federal portal, initially referred to as "webgov." At the same time, internet companies were developing search capability well before the founding of Google several years later. An early search engine industry leader, Inktomi, offered to index all government information on the web and make it searchable by the public—a proposal made by Inktomi CEO Eric Brewer to President Bill Clinton at the 1998 Davos Conference. The administration supported Brewer's idea and launched an initiative to expand webgov and develop "FirstGov"—the government's first cross-agency web portal linked to this new search capability. The effort served as the first major interagency technology effort, with leadership from OMB and the National Performance Review, and governance and funding from multiple deputy secretaries who served as a Board of Directors. FirstGov was launched in September 2000. Since then, it has evolved significantly in terms of functionality, was rebranded as www.usa.gov, and has expanded as a resource for government and the public. The site is still managed successfully by GSA.

Business Cases for IT Investment

As is the case today, new technology initiatives like FirstGov were constrained by legacy systems and performance issues with in-house IT operations. The Internal Revenue Service, the Office of Personnel Management, and a range of other agencies were managing large, complex, mainframe-based systems that delivered key mission services and programs—but had no common standards or metrics by which to measure that performance. To help manage this growing complexity of technology-mission intersection, OMB developed a common template for agencies to justify the investment and track progress in IT investments over time, based on commercial best practice and consistent with federal law in the implementation of the policy. This template was implemented as a budget requirement in the late 1990s, referred to as the "Exhibit 300," and significantly expanded in the early 2000s. Although the title and specifics around this requirement have evolved, agencies still track progress and submit a business case for their IT investments to OMB.

Security and Privacy

A key element of these business cases, and of success in agency IT delivery generally, revolved around computer security and privacy challenges that remain present for government today. The Privacy Act of 1974 and the Computer Security Act of 1987 provided initial statutory focus for agency leaders to address these imperatives. Genie Stowers' 2001 report, *The State of Federal Websites,* addressed legal and policy issues that remain challenges

today: "to ensure security, provide security against hackers, and protect citizens' privacy."[9]

In 1998, Congress updated the Computer Security Act to increase its focus on data protection; around the same time, agencies developed secure data transaction strategies through the introduction of digital signatures. Through efforts led by GSA and the Federal CIO Council, agencies leveraged digital signature and emerging encryption technologies to strengthen how the public exchanged information with government, providing key protections to help agencies address "issues of privacy and security as they increase access to information and delivery of services electronically," as noted in the 2001 report by Janine Hiller and France Belanger, *Privacy Strategies for Electronic Government.*[10] The digital signature programs were managed by GSA based on expert guidance from the National Institute of Standards and Technology (NIST) and overseen by agency CIOs and OMB, progress outlined by Stephen Holden's 2004 report *Understanding Electronic Signatures.*[11] These programs have evolved in maturity, but policies in this area remain in place today.

Accessibility

As more government programs and services moved online, the need to ensure digital access for populations who faced challenges with access to technology became a paramount objective—to ensure that all citizens could share in the benefits of this change. In 1998, Congress amended the Rehabilitation Act of 1973 to require federal agencies to make IT accessible to people with disabilities. Section 508 of this law[12] applies to all federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508, agencies must give disabled employees and members of the public access to information that is comparable to the access available to others. The implementation of this law continues twenty years later, with renewed focus on adapting digital technology being led by GSA and the Access Board (a small agency charged with Section 508 policy oversight).

Case Study: Student Financial Aid Modernization

An early example of agency movement to digital government that addressed all of these issues, and which remains instructive today, was the reform of the Department of Education's Student Financial Aid systems. The Department had already introduced a web option to apply for Federal Aid, launching this as one of the first online government applications in 1996—but Education's back-end systems remained beset with legacy performance issues. Working with National Performance Review and OMB's Office of Federal Procurement Policy, the Department awarded a contract that allowed its industry partner to make investments and be repaid from the savings that those investments brought by streamlined operations—a concept known as "share-in-savings." This incentive

structure enabled the industry partner to work in collaboration with the government to develop a modernization and integration roadmap. It also set the foundation for additional statutory authorizations of share-in-savings, as well as current consideration of funding models that support modernization and share risks and rewards between government and contractors.

EXPANSION: DIGITAL GOVERNMENT 2.0—ESTABLISHING LAW, POLICY, AND ORGANIZATIONAL STRUCTURES TO LEVERAGE EMERGING TECHNOLOGY

As government began to recognize the power that emerging digital technologies offered to help improve productivity and mission effectiveness while reducing costs, the need for leadership in driving change became apparent. This manifested itself in the form of federal law, policy, and strategy that enabled new technologies to improve mission and back-office operations, while also ensuring protections for cybersecurity and privacy.

Organizational Advances: The OMB Office of E-Government and the E-Government Act

OMB sought to elevate the focus on IT across the government in the early 2000s, in response to calls from the IT industry and Congress for a government-wide Chief Information Officer. The Bush Administration created a political appointee position in OMB dedicated to technology with the title of "Associate Director for E-Government and IT" in 2001. This official, Mark Forman, established a governance structure to bring commercial best practices to the federal government, lead implementation of IT and security law and policy, and formulate President's Management Agenda initiatives related to acquisition and use of IT. This led to a multi-faceted IT transformation initiative focused on managing IT as an investment and a set of cross-agency initiatives and policies, shifting OMB's role in federal IT from one largely focused on policy and general oversight to one that also drove specific government-wide initiatives designed to gain effectiveness with a focus on citizen services, and gain efficiencies by reducing duplicative systems—a role that continues today.

At the same time, Congress introduced bipartisan legislation to authorize this enhanced oversight role in IT. The E-Government Act of 2002[13] codified many of the policies and initiatives of the new E-Gov office. The Act designated the head of the new E-Gov office as the "Administrator for E-Government and Information Technology"—this position was the de facto federal CIO, and as discussed below would later receive that designation formally as

well. Mark Forman became the first Administrator

The E-Government Act also reauthorized an expansion of prior security statutes, renamed as the Federal Information Security Management Act (FISMA). Other provisions enhanced agency responsibilities and OMB authorities in numerous related areas, including privacy, records management, digital signatures, and citizen services. Finally, the Act authorized a fund for E-Government initiatives, administered by GSA and building on previous funding mechanisms that provided OMB with authority to direct spending on innovation. The budget approach used for the E-Gov Fund has since been revised and used for other purposes, and in 2017 was given impetus from a new statute (see the discussion of the Modernizing Government Technology Act later in this chapter).

The E-Gov office also expanded its role across areas related to IT activity in the agencies, raising attention to oversight and review of key agency systems and elevating resolution of significant issues through program reviews led by the OMB Deputy Director for Management. Other areas of increased attention that would be addressed by the E-Gov office included shared services across government back office functions, authentication of identities by federal employees and contractors in using government IT systems, greater focus on cybersecurity for civilian agencies, and coordination of IT security with the Intelligence Community.

The E-Gov Strategy

A key advance in the digital evolution of the federal government involved a three-part strategy led by the E-Gov office, which was incorporated into the first President's Management Agenda (PMA) in 2001.

Project Quicksilver

Under the first part of this strategy, OMB worked with the President's Management Council and the Federal CIO Council to develop a set of 25 cross-agency initiatives that improved service to four portfolio groups: citizens, businesses, state and local governments, and government employees. These initiatives, which resulted from an E-Government Strategy Study often referred to as "Quicksilver," were the product of a team of government innovators who followed a method for driving technology change in the private sector. The study team conducted interviews across all federal agencies and led public outreach efforts to solicit ideas for improved service to all constituencies—from small businesses to grant recipients to national park visitors. The team developed more than 50 project candidates organized into the four portfolios noted above and worked with the President's Management Council to select the 25 final projects based on review of high-level business cases. These projects were led by interagency teams, driven by a lead agency and involving multiple partners, who leveraged digital technology and related processes

to develop public-facing, user-friendly websites or consolidated systems that improved access to and service from agencies. Many of the initial E-Gov websites remain in operation today as models of digital government, ranging from Regulations.Gov (the subject of a 2013 report by Cynthia Farina, *Rulemaking 2.0: Understanding and Getting Better Public Participation)*[14] to IRS E-File (the subject of a 2006 report by Stephen Holden, *A Model for Increasing Innovation Adoption: Lessons Learned from the IRS e-file Program)*[15] to Disasterassistance.gov.

This citizen focus was intended to build trust in government through technology that enhanced citizen participation. As noted in the 2004 report led by Marc Holzer, James Melitski, Seung-Yong Rho and Richard Schwester, *Restoring Trust in Government: The Potential of Digital Citizen Participation,*[16] "Technology has created new tools for allowing citizens to more meaningfully participate in a dialogue with their fellow citizens and their government. In an increasing number of cases, these tools have been successfully employed and are improving the quality of public decisions." Trust among government and industry was similarly enhanced by greater efficiencies delivered through advanced procurement reforms introduced by OMB in the 1990s, and implemented through GSA by several e-procurement initiatives that improved business interactions with government. The federal government also learned from and was influenced by the e-procurement experiences of state governments and international governments, as outlined in a 2001 report by M. Jae Moon, *State Government E-Procurement in the Information Age: Issues, Practices, and Trends,* and Mita Marra *Innovation in E-Procurement: The Italian Experience* in a 2002 report.[17]

Federal Enterprise Architecture

The second part of the E-Gov Strategy sought to modernize the technology that supported public-facing applications and data systems through "enterprise architecture," a discipline that had driven commercial reforms in the financial and other sectors. Although the Clinger-Cohen Act created the requirement for a government wide architecture, this was never associated with a mechanism to measure and drive better return on IT investment. OMB created a "Chief Architect" position to drive this work forward—a position that still sits within the Office of the Federal CIO—and worked with federal CIOs to develop a Federal Enterprise Architecture (FEA). The FEA served as a blueprint for IT modernization at multiple layers: technology infrastructure, software applications, data, business processes, and performance information. Each layer was outlined through a reference model that set out common standards and approaches. In parallel, OMB aligned every federal IT investment with the architecture to identify redundant systems across agencies. The FEA has since been integrated into agency architectures and serves as a foundation for specific architectural initiatives like the recent Human Resources Integrated Business Framework that the Office of Personnel Management is using to drive common personnel approaches.

Shared Service Lines of Business

The third part of this strategy, begun under Mark Forman and significantly expanded by the next E-Gov Administrator, Karen Evans, involved the integration of common business functions, referred to as "lines of business" (LOBs) that brought together common back-end services across agencies. Similar to the governance of the Quicksilver initiatives, the LOBs were driven by lead agencies who developed standard processes that other user agencies could adapt. The initial LOBs focused on financial management, human resources, grants management, case management, and health IT—commencing progress that continued into 2018, with shared services now led by GSA's Unified Shared Services Management Office. This office has considerably advanced on the work of these early LOBs, especially in the financial and human resources space.

Integrating Digital Government and Cybersecurity

The tragic events of 9/11 changed the world, including government. At an organizational level, both the integration of civilian mission agencies into the new Department of Homeland Security (DHS) and the coordination of intelligence agencies under the Directorate of National Intelligence have helped enhance how government agencies work to protect the nation. In the Government IT space, the focus on cybersecurity significantly expanded post 9/11 as well, with Karen Evans leading cross-agency cybersecurity work alongside DHS, National Institute of Standards and Technology (NIST), and the Federal CIO Council—all working closely with intelligence community efforts. These federal efforts were aided by FISMA, discussed previously in this chapter (FISMA was reauthorized in 2014[18] and remains the primary cybersecurity law for agencies to follow).

Organizational Drivers for Cybersecurity

The need to build cybersecurity into the fabric of digital government continued to become more evident throughout the first decade of the 2000s. This focus expanded with the 2009 establishment of a National Coordinator for Cybersecurity in the White House, as well as OMB's later designation of a separate "Cyber Unit" in the Office of E-Government for policy and delegation to DHS for operations. These and similar organizational enhancements at DHS and NIST were accompanied by policies that required greater agency focus on cyber across the range of IT and mission programs. This digital policy infrastructure remains largely in place today.

Identity Management

As more government online transactions required greater protections for security and privacy, the need to bolster identity management policies and processes became a major priority. In the aftermath of 9/11, this objective moved forward significantly through a presidential policy mandating a digital ID credential for government employees and contractors—the Personnel Identity Validation (PIV) card required by Homeland Security Presidential Directive 12.[19] This Directive increased the government's priority on digital signature and secure authentication activity that had been introduced in the late 1990s, and expanded by the Quicksilver "E-authentication" initiative. PIV cards are now the standard for all physical (and a significant amount of IT) access to government resources. Identity policy evolved into the 2011 National Strategy for Trusted Identities in Cyberspace[20] and into a 2018 effort at upgrading identity management efforts led by OMB.[21]

Technology, Innovation, and Government Reform

The Obama administration built on the significant preceding activity to focus on open government, citizen participation, and cloud implementation. This work commenced with a tech-focused agenda in the 2008 Presidential Transition. As Beth Noveck and Stefaan Verhulst wrote in their 2016 report, *Encouraging and Sustaining Innovation in Government*: "the transition team set up the first ever presidential transition website to inform and engage the American people in the process of planning the first 100 days of the new administration…. The transition also notably included the first ever committee to design and plan a technology strategy for the first 100 days of the Obama administration called the Technology Innovation and Government Reform (TIGR) team."[22] This team drafted an Open Government directive that the president signed as one of his first actions after taking office, on Jan. 21, 2009.[23]

The administration then appointed the first Chief Technology Officer (2009) and later the first Chief Data Scientist (2015) in the U.S. Government, both of whom were positioned in the White House Office of Science and Technology Policy. Also, the E-Gov Administrator at OMB was given the additional title of federal CIO, which became and remains the primary title for the position today.

Advances in digital government were spurred on by the adoption of agile techniques in agencies. The government began a shift away from large-scale and long-term systems development that can take years before the first functionality is available for testing. A more innovative approach commenced with agile, a commercial best practice for software development relying on short, iterative "sprints," releasing new functionality in increments, and gathering user feedback using design thinking principles. This effort was first chronicled in a 2013 report by Phillipe Kruchten and Paul Gorans, *A Guide to*

Critical Success Factors in Agile Delivery.[24] Agile approaches have remained key tenets behind the work of new innovation and digital services offices described below.

Two Technologies that Drove Digital Government Expansion

The evolution of two specific technologies demonstrates how digital evolution brought about significant change in government: mobile computing and cloud computing.

Mobile Computing

Mobile computing transformed how people interact with technology, through a broad range of devices (from cell phones and tablets to watches and wearables) that enable communication anytime and anywhere over open networks. Mobile "apps" that improve how people interact in the private sector have also been adopted by government. There are two broad types of government apps:

- **Enterprise-focused apps:** mainly for internal use within a public organization. They are accessible to employees and operate within secure firewalls established by the agency.
- **Citizen-oriented apps:** intended for external use. They are accessible to anyone who seeks to use government services.

Mobile government has brought significant benefits to agency operations, including:

- Cost reduction
- Efficiency
- Transformation/modernization of public sector organizations
- Added convenience and flexibility
- Better services to the citizens
- Ability to reach a larger number of people through mobile devices than would be possible using wired internet only

The federal government has taken steps to drive mobility forward, led by GSA's Digital Government Division that promotes mobile-oriented testing, registry, and related solutions. For example:

- "Making MobileGov" was a multi-media project created by the cross agency MobileGov Community of Practice to help federal agencies discover, discuss, and design a citizen-centric path to mobile government services and information. Begun during the summer of 2011, this project served three strategic goals: educate, develop resources to accelerate mobile efforts, and build a Mobile Gov Community.[25]

- A state-level model can be found in "Gov2Go in Arkansas", recognized by the National Association of State CIOs as a leading "personal government assistant" app.[26]

However, while the foundations for mobile government have been put into place, the uptake in the use of mobile applications in government remains a work in progress. The report *Using Mobile Apps in Government* by Sukumar Ganpati found that as of 2014, only 3 percent of people interacted with federal agencies via digital apps, and only 17 percent of federal agencies had a digital app.[27] Advances have been made since, but room for progress remains.

Cloud Computing

Cloud computing has transformed businesses across industries, shifting how IT is delivered by hosting infrastructure and applications remotely at lower cost. A 2008 IBM Center report by David Wyld, *Moving to the Cloud: An Introduction to Cloud Computing in Government*, provided one of the first definitions of what was then a new term for distributed computing and has seen massive growth since: cloud computing is "delivered over the internet, on demand, from a remote location, rather than residing on one's own desktop, laptop, mobile device, or even on an organization's servers…to deliver applications, computing power, and storage."[28]

The private sector has built many applications that leverage cloud computing's cost and efficiency benefits. After a slow initial rate of cloud adoption, governments have also accelerated progress—though financial constraints and the continued reliance on older legacy systems to deliver services have limited agency deployment of cloud-based solutions.

While a major benefit of cloud computing involves containing costs through shared services and infrastructures, cloud adoption is also helping government agencies to improve operational flexibility despite a continued reliance on back-end legacy systems. Cloud computing has allowed the deployment of more current services with elastic capacity, helping government programs to respond to changing business conditions. Additionally, cloud computing has allowed agencies to increase agility in responding to new challenges and opportunities, accelerating expansion of digital government. For example, if critical websites get hacked, cloud applications can allow agencies to quickly rewrite the controlling software; cloud can also speed access to track real-time data for mission applications like air traffic control.

The federal government launched two programs to foster consistent implementation and compliance for cloud computing, which facilitated its expansion across agencies: CloudFirst and FedRAMP.

- **CloudFirst.** The government instituted its CloudFirst policy in 2010 to accelerate the pace of cloud adoption.[29] This policy promoted service management, innovation, and adoption of emerging technologies. Accord-

ing to the policy, "focus will shift from the technology itself to the core competencies and mission of the agency."[30] As a result, many agencies can now support their mission-critical operations with agile and innovative cloud deployments that incorporate mobile, social, and analytics technologies. However, they also have to take stringent compliance and security measures to protect their systems from internal and external threats.

- **Federal Risk and Authorization Management Program (FedRAMP).** FedRAMP, introduced in 2011, is designed to standardize security services and streamline assessments so that each cloud service considered by federal agencies is evaluated once, at the government-wide level.[31] FedRAMP is intended to avoid duplication of effort across agencies, saving time by supporting initial security evaluation and allowing continuous monitoring of cloud security. FedRAMP continues to address issues of slow processes that have been the subject of some critiques in agencies' ability to keep pace with commercial practices for cloud computing.

Crucial IT and business advances have been enabled by cloud applications in government. For example:[32]

- **IT consolidation**: Government agencies have realized the benefits of consolidating redundant or unnecessary IT assets to increase operational efficiencies. They are reducing the cost of IT ownership by integrating systems through the cloud. Similarly, data center consolidation, an effort that spans multiple administrations, is helping to reduce hardware costs and also to drastically reduce energy consumption.
- **Shared services**: More government agencies have moved towards sharing IT services to reduce costs and to improve business process efficiencies. Some key federal programs have leveraged shared cloud-based infrastructure and software solutions, as well as security capabilities like continuous diagnostics monitoring and threat detection.
- **Citizen services**: Cloud-based technology improves delivery of a variety of public applications, such as allowing citizens to monitor their energy and water consumption, check the status of their service requests to government programs (e.g., benefit and loan applications), and access their medical records.

A number of federal agencies, including the Departments of Defense, Justice, Agriculture, and Education, were early cloud adopters, setting the trend and direction for others to follow in expanding their use of the cloud. Many agencies started with email—GSA was the first federal agency to adopt cloud-based email back in 2010; the National Oceanic and Atmospheric Administration followed a year later, migrating employees and contractors; and the Department of Justice began migrating its email accounts in December 2016. The main drivers for cloud email adoption included money savings, enhanced data sharing capabilities, and improved collaboration.

State and local governments have also made significant progress in moving to the cloud. For example, the 2013 report by Shannon Tufts and Meredith Weiss, *Cloudy with a Chance of Success*, showed how North Carolina put in place five successful public sector cloud computing contracts.[33] Paul Wormeli's 2012 report, *Mitigating Risks in the Application of Cloud Computing in Law Enforcement,* discussed challenges and opportunities for public safety professionals to leverage the cloud in improving their productivity, and effectiveness in protecting and serving the public.[34]

Identifying Challenges to Institutionalization

Overall, federal agencies are still in the expansion phase for digital tools in general. Ganapati's 2016 report on mobile government, cited above, found that the top barriers for incorporating digital tools are:

- Limited or declining IT budgets
- Security and privacy concerns
- Lack of digital skills in the agency
- Limitations of legacy systems
- Cultural resistance
- Unclear long-term vision

In addition to these barriers, two longer-term challenges face agencies as they seek to institutionalize digital practices:

- **Governance:** Technology now permeates all aspects of organizational activity, whether in industry or government. Agency CIOs are a central—but by no means the only—player in technology adoption to improve mission performance; a range of other key stakeholders includes chief financial officers, procurement executives, customer experience and design experts, program managers, industry partners, oversight offices, and ultimately system users in the public. Absent a delineation of roles and responsibilities, consistent metrics, and a clear decision framework, digital advancement can be stymied if different elements spin out of control. A governance framework can help to bring these pieces together; related to governance is the challenge of "orchestration," which calls for integrating technology management with a skilled workforce, user experience, and service delivery to foster significant productivity improvements.
- **Investment Tools:** Government agencies often have difficulties obtaining capital investment dollars to upgrade and modernize systems. Technological innovation most often comes from the private sector, and government has struggled with limited experience using an investment model that allows agencies to leverage commercial innovation while minimizing substantial upfront investment costs; the student aid modernization case study discussed earlier in this chapter has proven to be the exception rather than the rule. Government faces a challenge of incentivizing investment in the private sector that public agencies then pay for through

operational budget savings over time. In response, through a service model where the private sector provides the technology, agencies can also build those costs into long-term contracts. Such "share in savings" or "gain sharing" models are often used by industry in moving to commercial providers for shared services management and operations, to improve service and reduce costs. As discussed below, the Modernizing Government Technology Act now authorizes flexible funding arrangements in government for investing across years with a savings payback requirement.

INSTITUTIONALIZATION: DIGITAL GOVERNMENT 3.0—DRIVING STRATEGY, SERVICES, AND MODERNIZATION

As digital technology took hold throughout the economy in the last decade, new business models flourished that rely on mobile, cloud, and now emerging technologies like artificial intelligence and blockchain, to enable reinvention of how users find information and receive services. As with each wave of the digital journey over the past 20 years, government has followed suit. At the federal level, this movement has been facilitated by strategic, organizational, and statutory drivers across the past decade.

Developing A Digital Strategy

The 2012 Digital Government Strategy, released by OMB with implementation led by GSA's Office of Citizen Services and Innovative Technologies, laid out a broad digital plan to harness information technology in federal agencies.[35] This strategy integrated and updated a set of IT-related actions that had been introduced under a "25-point plan" for IT reform championed by federal CIO Vivek Kundra in 2010.[36] The Strategy was premised on four principles:

- Create an information-centric government that focuses on open data and content
- Establish a shared platform within and across agencies
- Take a customer-centric approach in presenting data
- Build required security and privacy measures up front

The Strategy set out broad goals for the institutionalization of digital government:

- Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device.

- Ensure that as the government adjusts to this new digital world, agencies seize the opportunity to procure and manage devices, applications, and data in smart, secure, and affordable ways.
- Unlock the power of government data to spur innovation and improve the quality of services for the public.

Creating Digital Services and Innovation Offices

A number of new organizational structures have increased capacity and sustainability for digital government over the past decade. These include the Presidential Innovation Fellows, GSA's 18F office, agency innovation offices, and the U.S. Digital Service.

Presidential Innovation Fellows

The Digital Strategy's principles had already begun to be practiced through a new program designed to bring private sector technology talent into government: the Presidential Innovation Fellows.[37] Introduced by the federal chief technology officer in 2012, as Noveck and Verhulst write in their *Sustaining Innovation* report, the Fellows program "connects innovators from the business, nonprofit, and academic sectors with government departments. Together, they work to produce innovative, short-term projects to improve government efficiency. The program has evolved from one that parachutes new people into the White House to one that pairs innovators with civil servants to help implement change."[38]

GSA's 18F

The original Presidential Innovation Fellows model envisioned shorter details with government, followed by a return to the private sector. As Fellows moved into agencies, many found that they wanted to remain in the government for a longer tenure because of the impact they saw that digital transformation could have on key missions for the American people. To provide a home for Fellows who remained and a venue for other technology experts to join the government, GSA established an innovation office called "18F" in 2014 (so titled because GSA's DC headquarters are at 18th and F STs NW). 18F[39] brought in a high-tech start-up culture to government, aiming "to provide cutting-edge support for our federal partners that reduces cost and improves service."[40]

Agency Innovation Offices

As the Fellows and 18F began to use digital services to help a growing number of agencies modernize their applications, several agencies established their own innovation offices, led by the Department of Health and Human

Services. In a 2014 report by Rachel Burstein and Alyssa Black, *A Guide to Making Innovation Offices Work,* the authors identified key characteristics of federal innovation offices, comparing and contrasting them with state, local, and global counterparts to draw key lessons, such as: "moving forward with setting up a center of gravity for innovation should follow a careful assessment of the mission of the new office, financial resources available, and support from key partners."[41]

U.S. Digital Service

Even as government was transforming to institutionalize digital innovation, a core federal program suffered a major setback: the flawed release of the healthcare.gov website, which was the public's main channel to access health insurance exchanges in 2013. This website was critically linked to the success of the implementation of the Affordable Care Act. The website's operational problems resulted from numerous challenges identified above, including:

- a lack of governance across stakeholders
- limited use of agile techniques to deliver incremental functionality
- contract-related constraints on leveraging commercial innovation

In responding to these and other challenges, the administration brought on a "rescue team" of private sector technology and business experts who used digital best practices to fix issues with the website and its underlying IT systems. The success of this effort led the administration to conclude that replicating this approach would be a benefit to modernizing other large and complex technology systems—resulting in the 2014 establishment of the U.S. Digital Service (USDS) in OMB, driven by numerous IT leaders including federal CIO Steve VanRoekel.[42]

USDS drew on lessons learned from a similar office in the United Kingdom, the Global Delivery Service, to address challenges throughout government by using digital technology. As Ines Mergel wrote in her 2017 report, *Digital Service Teams: Challenges and Recommendations for Government*, USDS and other digital service teams "typically operate outside existing agency IT organizational structures and recruit IT talent directly from the private sector. They are given a mandate to rapidly implement change initiatives using commercially-developed tools and processes such as human-centered design and agile innovation management techniques—which are standard practice in the private sector, but have been infrequently adopted in the public sector."[43] Mergel's report also pointed out the challenges of integrating across new digital service and existing agency IT teams, including the different roles and cultures involving change agents relative to those involving the delivery of government operations at scale. This healthy tension can be made into a benefit through clearly defining responsibilities across the IT development lifecycle, communicating in a transparent manner as prototype digital applications migrate to a subsequent delivery phase, and approaching collaborative activities with mutual respect.

USDS summarized key digital service principles and recommended actions in its 2014 "Digital Services Playbook,"[44] which has since been used by agencies and industry partners to guide digital projects throughout government. Many of these elements focus on frequent interaction with users through agile development as well as "design thinking," an approach to innovation where groups of users collaborate in real time to innovate on new ideas and develop code; government and industry now even co-create together in a variety of "design studios."

Legislation Catches Up: FITARA and MGT

Government use of digital technology over the past two decades had been accomplished primarily through two statutes, the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Following the significant attention to the positive outcomes that technology could bring, as well as the risks that accompanied technology failures, Congress recognized the need to update frameworks that authorized agency activity, including CIO authorities to drive change and implement funding flexibility and respond to ever-increasing cybersecurity risks and threats. Two new laws have helped the government to lock in and drive forward progress in digital transformation.

New Approaches to CIOs and Governance: The Federal IT and Acquisition Reform Act of 2014 (FITARA)

FITARA[45] changed how federal agencies acquire and manage IT. A central purpose of FITARA was to give greater authority to agency CIOs in directing IT spending, procurement, and activity across their enterprises, with the goal of enhancing effectiveness. Under this statute, the CIO is accountable for the performance of all IT projects in his or her agency, including approval for IT procurements and oversight of IT staff; agencies are also charged with leveraging commercial best practices. FITARA requires CIOs to lead reviews of IT portfolios that enhance transparency and improve risk management, with additional provisions to improve IT management that include expanded training for IT staff, data center consolidation, enterprise software buys, and strategic sourcing.

OMB issued 2015 guidance[46] on FITARA implementation that further promoted institutionalization of sound digital management, largely by addressing the governance challenge cited above. The guidance set out a baseline for sound IT management and strong cybersecurity, and delineated specific roles and responsibilities for CIOs and their mission support brethren in integrating IT to improve performance across the enterprise: chief financial officers, chief acquisition officers, and chief human capital officers, among others. FITARA implementation is continuing to mature, with the Government Accountability Office (GAO) assessing agency progress through a set of metrics that ensure continued oversight for this important IT management statute. On the cyber

side, FITARA has been complemented by the FISMA reauthorization noted above, as well as two other 2014 statutes that strengthen DHS authorities to collaborate with industry and help agencies address risk, increase skills, and build resilience: the Cybersecurity Enhancement Act of 2014[47] and the Cybersecurity Workforce Assessment Act.[48]

Two IBM Center reports capture activities led by CIOs to drive improvements in digital government. First, consistent with the longstanding focus from GAO and multiple administrations on the importance of IT metrics, CIOs increased their focus on measuring outcomes for their work. Kevin DeSouza's 2015 report, *Creating a Balanced Portfolio of Information Technology Metrics*, noted that CIOs over time had not done enough "to invest in the creation of metrics that capture the performance of IT assets and their contribution to organizational performance."[49] DeSouza found improvements being made by CIOs who recognize the value of metrics to guide IT strategic planning, contract oversight, cost management, and benchmarking against commercial best practice.

Second, as CIOs sought to integrate innovation into their operations, working alongside new digital services and innovation offices have represented a challenge. Because many of these offices do not fall under the purview of the CIO, and are often staffed by outside IT experts without much prior experience in federal operations, their path to innovation often differs from the experience of government CIOs. A 2015 report by Greg Dawson and James Denford, *A Playbook for CIO-Enabled Innovation in Government*, provides a roadmap for CIOs to move forward in driving innovation that adapts evolving digital transformation to government. The authors found that "few agencies have a defined and repeatable process for enacting innovation. Rather, often the person who generates the idea is unaware of a process to enact the innovation, and either tries to create a process or simply gives up trying to implement it."[50] In understanding how to overcome this constraint, Dawson and Denford interviewed successful CIOs and concluded that "committed leadership and an enterprise-wide ecosystem can foster a culture of innovation, institutionalized through repeatable processes that garner buy-in from all stakeholders—from digital service teams to program offices."

New Approaches to Funding Innovation: The Modernizing Government Technology (MGT) Act of 2017

Another major challenge to institutionalization identified above revolves around funding for digital transformation. In order to provide agencies with flexibility to invest in change and benefit from returns on that investment, agencies need funding flexibility. The MGT Act[51] now gives OMB and agencies the authority to establish working capital funds that support IT modernization by authorizing multi-year, commercial-style budgeting; this provides agencies with more tools to move to the cloud, implement shared services, and improve cybersecurity. MGT implementation has just begun, with federal CIO

Suzette Kent leading a cross-agency board that selects and oversees investments in a central Technology Management Fund.

The President's Management Agenda Redux: The Cross-Agency Priority Goal for IT Modernization

MGT Act implementation is one part of a broader strategic imperative for IT modernization that will fuel progress in digital government. Just as a three-part E-Gov Strategy brought IT into focus as a major administration priority in the President's Management Agenda of 2001, the current administration's Management Agenda designates IT Modernization as its first Cross-Agency Priority (CAP) Goal (see the discussion of CAP goals in Chapter Four). The new 2018 IT Modernization goal, which builds on the previous administration's Cross-Agency Priority Goal of "Smarter IT Delivery,"[52] captures recommendations made by government and industry leaders over the past year, and reflects on lessons learned over the past twenty years. The goal's central tenet calls on agencies to "build and maintain more modern, secure, and resilient information technology (IT) to enhance mission delivery and productivity—driving value by increasing efficiencies of Government IT spending while potentially reducing costs, increasing efficiencies, and enhancing citizen engagement and satisfaction."[53]

Another element of the CAP Goal drives forward toward greater use of cloud computing, furthering the efforts discussed earlier in this chapter. Eight years after the federal government adopted the 2010 Cloud First policy, agencies still faced hurdles in deploying cloud solutions. An interagency working group led by GSA has started to make headway on smoothing the path to the cloud for agencies. The group, called the Cloud Center of Excellence, kicked off in January 2017 and aims to provide agencies with advice on best practices for cloud adoption. The Center of Excellence, one of five such Centers at GSA helping to drive IT modernization forward, includes more than 140 participants representing 48 different agencies, and serves as a knowledge-sharing network and a clearinghouse for cloud adoption tips. The group is working on documents to help agencies address cloud funding challenges, acquire cloud solutions more rapidly, and provide for enhanced cloud security.

Importantly, the IT Modernization agenda is overseen by a strong governance coalition that includes OMB, GSA, the new White House Office of American Innovation, and lead agencies (starting with the U.S. Department of Agriculture). The agenda focuses on accelerating agency movement to the cloud, carries forward agile principles, and strengthens collaboration among CIOs, digital service offices, and other stakeholders—with strong support from the OMB Deputy Director for Management. Another key element of this agenda draws from a digital evolution in the commercial sector reflecting new technologies that rely more on data and less on the computing platforms that produce that data, as well as a workforce with 21st century skills to implement these emerging innovations; the pairing of the IT Modernization initiative

with related CAP goals that focus on data and workforce modernization will help expand institutionalization of digital government.

A 2018 report by Greg Dawson, *A Roadmap for IT Modernization in Government*,[54] recommends a series of key actions and steps that agencies can take to plan, assess, execute, and measure modernization activities, based on research into recent successes in public and private sector IT modernization. Dawson presents several findings that CIOs and other IT leaders can adapt to help drive digital transformation:

- Modernization must be an ongoing process rather than a single standalone event, to allow for continuous improvement.
- Technology must support mission goals.
- IT implementation must include a strong technical approach and acquisition strategy.
- Collaborative governance, measurement identification and communication, and stakeholder feedback must occur throughout the process to capture lessons learned.

LESSONS LEARNED

Much of the government's digital experience over the past 20 years demonstrates the need to balance disruptive innovation with sound IT management, cost-effective outcome measurement, and strong cybersecurity. A leading government-industry IT partnership, the American Council for Technology and Industry Advisory Council, issued a framework entitled *7S for Success*[55] that captures 7 key findings to assist in delivering positive results and reducing risk for digital government. These lessons demonstrate how agencies can move from traditional command-and-control implementation, and toward an emphasis on business outcomes delivered in short increments with continuous improvement in the face of inevitable change.

This framework, the subject of congressional testimony and an influence on government policy and practice, recommends seven actions for effective digital transformation based on lessons learned—many of which echo key findings described throughout this chapter.

- **Stakeholder commitment and collaborative governance:** Most complex programs involve numerous stakeholders at political, policy, and management levels, and often multiple agencies, contractors, and other non-government constituencies. These players should have clear roles and responsibilities, and engage key stakeholders. Finally, there should be a shared commitment to the program's outcomes.
- **Skilled program manager and team:** An accountable, qualified, and properly positioned senior leader of the team should be highly proficient at technical, business (both government and commercial business process), organizational, programmatic, and interpersonal levels.

- **Systematic program reviews:** Governance leaders and the program manager should review progress in achieving key results on a regular basis. As part of these reviews, success should be celebrated and actual or potential problems promptly and openly identified for correction. This will promote timely consideration of whether the program is making rapid progress and minimizing risk.
- **Shared technology and business architecture:** Major IT programs involve complex interfaces with internal and external users, back-end applications, operational processes, policies, and supporting infrastructure. A business and technology architecture should guide activities across the team.
- **Strategic, modular, and outcomes-focused acquisition strategy:** The program manager must collaborate with the acquisition organization and other stakeholders, and then work with the private sector early on, to define a set of strategic requirements, a program management model that relies on incremental improvements, and an acquisition strategy that supports the program's outcome-based goals.
- **Software development that is agile:** Applications should be developed in an iterative fashion whenever possible, with small-scale rollouts, frequent feedback from end users, and communication with program management and governance leaders on changes. This approach reduces risk and increases the chances for program success.
- **Security and performance testing throughout:** Software modules should be tested and released in phases throughout design, development, and operations—both for individual components and collective system performance.

LOOKING FORWARD

For digital technology to transform operations, governments will also need to change both culture and policy. To take full advantage of the transformational changes made possible through the speed and scale of digital technologies, citizens must help drive how agencies work with them. Digital government in the future must adapt to the needs and expectations of citizens, businesses, non-profits, and other partners, creating user experiences that are personalized, interactive, and easy to access and use. Digital technologies can enable "cognitive systems" that help agencies understand, reason, and learn, allowing government to interact in real time with the public to deliver mission and mission support services with strong security and privacy protections.

Ultimately, new technologies will continue to help government drive performance improvements based on leveraging data and analytics over the cloud, in a secure manner, and in real time—emerging technologies that include artificial intelligence, blockchain, the internet of things, and initial steps toward quantum computing. Early innovators have shown a path for agencies to move forward in engaging with and serving the public. For

example, two 2018 reports on artificial intelligence—*The Future Has Begun: Using Artificial Intelligence to Transform Government*[56] (published with the Partnership for Public Service) and *Delivering Artificial Intelligence in Government: Challenges and Opportunities*[57] by Kevin DeSouza—highlight visible progress in the adaptation of that revolutionary technology to government at all levels—federal, state, local, and international.

The evolution of digital government over the past two decades shows that when implemented effectively, securely, and with cost-effective approaches, agencies can drive significant and positive change while managing risk to the government and the taxpayer. As discussed in Part II, government in the next twenty years can act responsibly to accelerate this progress.

Daniel J. Chenok *is Executive Director of the IBM Center for The Business of Government, where he oversees all of the Center's activities in connecting research to benefit government. He serves in numerous industry leadership positions, with organizations that include the Partnership for Public Service, the National Academy of Public Administration, and the Senior Executives Association. His previous positions included Chair of the Industry Advisory Council (IAC) for the government-led American Council for Technology (ACT). As a career government executive, Mr. Chenok served as Branch Chief for Information Policy and Technology with the Office of Management and Budget.*

Endnotes

1 Kevin Desouza, *Delivering Artificial Intelligence in Government: Challenges and Opportunities,* IBM Center for The Business of Government, 2018.

2 Jane Fountain, *Building the Virtual State* (Washington, DC: Brookings Institution Press, 2001).

3 U.S. Federal CIO Council, *State of Federal Information Technology Report*, January 2017, https:www.cio.gov/sofit.

4 *The Privacy Act of 1974*, Public Law 93-479, 5 U.S.C. 552(a), Dec 31, 1974.

5 *The Paperwork Reduction Act of 1995*, Public Law 104-13, May 22, 1995.

6 *The Computer Security Act of 1987*, Public Law 100-235, June 11, 1987.

7 *The Clinger Cohen Act of 1996*, Public Law 104-106, Feb 10, 1996.

8 Diana Gant and Jon Gant, *State Web Portals: Delivering and Financing E-Service*, IBM Center for The Business of Government, 2002, 3.

9 Genie Stowers, *The State of Federal Websites: The Pursuit of Excellence*, IBM Center for The Business of Government, 2001, 8.

10 France Belanger and Janine Hiller, *Privacy Strategies for Electronic Government*, IBM Center for The Business of Government, 2001, 6.

11 Stephen Holden, *Understanding Electronic Signatures: The Key to E-Government*, IBM Center for The Business of Government, 2004.

12 *Electronic and Information Technology*, Section 508 of the Rehabilitation Act of 1973, as amended, 29 U.S. Code §794d, 1998.

13 *The E-Government Act of 2002*, Public Law 107-347, Dec 17, 2002.

14 Cynthia Farina, *Rulemaking 2.0: Understanding and Getting Better Public Participation*, IBM Center for The Business of Government, 2013.

15 Stephen Holden, *A Model for Increasing Innovation Adoption: Lessons Learned from the IRS e-file Program*, IBM Center for The Business of Government, 2006.

16 Marc Holzer, James Melitski, Seung-Yong Rho and Richard Schwester, *Restoring Trust in Government: The Potential of Digital Citizen Participation,* IBM Center for The Business of Government, 2004, 3.

17 M. Jae Moon, *State Government E-Procurement in the Information Age: Issues, Practices, and Trends*, IBM Center for The Business of Government, 2002; and Mita Marra, *Innovation in E-Procurement: The Italian Experience*, IBM Center for The Business of Government, 2004.

18 *Federal Information Security Modernization Act of 2014*, Public Law 113-283, Dec 18, 2014.

19 George W. Bush, HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.

20 The White House, *National Strategy for Trusted Identities in Cyberspace*, April 2011.

21 U.S. Office of Management and Budget, *M-18-XX (Draft, as of April 6, 2018) Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management*.

22 Beth Noveck and Stefaan Verlhust, *Encouraging and Sustaining Innovation in Government,* IBM Center for The Business of Government, 2016.

23 The White House, *Transparency and Open Government*, January 21, 2009.

24 Phillipe Kruchten and Paul Gorans, *A Guide to Critical Success Factors in Agile Delivery,* IBM Center for The Business of Government, 2013.

25 Jacob Parcell, "Making Mobile Gov Project," *DigitalGov*, published June 21, 2011. https://www.digitalgov.gov/2011/06/21/making-mobile-gov-project.

26 Bob Brown, "Mobile Apps Still Have a Long Way to Go in State Governments: But Arkansas Stands Out with Gov2Go Mobile App" *Networked World*, September 21, 2016.

27 Sukumar Ganapati, *Using Mobile Apps in Government*, IBM Center for The Business of Government, 2016.

28 David Wyld, *Moving to the Cloud: An Introduction to Cloud Computing in Government*, IBM Center for The Business of Government, 2009.

29 The White House, *Federal Cloud Computing Strategy*, February 8, 2011.

30 The White House, *Federal Cloud Computing Strategy*.

31 FedRAMP, accessed May 25, 2018, https://www.fedramp.gov.

32 Sujatha Perepa, "Why the US Government is Moving to Cloud Computing," *Wired.com*, (September 2013).

33 Shannon Tufts and Meredith Weiss, *Cloudy with a Chance of Success*, IBM Center for The Business of Government, 2013.

34 Paul Wormeli, *Mitigating Risks in the Application of Cloud Computing in Law Enforcement*, IBM Center for The Business of Government, 2012.

35 Digital Gov, "2012 Digital Government Strategy." Accessed June 20, 2018, https://digital.gov/resources/2012-digital-government-strategy.

36 The White House, *25 Point Implementation Plan to Reform Federal Information Technology Management*, December 9, 2010.

37 Presidential Innovation Fellows, accessed May 25, 2018, https://presidentialinnovationfellows.gov.

38 Noveck and Verhulst, *Encouraging and Sustaining Innovation in Government,* 20.

39 General Services Administration, 18F, accessed May 25, 2018, https://18f.gsa.gov.

40 Adam Mazmanian, "GSA Launches Digital Incubator," *Federal Computer Week* (March 19, 2014).

41 Alyssa Black and Rachel Burstein, *A Guide to Making Innovation Offices Work*, IBM Center for The Business of Government, 2014, 4.

42 The U.S. Digital Service, accessed May 25, 2018, https://www.usds.gov.

43 Ines Mergel, *Digital Service Teams: Challenges and Recommendations for Government,* IBM Center for The Business of Government, 2017, 6.

44 "Digital Services Playbook," The U.S. Digital Service, accessed May 25, 2018. https://playbook.cio.gov.

45 *Federal Information Technology and Acquisition Reform Act*, Public Law 113-291, December 19, 2014.

46 U.S. Office of Management and Budget, *M-15-14: Management and Oversight of Information Technology*, June 10, 2015.

47 *Cybersecurity Enhancement Act of 2014*, Public Law 113-274, December 18, 2014.

48 *Cybersecurity Workforce Assessment Act*, Public Law 113-246, December 18, 2014.

49 Kevin DeSouza, *Creating A Balanced Portfolio of IT Metrics*, IBM Center for The Business of Government, 2014, 8.

50 Greg Dawson and James Denford, *A Playbook for CIO-Enabled Innovation in the Federal Government*, IBM Center for The Business of Government, 2015.

51 *National Defense Authorization Act for Fiscal Year 2018*, Title X, Subtitle G, Public Law 115-91, January 3, 2017.

52 "Cross-Agency Performance Goals," Performance.gov, accessed May 25, 2018, https://obamaadministration.archives.performance.gov/cap-goals-list.html.

53 "Modernize IT to Increase Productivity and Security," Performance.gov, accessed May 25, 2018, https://www.performance.gov/CAP/CAP_goal_1.html.

54 Greg Dawson, *A Roadmap for IT Modernization in Government*, IBM Center for The Business of Government, 2018.

55 ACT-IAC, *Key Success Factors for Major Programs that Leverage IT: The '7-S for Success' Framework*, May 2014.

56 IBM Center for The Business of Government and Partnership for Public Service, *Using Artificial Intelligence to Transform Government*, 2018.

57 Kevin Desouza, *Delivering Artificial Intelligence in Government: Challenges and Opportunities*, IBM Center for The Business of Government, 2018.