The State of Federal IT Report

> We were at or about to enter a critical inflection point not only with IT, but with the Federal government as a whole. It was this digitization point. It was going to be disruptive and painful, and filled with hard challenges along the way. I had no idea that OPM would happen or any of those things, but in my head I could imagine those kinds of problems were things that would come up. As I was talking to folks, I was told if you are interested in this field and wanted to work on hard problems, this is the right place. You will be successful or it will kill you.
>
> — Federal CIO Tony Scott
> Management of Change Conference, May 2016

Introduction

On January 20, 2017, the new administration and its appointees assume office. Among these appointees are approximately one-third of the CIO Council's members (agency CIOs) and the Chairperson. The CIO Council, codified by the E-Government Act of 2002, serves as a forum for agency CIOs to share leading information technology (IT) practices and develop recommendations for Federal IT leaders.

We're at a crossroads - opportunities abound, but so do challenges and outside threats. Our IT infrastructure supports all aspects of government operations and how we respond to these challenges and embrace these opportunities will determine the effectiveness of our government for years to come. Over the last decade, there has been significant progress towards improving Federal IT across the government. However, this remains an ongoing effort.

The CIO Council's State of Federal Information Technology (SOFIT) report frames the landscape, illuminates the problems, and provides potential solutions. In addition, it provides recommendations on a variety of initiatives in order to improve Federal IT. While the observations and analysis in this report are based, in part, from interviews of the Council's member CIOs, their opinions do not necessarily represent a government-wide consensus position - individual agency experiences vary. The recommendations and findings from this report will help illuminate a path forward for the CIO Council in the coming years.

How We Got Here

When Federal agencies first adopted information technology, computers provided limited ability to radically change an organization's underlying business processes. Instead, computers, mainframes, and software were used to automate and enhance existing business processes. For example, rather than having an employee manually perform data quality checks, early IT enabled automated checks that minimized mistakes and saved time.

While the adoption of information technology created new efficiencies, it also posed new challenges to agencies. In a 1994 report that may as well have been written today, the Senate Governmental Affairs Committee (now the Senate Homeland Security and Governmental Affairs Committee) reported on challenges adopting IT in the Federal government. The report, titled *Computer Chaos*, identified examples of agencies struggling to adopt IT to perform basic functions, such as automating manual processes and hesitating to use commercial off the shelf (COTS) software because of a belief it was not suited to the existing tasks. The findings of this report spurred the creation of the Clinger-Cohen Act in 1996, which first defined the role of the agency CIO.

> *"Compared to the private sector, the government spends too much time and effort developing unique software programs and hardware rather than buying commercially available products."*
>
> — Computer Chaos (1994)[1]

Over the last two decades, there have been improvements in the management, procurement, and development of Federal IT. Despite these efforts, many legacy systems still exist throughout the government. Over time, agencies may have modernized the technological components of systems, but rarely did these efforts accompany a larger scale business process re-alignment. These decisions, which seemed reasonable at the time, built upon one another over the years, creating a gap between the business process and the technology available. This resulted in inefficiencies and an inability for agencies to take full advantage of advancements in technology. By replacing these legacy systems with a modern technological solution and a digital-focused business process, we can harness true transformational change and fully leverage the benefits of these improvements.

The speed of today's technology enables us to make decisions about improving processes in ways previously thought impossible. Accomplishing all of this change, however, requires a holistic look at how agencies approach IT - there are significant challenges that need to be overcome in hiring and retaining the right workforce, managing acquisitions, and how agency leadership perceives the role of IT. We've reached a point where we need to invest the time and money necessary to transform the way we do business in the government. Otherwise, our current path will continue to become increasingly unsustainable. CIOs, and the rest of an agency's leadership, need to play a key role in driving this transformation.

Road to Transformation

The rapid transformation of how Americans interact with businesses, news, entertainment, and other services has radically raised their expectations of how they interact with government. Lengthy paperwork, cumbersome processes, and organizations centered around procedures and tradition are no longer acceptable in the eyes of the people.

The importance of changing how government views and manages information and information technology cannot be understated. No longer can federal IT be seen as merely a back-room function and the management of government information relegated to a low-level priority. Federal agencies must adapt to the modern, digital world.

Understanding the Challenge

Integrating technological advancements that fundamentally transform private and public life can be difficult. Take, for instance, the advent of the automobile and the impact it had on cities. Prior to automobiles, roads and paths were carved out for pedestrian traffic, horses, and horse-drawn carts - the existing transportation at that time. Over time, to accommodate increasing amounts of automobile traffic, these cities began paving their historically narrow “legacy roadways.” Though these decisions may have been right at the time, 100 years later, we are dealing with unexpected navigation challenges and an ever increasing amount of time spent in traffic.

To move beyond these “legacy roadways”, cities like Boston are facing costly improvements, such as the Big Dig, to update their legacy infrastructure to meet modern transportation needs. In comparison, we can look to cities built primarily after the automobile became ubiquitous. A city like Denver did not have “legacy roadways” to modernize which allowed them to develop infrastructure with the automobile in mind.

In many ways, Federal IT faces a similar dilemma - how to modernize its legacy systems and the underlying business processes alongside it.

In comparison to the challenges that we face in Federal IT, we can look to the country of Estonia, which gained its independence in 1991 after the fall of the Soviet Union. Estonia had the opportunity to create a digital-centric government from the ground-up, leveraging significant online presence and interaction, including allowing citizens to vote over the Internet.[2] We do not have that same opportunity, and, as a result, must walk a more difficult path to transform the way we do business.

Achieving Transformative Change

Agency CIOs must play a pivotal role in leading the transformation of Federal IT - it is not enough for the CIO to just have a "seat at the table." CIOs must be fully integrated, as an independent stakeholder, into all the elements of the agency's process for developing and delivering IT investments.

The CIO must sit at the intersection where the technology and the business of the agency meet.

A fully integrated CIO has the ability to view common business challenges across the entire agency and use that knowledge to provide solutions that drive efficiency and scale. Too often we see business challenges as unique, but many challenges we face are more common than we realize. The CIO's ability to analyze solutions across the organization allows for agency- or government-wide tools and technologies that enable us to solve persistent challenges.

The changes required to move to a digital government will significantly impact every Federal agency and its employees. The next decade will bring increasingly complex challenges but these challenges are not insurmountable. The path to a successful IT future is possible through better internal collaboration, improvements to human resources and procurement operations, a shift away from legacy systems, and a continued push towards transparency and open data. Such a transformation will require changes to both culture and policy.

This transformational change requires CIOs to think beyond their traditional roles and responsibilities, about their place in the broader Federal IT ecosystem. Building relationships outside of the agency will be critical to identify common challenges and solutions. The government-wide CXO Councils can help agencies leverage the experiences of others to avoid duplication and wasted effort.

Improving Visibility into IT Spending

Progress has been made towards using data to make better decisions in government. For example, in May 2014, the Digital Accountability and Transparency Act (DATA Act) was enacted, requiring agencies to publicly disclose detailed information on Federal spending. The law also required OMB to create a set of data standards in order to define how this data is reported.

In addition, the CIO Council is working to improve transparency through the Technology Business Management (TBM) taxonomy effort. Today, agencies spend roughly three-quarters of their IT budgets on maintaining current systems. By implementing the TBM taxonomy, agencies can better model and manage IT costs and services. Ultimately this will allow for improved evaluation of cost and performance and help decision-making on where and how to invest resources.

The effort to improve data quality and combine disparate data into a more usable form will aid the government in how to best utilize its own, existing data. The DATA Act and TBM efforts are just the initial steps towards helping agencies move towards a more data driven, digital, agile government. Ultimately, the goal is to make data useful, relevant, and actionable enabling decision makers to make better informed choices by acting on real, trustworthy information.

Structuring Policy to Enable this Change

Over the past six months, the project team conducted more than 45 interviews and undertook countless hours of research. A large portion of this work examined how the creation, implementation, and oversight of a policy or initiative can drive change across the Federal government. The focus of this effort was on leveraging lessons learned from previous initiatives to usher in this crucial transformation.

One of the key lessons learned is that policy is but one piece of a much larger puzzle. On its own, a policy or guidance can drive some changes, but true transformation will require a combination of well-crafted policies, sustained agency execution, and consistent oversight. Each of these pieces are equally important to achieve the changes needed in Federal IT.

The project team found several recent examples of these concerted efforts providing CIOs with an effective toolkit to drive change. First, agency CIOs frequently cited the Cyber Sprint, a short-term effort focused on a few key cybersecurity initiatives, as one of the more effective OMB and leadership led engagements. Second, CIOs cited OMB's guidance on the Federal IT Acquisition Reform Act (FITARA) for allowing agencies to focus on outcomes and characteristics intended, instead of prescribing specific activities. However, agency implementation of FITARA is still ongoing. OMB and agencies have significant work to do to ensure that the changes required by FITARA result in positive IT outcomes. These recent efforts, and others examined by the project team, provide evidence of key attributes for successful policy engagement:

Policy implementation is a team sport

No policy lives in a vacuum. Policymakers need to be cognizant of the impact policies have on other management functions. Policymakers should identify how CXO partners can engage in implementation and execution and define those responsibilities at the outset.

Outcome-focused objectives

All policy guidance should leverage an outcome-focused approach. By highlighting descriptions of end-state or specific performance metrics instead of mandating prescribed actions, policymakers can provide flexibilities for agencies to implement policy in a way that best aligns with their mission. Recent guidance from OMB on data center optimization efforts provides a potential model for creating outcome-oriented requirements.

Customer-centric development process

Agencies should make significant contributions to the policy development process. By ensuring that agencies have significant early buy-in, policymakers will increase the level of understanding of the policy requirements. Early engagement may also identify innovative approaches already underway and scale them for use by other agencies.

Actionability

Agency engagement in the creation of a policy can help ensure that any requirements are grounded in a firm understanding of how they can be implemented. Policymakers should align requirements with achievable outcomes and built on an understanding of the agencies' current state. Execution of certain policy requirements should happen quickly and efficiently. Whole-scale reinvention by agencies need not be the default for all efforts.

Follow-through is critical

Though the creation of a policy alone can bring about change, it is usually insufficient. An agency's implementation and the associated oversight of that policy is just as important, if not more so, than the policy itself. If policymakers disconnect from the implications of their activities, agencies will feel uncertain about how to best utilize their resources to comply with the requirements. By focusing on sustained senior level engagement, feedback loops, a clearly defined strategic vision, and a targeted set of policy actions, execution becomes the focus. Ultimately, a "fire and forget about it" approach to policies and initiatives can do more harm than good.

Strategic integration

Organize policies, laws, regulations, and guidance around strategic objectives. New policies overlaid on the large volume of existing material can easily create conflicts or complications with existing policies and initiatives. Efforts to understand what already exists can minimize these potential risks and better target policies towards filling identified gaps. Similarly, policymakers should ensure that outdated policies are sunset or rescinded appropriately. Recent efforts underway to identify, catalog, and organize the library of existing OMB policies can provide the necessary foundation to these efforts.

Measurability

"What gets measured, get's done." Metrics and data collection (both their development and their consistency) drive performance. Consistent, business-oriented metrics create meaningful data for agencies to evaluate and enhance their performance. On the other hand, inconsistent metrics, unclear definitions, or metrics that do not align to the business create a compliance culture that ultimately inhibits performance. The development of data center definitions under early data center consolidation efforts exemplifies this. In that instance, the ever-changing metrics resulted in increased compliance costs or forced agencies to restart or revise their efforts again and again. At the end of the day, realizing successes and opportunities from early data center policies became difficult for agencies.

Willingness to learn from mistakes

Adopt the 'fail fast' attitude of modern IT practices to the policy development and oversight process. Efforts to develop policy should focus on relevant and targeted actions to guide agencies. If circumstances change, policymakers should pivot and change their approach in order to deliver the best value to the taxpayers.

Leadership Drives Change

Policies can help drive progress and teach us valuable lessons about how to achieve success. However, policies alone cannot transform government - even if they are perfect. Federal IT leaders need to resist the urge to immediately draft a new policy every time a challenging situation appears. If, instead, leaders turn to existing authorities and strive to execute fully and build effective relationships, accomplishing significant change can happen without the need for new policies or initiatives. True change relies on strategic leaders who can capitalize on bold ideas and remain dedicated to seeing them through. As we continue into this digital era of government, leaders must continue to harness the tremendous power of IT to provide economies of scale, create efficiencies, and disrupt traditional processes.

Current Federal IT Landscape

The current Federal IT landscape is broad and diverse, with many key players and a budget for Fiscal Year (FY) 2017 of more than $80 billion. Technology is at the heart of every government program, whether it be back-end hosting, internal systems management and communications, or customer-facing digital channels. The public relies on this infrastructure everyday to interact with the Federal government and draw on its services. Below are some of the most visible players in the Federal IT community.

Federal CIO

Leading this effort is the Federal Chief Information Officer (CIO) who has the formidable task of overseeing technology policy, strategic planning, and technology investments for the entire Federal government, and ensuring that these investments help agencies meet their mission and goals in a secure, reliable, and cost-effective way.

The next Federal CIO should focus on a broad array of objectives including:

1. Ensuring the highest value in IT investments;
2. Expanding and improving digital services;
3. Emphasizing cybersecurity for Federal IT assets and information; and
4. Training and developing the IT workforce.

These core objectives lay the foundation for how agencies should view their IT programs, projects, and requirements under existing law and will present both opportunities and challenges to the next Federal CIO on day one.

Office of Management and Budget

The Federal CIO heads the Office of the Federal CIO (OFCIO) within the Office of Management and Budget (OMB) in the White House (note, the OFCIO is also known as the Office of E-Government and Information Technology). OFCIO's role is to develop IT policy and help agencies implement and operationalize those policies. They also play an oversight role in determining benchmarks and working with agencies to measure success. Over the last decade, Federal IT policies focused on boosting IT security, encouraging use of shared services and the cloud, and strengthening the role of the agency CIO.

Agency CIOs

The role of the agency CIO is broad and challenging. To be successful, agency CIOs need proper authority and oversight of the agency's IT portfolio. They must also understand the language of their agency's mission and leadership to provide clear insight and effective IT solutions to meet agency business needs.

Differing levels of authority over IT-related investment and spending have led to inconsistencies in how IT is executed from agency to agency. For those agencies where the agency CIO has broad authority to manage all IT investments, great progress has been made to streamline and modernize the agency's IT footprint. For the others, where

agency CIOs are only able to control pieces of the total IT footprint, it has been harder to achieve improvements.

CIOs continue to face a host of challenges ranging from budget shortfalls, large legacy IT portfolios, ever-increasing cybersecurity threats, and difficulties in attracting and retaining top-tier talent in a highly competitive field. Many agency CIOs understand the need to tie together mission and business needs in order to secure funding for major IT investments.

C-Suite Agency Leaders

Across agencies, business leaders need to understand the importance of IT infrastructure. Without reliable, secure IT systems, most government programs would not be able to function or carry out their missions successfully. From the White House and OMB to agency management teams and C-Suite leaders who oversee budget, procurement and human resources, coordination is vital to success. Cooperation and strong working relationships amongst these key business leaders will allow for full line of sight into the entire operations of the agency and will facilitate a deeper understanding into the impacts of IT agency wide.

From a financial perspective, a holistic evaluation of the agency's IT portfolio can help eliminate duplication and waste. Common performance metrics should identify and illustrate whether IT processes and programs are efficient and effective in order to achieve mission success. Leaders across the agency must place a premium on strong, secure, reliable systems, and work together to ensure these systems are properly resourced to effectively meet agency needs.

The New Chiefs

The last few years have seen an increase in different "Chiefs" - Chief Technology Officers, Chief Data Officers, Chief Innovation Officers and the like - who were brought on to address specific challenges or to counter perceived gaps. These new chiefs joined CIOs and Chief Information Security Officers (CISOs) as part of the IT leadership, often in response to a perceived opportunity or business need at agencies.

However, unlike most CISOs, these new chiefs joined organizations in a disparate manner. Some, brought on at the behest of agency leadership, report directly to the Secretary or Deputy Secretary. In those instances, the CIO is often not included in the reporting structure. In other cases, these positions report directly to the CIO and are fully integrated into the overall IT leadership framework.

If the IT framework is fragmented, it can be more difficult for leadership to obtain an enterprise wide view of an agency. There needs to be one central point of accountability for the information and information technology of an agency and the most natural and logical position is the statutorily created Chief Information Officer. Agency CIOs need to be the focus point for agency IT activities and, working with senior agency leadership, must drive transformative changes in the way we do business.

These other chiefs are all part of this effort and their relationship to the CIOs needs to be more clearly defined as these roles become institutionalized. With a customer-centric CIO focused on aligning IT capabilities to achieving mission, these chiefs become natural partners. CTOs can provide the expertise on how to leverage modern technologies to transform the business process; CISOs provide risk-based approaches to improve security; and CDOs provide detailed analysis of data to inform decisions and communicate this to external stakeholders. A transformative CIO sits at the center of this effort, providing the strategic vision to ensure all of these parts work together seamlessly. In addition, the CIO needs to work closely with business leads to identify opportunities to leverage modern, digital solutions. IT is truly a team sport that requires an effective group of dedicated individuals to succeed.

Federal IT Workforce

The Federal IT workforce is the backbone of all of these technology efforts. Today, over 80,000 people hold the employment classification of "Information Technology Management." These individuals work to build, operate, manage, and make policy for IT organizations across the government. With the number of retirement-eligible Federal employees increasing every day, new talent must be hired into the government in order to handle constantly evolving tools and technologies. Recruiting new Federal employees and ensuring that existing personnel receive the right training and have the right tools to make use of new technologies needs to be at the forefront of the IT workforce efforts.

Government-wide IT Agencies

There are several Federal agencies with responsibilities for security, policy, and oversight of government-wide IT efforts. These organizations, along with OMB and the White House, play a major role in setting the landscape and direction for IT initiatives.

General Services Administration (GSA)

GSA has three main offices that support various centralized IT functions for the Federal government. The Office of Government-wide Policy (OGP) provides support and guidance to agencies to help them comply with Federal IT requirements in areas such as security and authentication, accessibility, and data center optimization. OGP also supports the Federal CIO Council and CIO.gov website. GSA's Technology Transformation Service (TTS) improves the public's experience with government by helping agencies build, buy, and share technology that allows them to better serve the public, through arms such as 18F. Finally, the Federal Acquisition Service (FAS) helps agencies leverage common procurement vehicles in order to achieve cost efficiencies via volume discounts and leveraging best practices.

Department of Homeland Security (DHS)

DHS plays a major role in the Federal government's cybersecurity efforts. Within the National Protection and Programs Directorate, the agency houses the National Cybersecurity and Communications Integration Center (NCCIC), which provides 24/7 situational awareness, incident response, and management of cybersecurity communication for the Federal government, intelligence community, and law enforcement. The United

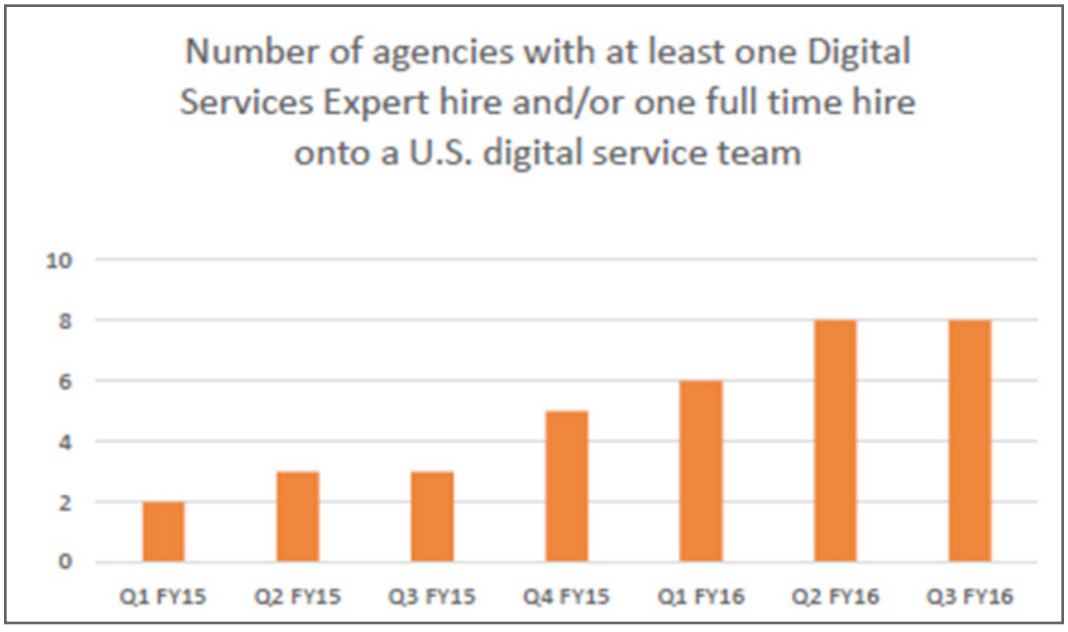
States Computer Emergency Readiness Team (US-CERT) is a core branch of NCCIC, bringing advanced network and digital media analysis expertise to bear on malicious activity targeting the nation's networks. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered Federal agencies.

National Institute for Standards and Technology (NIST)

NIST, a component of the Department of Commerce, is a technically oriented organization charged with developing standards and guidelines for non-national security Federal information systems, in coordination with OMB and other Federal agencies. Although NIST standards for Federal systems are mandatory for agencies to implement, NIST itself does not have an oversight role and does not assess security implementation status. OMB works closely with NIST in updating policies and issues numerous publications to help guide agencies in their IT implementation. One of the most important of these is the 800 series of special publications, which provide requirements and guidelines for information system security across the Federal space. As an example, NIST SP 800-53 outlines a Risk Management Framework for security control selection for all Federal information systems that incorporates common technical standards.

18F and USDS

In 2014, both GSA's 18F and the White House's U.S. Digital Service (USDS) were established. Both organizations are largely composed of experienced developers, engineers, designers, and managers who leverage innovative approaches and best practices from successful digital services companies for projects within Federal agencies. In conjunction with the establishment of 18F and USDS, OMB partnered with OPM to develop a "digital services expert" job description for use by agencies to attract and recruit private sector talent.



USDS also emphasizes training programs and tools to enable Federal contracting officers to apply industry best practices to digital procurements and serve as expert advisors to their CIOs on procurements. For example, USDS piloted a new Digital Service Contracting Professional training program designed to teach agency contracting officers about how to better support and enhance IT procurements to leverage modern digital practices. In addition to developing new talent and supporting agency services, USDS also demonstrates modern practices: applying user-centered design framework and using agile software development practices in government.

18F partners with agencies for a fee. The team provides acquisition services, builds shared technology platforms that can be used across government, and provides training. 18F has also developed a number of government-wide shared platforms such as cloud.gov, a government-wide cloud platform. These platforms have helped its digital services experts (as well as those at USDS and agencies) to work more efficiently and effectively, accomplish common tasks in a repeatable fashion, or address long-standing policy or technology obstacles.

Oversight

Congress, the Government Accountability Office (GAO), and Inspectors General (IGs) at each agency provide important oversight of how Federal agencies spend money and allocate resources. Congress oversees the activities of the Executive Branch and Federal agencies through its Committees and their hearings. Specifically, the House Oversight and Government Reform Committee and the Senate Homeland Security and Governmental Affairs Committee have general jurisdiction over the entire Federal government in order to evaluate the efficiency and effectiveness and ensure the accountability of all agencies and departments. GAO supports Congress by auditing and analyzing agency operations, analyzing programs, and investigating illegal activity. Where GAO has a government-wide role, agency IGs perform similar oversight functions focusing solely within the agency itself. Ultimately, the oversight role strives to ensure that Americans are getting the most from their taxpayer dollars.

Notes

1. https://acc.dau.mil/adl/en-US/22163/file/2121/Cohen%20Computer%20Chaos%201994.pdf
2. http://www.wired.co.uk/article/digital-estonia