

# State of Federal Information Technology



January 2017

## About the Report

The State of Federal IT report represents more than six months of work by the Federal CIO Council (CIOC), in partnership with GSA's Office of Government-wide Policy (OGP), to provide an independent, comprehensive analysis of the current Federal IT environment. The CIOC and OGP provided the core project management team and enlisted the support of a liaison from the Office of the Federal CIO to provide data and relevant artifacts and to facilitate the research for the report.

The CIOC enlisted the support of two contractor teams to create content for the report. The first team of REI Systems, Inc., and Incapsulate, LLC, focused on the perspectives of Federal agencies and a detailed analysis of the current policy landscape. The second team, Gartner, Inc. focused their research on how to leverage lessons learned and leading practices from organizations outside the Federal space.

To carry out their research, the teams conducted more than 45 interviews with agency CIOs, the Federal CIO and DCIO, and Federal CISO and DCISO, and numerous other Federal IT leaders. Underpinning these interviews was rigorous policy analysis, evaluation of publicly available agency IT strategy documents such as Information Resource Management plans, and review of public reports/data on Federal IT such as the IT Dashboard.

## Acknowledgements

This report would not be possible without the tireless efforts of REI Systems, Inc; Incapsulate, LLC; and Gartner, Inc. who developed the report's content; the staff of the Office of the Federal CIO for their feedback and contributions; and the CIOs and other IT leaders who provided their candid perspectives. And a special thanks to Eagle Hill Consulting for their invaluable efforts in pulling together the final formatting and design for large portions of this report.

### State of Federal IT Federal Project Team

Trey Kennedy, CIO Council

Jonathan Kraden, GSA OGP

Mindy Levit, GSA OGP

Laura Szakmary, GSA OGP

Justin Grimes, OMB OFCIO

# 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)<sup>1</sup>

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.<sup>2</sup> 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

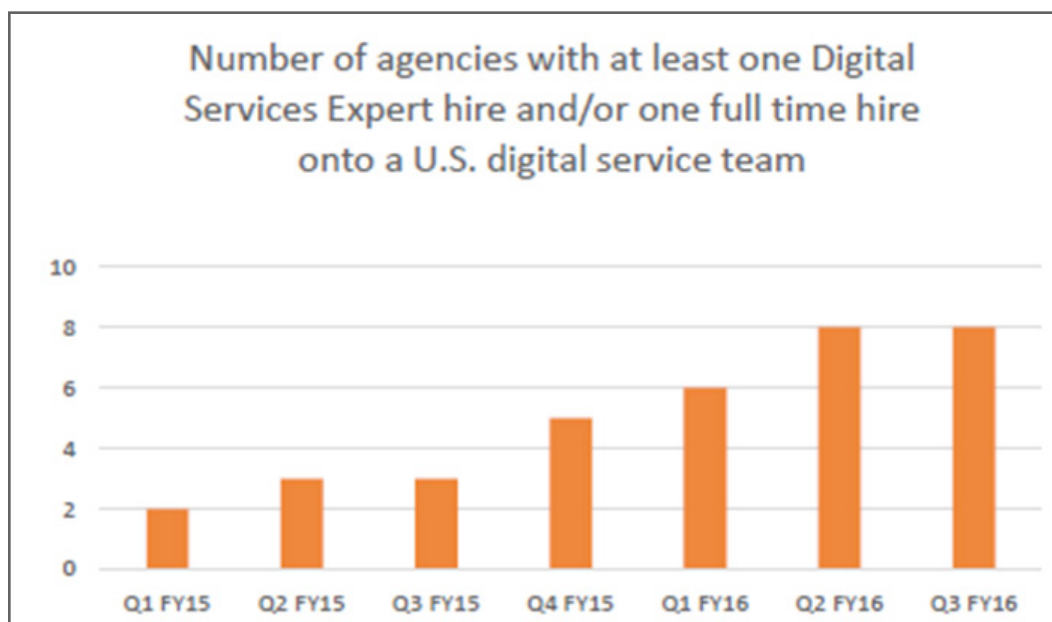
States Computer Emergency Readiness Team (US-CERT) is a core branch of NCCIC, bringing advanced network and digital media analysis expertise to bear on malicious activity targeting the nation's networks. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides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

# Policy Volume

## Introduction

The policy chapters in the State of Federal IT report provide an analysis of key government-wide IT policies, strategies, and initiatives over the last decade. Beginning with a list provided by the Federal CIO Council (CIOC),<sup>1</sup> the scope was then widened to include a total of 188 statutes, executive orders, presidential directives, and Office of Management and Budget (OMB) memoranda, circulars, strategies, and guidance.<sup>2</sup> From this list, a subset of policies were chosen for analysis and were grouped into six distinct topics:

A.	Management and Oversight of IT
B.	IT Infrastructure Modernization
C.	Open Data and Open Government
D.	Federal Shared Services
E.	Cybersecurity
F.	Acquisition and Contracts Management

Each topic is discussed in a subsequent chapter, broken down into the following sections:

### **Summary**

A list of high-level observations about the policy area

### **Overview**

A summary of the policy area, including history, goals, major terms, and definitions

### **Policy Evolution**

A list of significant strategies and initiatives related to the policy area, including a narrative description, and the key strengths, challenges, and impact of each

### **Evaluating Metrics**

A description of the primary objective(s) for a policy area, as well as examples of metrics and oversight methods

### **Agency Observations and Findings**

A series of short narratives designed to highlight agency perspectives on specific government-wide policies and initiatives. Findings can include opportunities for improvement as well as success stories and best practices<sup>3</sup>

## Other Key Policy Information

### Cross-Agency Priority Goals and PortfolioStat

OMB has used a number of mechanisms to evaluate agency performance on IT initiatives, including the Cross Agency Priority (CAP) Goals. To speed progress on cross-government collaboration and tackle government-wide management challenges affecting most agencies, OMB created the CAP Goals in February 2012.<sup>4</sup> CAP Goals are a subset of Presidential priorities and complement other cross-agency coordination and goal-setting efforts. A number of IT-related CAP Goals track agency commitments and key performance indicators over multiple years, with quarterly updates posted publicly.

The other mechanism is PortfolioStat, which has been the primary agency oversight mechanism for the Office of the Federal CIO (OFCIO) since 2012. PortfolioStat is an examination of an agency's entire portfolio of IT investments. Progress is measured using key performance indicators (KPIs) evaluating major policy priorities. KPIs provide "high-quality, targeted data on the maturity of agency portfolios, as well as strategic, architectural, and asset inventory information."<sup>5</sup> The KPIs used in PortfolioStat have varied over the years, in part reflecting changes in government-wide policies and priorities from year to year. The following figures summarize the reuse of KPIs, and the usage of other metrics during the same time period.

Figure Pol-1 is based on an analysis of PortfolioStat Briefing Books, provided by OFCIO, from every year and illustrates the changes in KPIs from year to year. As shown below, many KPIs (50 out of 64, or 78%) only appear in one Briefing Book and are not reused in future books.

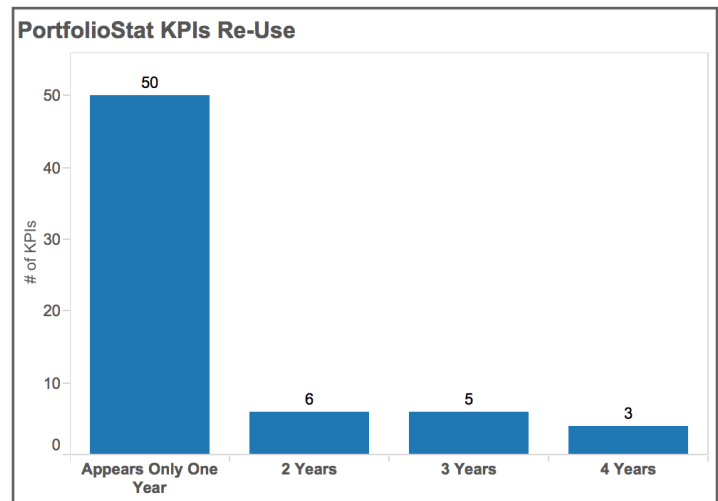
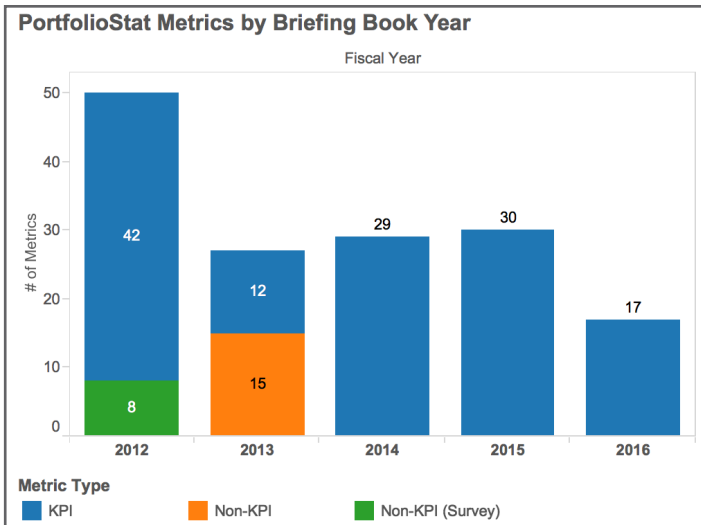


Figure Pol-1: PortfolioStat KPIs, Reuse Year to Year, FY 2012 - FY 2016

While there are valid reasons a particular metric or KPI may change or shift from year to year, the fact that nearly 80% of PortfolioStat KPIs do not appear more than once has likely impacted the ability of agencies and OMB to benchmark progress in certain policy areas. A full list of the PortfolioStat KPIs used from FY 2012 through FY 2016, broken down by both policy area as well as specific policy efforts being measured, is provided in the Appendix.



In addition, some years of PortfolioStat Briefing Books include quantitative data not marked as KPIs. For example, the FY 2012 Book included eight (8) responses to survey questions and the FY 2013 Book included other data that were not identified as KPIs.



## Government-wide Policy Focus: Agency vs. Bureau

OMB policies and oversight typically focus on engaging with the headquarters of agencies. In turn, an agency CIO then works internally with bureau IT counterparts and other leadership to ensure implementation of a policy or initiative across the entire agency.

However, because of the size and independence of some bureaus in their agencies, many CIOs face challenges coordinating policy priorities or requirements across an agency. A larger or more politically important bureau will more likely have their own direct relationship with agency leadership and members of Congress, or significantly different mission and operational needs from the rest of the agency. As a result, many CIOs do not have the ability to push Administration priorities down into the lower levels of the agency.

In fact, some agency bureaus are actually larger and have bigger IT budgets than whole agencies with whom OMB engages directly. For example, OMB holds a PortfolioStat session with the Department of Education, but not with the leadership of U.S. Customs and Border Protection (CBP), even though CBP spends twice as much as Education on IT per year (see table on following page).

It is critically important that Federal policymakers and agency leadership familiarize themselves with the different methods used for the oversight of government-wide strategies and initiatives. Additionally, an equally strong familiarity with the various agencies and bureaus will provide leaders with a more comprehensive viewpoint from which to drive towards successful outcomes.

The following policy chapters will provide additional context regarding the successes, failures, and opportunities for improvement in the execution of government-wide policy strategies throughout the wide variety of Federal agencies.

Bureaus and Agencies with Annual IT Spending > \$500 Million<sup>6</sup>

Bureau or Agency Name	Type	IT \$M
DOD (Agency)	Agency	30,780
HHS (Agency)	Agency	12,566
Bureau - Defense-wide (DOD)	Bureau	11,318
Bureau - Centers for Medicare and Medicaid Services (HHS)	Bureau	9,040
Bureau - Army (DOD)	Bureau	7,792
Bureau - Navy, Marine Corps (DOD)	Bureau	6,553
DHS (Agency)	Agency	6,204
Bureau - Air Force (DOD)	Bureau	5,117
VA (Agency)	Agency	4,403
Treasury (Agency)	Agency	3,940
DOT (Agency)	Agency	3,507
USDA (Agency)	Agency	3,418
Bureau - Federal Aviation Administration (DOT)	Bureau	3,054
Justice (Agency)	Agency	2,699
Bureau - Internal Revenue Service (Treasury)	Bureau	2,449
Commerce (Agency)	Agency	2,312
State (Agency)	Agency	1,966
Bureau - U.S. Customs and Border Protection (DHS)	Bureau	1,672
Energy (Agency)	Agency	1,655
SSA (Agency)	Agency	1,501
NASA (Agency)	Agency	1,361
Interior (Agency)	Agency	1,121
Bureau - Food and Nutrition Service (USDA)	Bureau	1,084
Bureau - General Administration (Justice)	Bureau	933
Bureau - Federal Bureau of Investigation (Justice)	Bureau	896
Bureau - Citizenship and Immigration Services (DHS)	Bureau	850
Bureau - National Institutes of Health (HHS)	Bureau	828
Bureau - Fiscal Service (Treasury)	Bureau	827
Bureau - Office of Chief Information Officer (USDA)	Bureau	786
Bureau - National Protection and Programs Directorate (DHS)	Bureau	775
Bureau - Administration for Children and Families (HHS)	Bureau	772
Bureau - Transportation Security Administration (DHS)	Bureau	751
Labor (Agency)	Agency	714
GSA (Agency)	Agency	710
Bureau - Bureau of the Census (Commerce)	Bureau	690
ED (Agency)	Agency	689
Bureau - National Nuclear Security Administration (Energy)	Bureau	675
Bureau - Food and Drug Administration (HHS)	Bureau	674
Bureau - U.S. Patent and Trademark Office (Commerce)	Bureau	665
Bureau - National Oceanic & Atmospheric Administration (Commerce)	Bureau	562
Bureau - Centers for Disease Control and Prevention (HHS)	Bureau	504

# Notes





1. Federal CIO Council. "IT Policy Library". <https://cio.gov/resources/it-policy-library/>
2. For a list of all policies, strategies, and initiatives examined as part of the report, see *Appendix A: Policies and Initiatives*
3. The primary source of information for developing these observations and findings was a series of interviews conducted throughout the Summer and Fall of 2016 with agency CIOs and DCIOs. For more information about these interviews and the agencies involved, please see *Agency Volume Introduction*
4. OMB first established a limited number of interim [CAP Goals] in February 2012 and released a new set of goals in March 2014. Performance.gov. "Frequently Asked Questions." <https://www.performance.gov/faq>
5. OMB M-13-09. "Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management." 3/27/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>
6. Federal IT Dashboard. <https://itdashboard.gov>. The agency totals are inclusive of all components at that agency. For example, the HHS total reflects all components, including CMS, resulting in CMS accounting for nearly 75% of the IT spend at HHS

# Management and Oversight of IT

I think FITARA presents a historic opportunity to reform the management of information technology across the Federal government. It is important that we do not underestimate the work and the commitment required by agencies and the broader ecosystem to fully implement this law. And the changes it represents in culture, governance, IT processes, business process, and quite frankly the way we do oversight. Simply replaying pages from our old playbook is not the solution.

— Federal CIO Tony Scott<sup>1</sup>

## Summary

 Cost	The Federal government has long struggled with acquiring, developing, and managing information technology (IT) investments. For example, although the Federal government spends over \$80 billion a year on IT, almost half (43%) of Federal IT projects reported on the IT Dashboard are over budget or behind schedule.
 Accountability	Budget, spending, acquisition, and management decisions are frequently made by programs or bureaus of an agency without any CIO visibility or input.
 Risk	In the wake of recent security breaches in the public and private sector, improving the government-wide cybersecurity posture is critical. However, inadequate coordination between agency CIOs and bureaus can impede the implementation of related initiatives.
 Policy	The Federal Information Technology Acquisition Reform Act (FITARA) can be used to further empower CIOs to be more fully integrated into all agency processes for developing and delivering IT investments. OMB's continued focus and oversight is critical to FITARA's success.

# Management and Oversight of IT

## Overview

Over two decades ago, then Senator William Cohen of Maine led an investigation into the Federal government's ability to manage its IT investments. The resulting 1994 report, entitled "Computer Chaos," could just as easily be written in 2016 and listed many of the same problems that Federal agencies face today - poor management of IT systems, wasted and duplicative investments, and billions of dollars spent on older, outdated, and expensive "legacy" systems.<sup>2</sup>

The Federal government continues to have a poor track record in acquiring, developing, and managing Federal IT investments. Individually, too many Federal IT projects run over budget, fall behind schedule, or fail to deliver on their promises. For example, in September 2016, the Federal IT Dashboard listed over 4,300 IT projects in 780 major IT investments across Federal government agencies. Nearly half (43%) of those projects were listed as over budget or behind schedule.

In addition to the challenges that agencies face in acquiring and developing specific IT investments, the stove-piped nature of many Federal agencies has led to a proliferation of duplicative IT investments. Many agencies manage their IT in a decentralized manner and Chief Information Officers (CIOs) have limited to no visibility into all of the IT

systems in their agency. As a result, agencies are unable to take an enterprise-wide view of their IT investments which frequently results in duplication, waste, and poor outcomes.<sup>3</sup> Too often, agencies, or components, seek to develop new solutions first, before assessing existing options, or identifying ways to achieve shared agency-wide IT solutions. For example, in 2012, OMB reviewed over 7,000 Federal agency IT investments that had been reported to OMB and found many potential redundancies and billions of dollars in potential savings that could be achieved through either consolidation or a shared approach to IT service delivery.<sup>4</sup>

To improve the management of IT across the Federal government, Congress and OMB have repeatedly attempted to empower the agency CIO to serve as the key leader for the management and oversight of agency IT systems. In 1996, Congress passed the Clinger-Cohen Act which, among other things, established the position of agency CIO.<sup>5</sup> This seminal piece of legislation also set forth OMB's overall responsibility for improving Federal IT, outlined detailed requirements for IT capital planning, investment control, performance, and results-based management. Several years later, the E-Government Act of 2002 reiterated the CIO's responsibility for IT management and information security at their respective agencies.<sup>6</sup>

More recently, the Federal Information Technology Acquisition Reform Act (FITARA) was enacted in 2014 to further strengthen the authority of a CIO.<sup>7</sup> For example, the law specifies that agencies may not submit an IT budget, enter into IT acquisitions, or hire bureau CIOs without the approval of the agency CIO. OMB translated these statutory requirements into an overall framework of responsibilities called the “Common Baseline for IT Management” (Common Baseline) and is working with agencies to take actions which would ensure CIOs had all the responsibilities described in FITARA.

With the passage of FITARA and the creation of the Common Baseline, agencies now have new levers that can be used to more fully integrate their CIOs into all aspects of IT management, budgeting, and decision-making. Even with these tools, though, the maturation of an agency’s IT management practices is something that will always present challenges.

Ultimately, there are many factors that must be in place for an agency to successfully acquire, implement, and manage its IT investments, including senior executive support for the program, active end-user involvement in developing requirements and testing, having skilled program managers and teams, and having consistent and qualified personnel. The transformational changes that must take

place in agencies will take time, resources, energy, and, most importantly, consistent engagement and oversight from agency leadership, OMB, and Congress.

The rest of this policy chapter provides more information about the specific initiatives and strategies that OMB has employed to strengthen the role of the CIO in IT decisions, improve IT management practices, and ultimately improve the Federal government’s return on its IT investments.

*The CIO position at my agency is not a member of the Working Capital Fund (WCF) - nor is there anything planned to change that. Decisions are made in the WCF that have IT impact without having the CIO there to provide input or insight.*

— Agency CIO

## Policy Evolution

Various strategies have been employed over the years to examine an agency IT portfolio and assess the business justification for specific new investments. Led by an increased desire for transparency into government spending, more of these results were shared with the public thereby bringing more attention and accountability to agency performance. In many agencies, CIOs do not have direct supervision, budget authority, or management control of the IT activities of the agency. However, CIO authority over an agency's IT portfolio was recently strengthened in FITARA.

## Key Initiatives

- 1996**  
– present

**Strategic Business Management Framework**

Reports to OMB major IT investment business cases, spending on IT investments, information resource management plans, and enterprise architecture materials.
- 2002**  
– 2008

**President's Management Agenda - E-Government**

Developed a quarterly score for agency capital planning materials, IRM plan, and enterprise architecture plans. Tracked high risk projects through the High Risk List & Management Watch List.
- 2009**

**Federal IT Dashboard and TechStat**

A data-driven dashboard that provides monthly status updates for major IT investments and data-driven reviews of underperforming investments.
- 2012**

**PortfolioStat**

Portfolio-wide review of an agency's IT investments.
- 2013**

**Benchmarking Initiative / FedStat**

Measurement of key management services, including IT, at each agency and bureau.
- 2014**

**Federal Information Technology Acquisition Reform Act (FITARA) and FITARA Common Baseline**

Legislation to strengthen CIO authorities. The Common Baseline established a framework of the responsibilities and authorities expected of agency CIOs and other senior agency officials involved in the management of IT.

## 1996 – present

### Strategic Business Management Framework

An integrated strategic business management framework for Federal agencies consists of agencies' Information Resources Management (IRM) Strategic Plan, Enterprise Architecture (EA), Capital Planning and Investment Control (CPIC), and the Government Performance and Results Act (GPRA) Strategic Plan.<sup>8</sup> Since 1996, CIOs have used some of these tools to establish internal reporting requirements and governance mechanisms. As a result, CIOs were able to increase their involvement with IT budget, acquisition, and project management decisions at their agency.

*IRM Strategic Planning.* OMB requires agencies to write "information resources management plans" focusing on improving the efficiency and effectiveness of each agency's management of information and IT resources. The contents of these plans has varied over the years but the plans generally provide a description of how IRM activities help agency's accomplish their missions and seek to ensure that IT planning, budget, and program decisions are integrated across an organization. The IRM Strategic Plan, in turn, informs the EA and CPIC processes described below.

*Enterprise Architecture.* EA facilitates the CPIC process by providing recommendations to streamline investments, eliminating duplication of effort, and encouraging adoption of technologies that are required to achieve the future state. EA requirements were augmented in 2002 by the establishment of government-wide Federal Enterprise Architecture (FEA) guidance and reporting. FEA established government-wide standard reference models for identifying businesses, services, technical components, and other aspects of each agency's overall IT environment. FEA was designed to describe each agency's current and future architecture in a common way in order to help agencies share resources, lessons learned, and management approaches that could be applied to similar types of activities across the government.



**Capital Planning and Investment Control.** A key tool in the oversight of IT investments is the CPIC process which was first introduced in 1996 through the Clinger-Cohen Act as a series of high-level guidelines.<sup>9</sup> The CPIC process describes the agency’s previous, current, and future fiscal year spending plans on each investment and its impact on mission and establishes a continuing role for OMB in the development and review of agency IT budget requests. Each year as OMB produces the President’s Budget, a team of analysts reviews agencies’ overall list of all IT investments and the detailed business cases for major investments.<sup>10</sup> This led to the increasingly detailed “Capital Planning Guidance” updated annually in OMB Circular A-11.<sup>11</sup> For example, the guidance being developed for FY 2019 explores changes to help standardize data submissions across the Government and make agency IT spending more comparable. It also includes a new emphasis on “IT Security and Compliance” to ensure visibility into how agencies are managing their spending on cybersecurity.

Strategic Business Management Framework	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided a common language for agencies to describe their enterprise architecture and IT investments</li> <li>• Reporting requirements provided the agency CIO increased visibility into IT investments</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Agency IT spending levels are self-reported by CIO staff, not an export from agency financial systems, often leading to data quality questions</li> <li>• The CPIC and EA reporting requirements are frequently treated as compliance exercises and are not consistently used to improve IT management and oversight</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Provided a baseline for CIOs to improve their IT investment decision making</li> <li>• Future updates, such as the CPIC enhancements underway, provide a known process to drive continued change</li> </ul>

2002 – 2008

**President’s Management Agenda - E-Government**

The President’s Management Agenda (PMA) Scorecard was introduced in 2001 as a method of providing oversight over five major management areas, including E-Government and IT.<sup>12</sup> The PMA Scorecard aggregated evaluations of agency IT business cases, enterprise architecture plans, and IRM strategic plans into an overall assessment for the agency.

In addition, OMB established a Management Watch List and High Risk List that focused on individual programs or investments that needed more attention and oversight.<sup>13</sup> The Management Watch List and agency PMA Scorecards were posted online, thus requiring agencies to publicly post justifications for their major IT investments.

President’s Management Agenda - E-Government	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided a regular (quarterly) measurement of each agency’s progress on key OMB initiatives, allowing OMB to see where more work was needed and target follow-up efforts</li> <li>• Shared government-wide results with the public</li> <li>• Provided clear communication to agencies of OMB management priorities and how agencies’ progress would be measured over time</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Translating qualitative agency artifacts (business cases, plans) into quantitative scores every quarter required significant staff time</li> <li>• By prohibiting changes to categories from period-to-period in order to improve the consistency over time, it was difficult to incorporate new priorities into the framework as they emerged</li> <li>• The compliance-oriented focus on the scorecard detracted from efforts to implement new strategies and make fundamental outcome-oriented improvements</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Repeated feedback to agencies around consistent strengths and weaknesses reinforced clear understanding of OMB’s expectations regarding business cases which endured even after PMA ended</li> <li>• Provided a model for how the priorities of OMB’s management offices’ could be incorporated into an agency’s budget review</li> </ul>

2009

**Federal IT Dashboard and TechStat**

In 2009, OMB publicly launched the Federal IT Dashboard with information as to whether major IT investments were on schedule and within budget, as well as an assessment by the agency CIO of the investment’s overall level of risk. Using the data in the Federal IT Dashboard, OMB launched TechStat Accountability Sessions (“TechStat”) as a “face-to-face, evidence-based review” designed to identify and turnaround underperforming IT investments.<sup>14</sup>

- The majority of OMB-led TechStat sessions were conducted in 2010,<sup>15</sup> and led to \$3 billion in total cost implications and an average acceleration of project deliverables from over 24 months to 8 months.<sup>16</sup>
- In 2010-2011, OMB shifted the leadership of TechStat reviews to agency CIOs, and agencies then identified an additional \$930 million in cost implications by the end of 2011.<sup>17</sup>
- Under FITARA, OMB is required to continue both the IT Dashboard and TechStat sessions.
- In 2015, agencies began to indicate on the Dashboard whether they used incremental or agile development practices when describing each IT project.
- OMB’s 2015 FITARA implementation memo updated its requirements for agency-led TechStat sessions, requiring agencies to notify OMB of each session.

Federal IT Dashboard and TechStat	
Key Strengths	<ul style="list-style-type: none"> <li>• Improved transparency into major IT investments</li> <li>• Made data available so the public could see how agencies spend taxpayer dollars</li> <li>• Early TechStats saved money and turned around underperforming investments</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• The IT Dashboard draws from data that is self-reported by agencies leading to questions about data quality and completeness</li> <li>• Unclear if OMB has performed any TechStats in recent years</li> <li>• Shifting TechStats from OMB to agencies diminished the executive scrutiny and impact of the initiative</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• The IT Dashboard represents a major shift away from the static, document-driven approaches, toward live data visualizations</li> <li>• The public could download and analyze the data themselves increasing citizen engagement and oversight</li> <li>• The IT Dashboard and TechStat sessions helped agencies, OMB, and Congress identify at-risk IT projects and implement corrective measures</li> <li>• When asked about OMB’s current approach to management and oversight of IT, none of the agency CIOs mentioned TechStat efforts</li> </ul>

2012

**PortfolioStat**

When IT systems are managed in a decentralized manner, the result is a proliferation of duplicative IT investments across agencies and the broader Federal government. To address this problem, the Administration implemented the PortfolioStat process in March 2012, requiring agency Chief Operating Officers to meet annually with the agency CIO and the Federal CIO to evaluate the agency’s overall IT performance.<sup>18</sup> In comparison to the TechStat reviews which examine IT performance at the specific project or investment-level, PortfolioStat was designed to examine an agency’s IT portfolio as a whole.

- PortfolioStat requires agencies to take a holistic view of IT investments to identify duplication and investments that do not appear to be well-aligned with agency missions.
- The first year of PortfolioStat focused on the consolidation of duplicative commodity IT systems (e.g., email, desktops, mobile devices).
- In 2015, PortfolioStat sessions stopped including agency Deputy Secretaries, became less formal discussions, and were held quarterly rather than annually.<sup>19</sup>
- FITARA requires a CIO to work with the Deputy Secretary of their agency and the Federal CIO to “conduct an annual review of the [IT] Portfolio” of the agency.

PortfolioStat	
Key Strengths	<ul style="list-style-type: none"> <li>• Applied the same Key Performance Indicators (KPIs) and data assessments for all agencies, which allowed for benchmarking and peer comparison</li> <li>• Significant quantitative detail improved CIOs’ awareness of peers’ performance</li> <li>• Sessions which included Deputy Secretaries succeeded in bringing executive attention to significant IT management issues, but were ended in FY 2015</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• The KPIs used in PortfolioStat varied from year to year which made it more challenging for agencies to implement and mature management and measurement programs</li> <li>• Unclear how strongly the discussions between OMB and agencies are connected with KPIs and briefing books</li> <li>• The removal of agency Deputy Secretaries from the PortfolioStat meetings in 2015 may have diminished the executive focus and impact of the initiative</li> <li>• While agencies and OMB have attributed cost savings to PortfolioStat, it is hard to tell what savings would exist in the absence of PortfolioStat</li> <li>• Unclear how opportunities identified in PortfolioStat factored into agency budget requests or OMB budget review</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• In November 2015, OMB reported that PortfolioStat, TechStat, “and related reform efforts have saved the Federal government at least \$3.44 billion dollars since FY 2012.”<sup>20</sup></li> <li>• Future updates, such as enhancements to CPIC reporting, provide a known process to drive continued change</li> <li>• PortfolioStat sessions have been held from 2012 - 2016, one of the more enduring approaches to IT oversight in recent years</li> <li>• Impact and follow-up on “PortfolioStat Action Items” has varied widely between agencies</li> <li>• Other “-Stat” oversight efforts at OMB and GSA are in part modeled on PortfolioStat’s process (e.g., CyberStat, FedStat, ProviderStat, AcqStat)</li> </ul>

2013

### Benchmarking Initiative / FedStat

Launched in 2013 as a part of the the President’s Management Agenda, the Benchmarking Initiative focused on several key management functions: human capital, financial management, real property, and IT. Within IT, the first year of the Benchmarking Initiative focused on collecting data on overall spending on IT help desk operations and email. In subsequent years additional IT services metrics, operational effectiveness metrics (e.g., “number of help desk tickets closed per month”), and customer satisfaction scores (from a standard survey of users and stakeholders) were added.

This data is used as the basis for FedStat meetings between OMB and agencies. Since 2015, OMB has used FedStats as an annual “single, coordinated...meeting covering a prioritized set of mission and management issues” which combines lessons learned from PortfolioStat and the Benchmarking initiative.<sup>21</sup> Furthermore, the Benchmark and Improve Mission-Support Operations Cross-Agency Priority (CAP) Goal includes KPIs evaluating the data completeness and agency participation in Benchmarking.<sup>22</sup>

Benchmarking Initiative / FedStat	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided CIOs with data to make arguments about spending levels based on peers’ experience</li> <li>• Calculated bureau-level spending benchmarks for IT services</li> <li>• Increased executive awareness and use of agency data, leading to improvements in data quality over time</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Data quality and comparability across the government have been called into question (services and calculation methods varied between agencies)</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Helped agencies identify management and contracting issues (such as with double-counting help desk ticket closures)</li> <li>• Established potential cost savings which helped make the case for government-wide initiatives around Financial Management shared services and Unified Shared Services Management (USSM)</li> </ul>

2014

# Federal Information Technology Acquisition Reform Act (FITARA) and FITARA Common Baseline

In creating the position of the CIO, Congress intended for that person to serve as a senior decision-maker, providing leadership and direction for the development, procurement, and management of IT. Despite statutory requirements and OMB policy guidance, many CIOs do not have the necessary authority and are frequently not recognized as the key leaders in

managing IT at an agency. For example, in a 2011 survey of agency CIOs, the Government Accountability Office (GAO) found that many CIOs faced limitations in their ability to influence agency decisions on IT investments because a significant portion of an agency’s IT funding is allocated and spent at the component, or bureau level, of an agency.<sup>23</sup>

Figure A1: Summary of Common Baseline for IT Management<sup>24</sup>

Common Baseline for IT Management					
Section	Budget Formulation	Budget Execution	Acquisition	Organization & Workforce	CIO ASSIGNMENT PLAN (optional)
Responsibility					
Visibility	A1: Visibility of IT resource plans/decisions to CIO A2: Visibility of IT resource plans/decisions in budget materials	F1, F2: Visibility of IT expenditures reporting to CIO			
Planning	B1, B2: CIO role in pre-budget submission for programs C1, C2: CIO role in planning program management		I1: Shared acquisition and procurement responsibilities	P1, P2: IT Workforce planning	
Governance		H1, H2: CIO role on program governance boards F2: Participate with CIO on governance boards J1: CIO role in modification, termination, or pause of IT G1: CIO defines IT processes and policies	K2: CAO is responsible for ensuring contract actions which require IT are consistent with CIO-approved plans and strategies I1, I2: Shared acquisition and procurement responsibilities	Q1: CIO reports to agency head (or to Deputy/COO)	
Program Collaboration		E1, E2: Ongoing CIO engagement with program managers		N1, N2: CIO role in ongoing bureau CIOs' evaluations O1, O2: Bureau IT leadership Directory	
Certifications & Approvals	D1, D2: CIO reviews and approves major IT investment portion of budget request	L1, L2: CIO approval of reprogramming requests	K1: CIO review and approval of acquisition strategy and acquisition plan.	M1: CIO approval of new bureau CIOs	

This summary of the 17 elements of OMB’s Federal Information Technology Acquisition Reform Act (FITARA) Common Baseline matches each element with an overall category of agency management and the objective of improvement in that element.

Congress passed the FITARA in 2014 to clarify and strengthen the role of the agency CIO by providing them with more authority over the budget, governance, and personnel processes for agency IT investments. Among other things, the law specifies that agencies may not submit an IT budget, enter into IT acquisitions, or hire bureau CIOs without the approval of the agency CIO.

In 2015, OMB translated the statutory requirements of FITARA into a framework of IT responsibilities called the “Common Baseline for IT Management” and required agencies to:

- Conduct a self-assessment of current IT management capabilities in four areas: (1) budget formulation; (2) budget execution; (3) acquisition; and (4) organization and workforce; and
- Create an implementation plan to improve an agency’s management practices in each of these areas.

OMB also emphasized that leadership from across the agency (e.g., Human Resources, Financial Management, Information Technology, and Acquisition) are expected to collaborate together to implement the responsibilities in the Common Baseline. Agencies are required to report progress on their implementation plans on a quarterly basis. As of September 2016, no agency had fully implemented all elements of the Common Baseline and no single element has been fully implemented at all agencies. OMB makes a dashboard of agency progress available through monthly FITARA implementation meetings coordinated on [Management.cio.gov](http://Management.cio.gov).

FITARA and FITARA Common Baseline	
Key Strengths	<ul style="list-style-type: none"> <li>• Statutorily reinforced that CIOs have the authority and responsibility for all IT at an agency</li> <li>• The Common Baseline provided a standard, government-wide framework for evaluating and improving agency CIOs’ involvement with IT decisionmaking</li> <li>• Emphasized partnership between CIO and CXO peers as a key expectation in agency management</li> <li>• Required agencies to commit to specific, verifiable actions over time to improve overall IT management</li> <li>• Codified the IT Dashboard, TechStat sessions, and the PortfolioStat process</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Agency commitment to closing gaps identified through FITARA self-assessments has varied significantly</li> <li>• Agency leadership and CXOs have often left FITARA implementation to the CIO, though certain gaps require broader changes to agency business processes</li> <li>• Agency plans and commitments varied in level of detail, potentially allowing some agency weaknesses to go unaddressed</li> <li>• There are no Common Baseline-related KPIs in PortfolioStat, Benchmarking, or FedStat in 2015 or 2016</li> <li>• It is unclear how OMB will assess agencies’ ongoing FITARA implementation</li> <li>• There is currently no government-wide method for measuring improved mission, business, or public outcomes due to improvements in management of IT</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Agency implementation has varied, with some agencies using FITARA to help centralize IT from bureaus, while others focus primarily on compliance with reporting requirements</li> <li>• Public conversation about agency progress has often been driven by GAO and Congress</li> <li>• OMB has not released an evaluation of each agency’s progress publicly, or shared its evaluation of agency progress with Congress</li> </ul>

## Metrics and Oversight

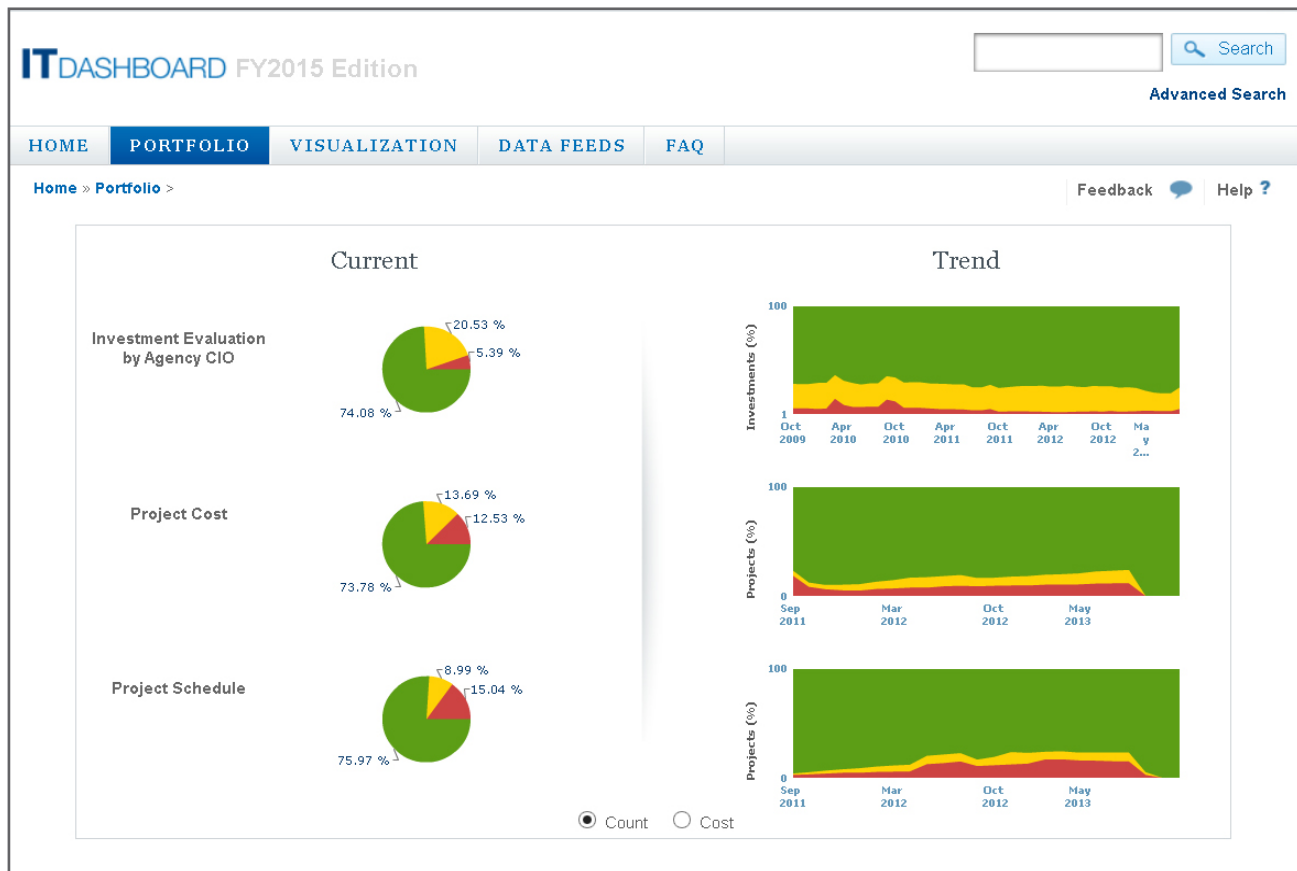
### Primary Objective Emphasized in Metrics and Oversight

The primary objective of OMB's oversight and metrics in this policy area is successful delivery of IT projects ("on time," "on budget," and with a higher level of success). By improving the success of IT projects, CIOs would increase the value IT provides to the rest of the agency. A history of schedule and budget overruns in high profile IT systems plagued the Federal government for decades – increasing CIO oversight of these projects, adopting common planning methods, and greater OMB scrutiny of business cases were intended to lead to more reliable delivery.

### Examples

*Federal IT Dashboard.* OMB launched the Federal IT Dashboard in part to make smarter use of IT project information reported through the CPIC process. By turning agency project plans and execution reports into simple, color-coded summaries of overall schedule and cost variance, both OMB and agency CIOs could more easily identify trouble spots in IT portfolios. Over time, OMB incorporated performance metrics based on these scores into agencies' overall oversight conversations.

Figure A3: IT Dashboard Portfolio Investment and Project Schedule



The Federal IT Dashboard had a Portfolio view which illustrated the proportion of investments across the Federal government which were rated high risk by the agency CIO, or were over budget or behind schedule. (Screenshot from July 2014, prior to a redesign of the IT Dashboard)



**Customer value.** Recognizing that timely delivery is not the only factor in IT success, OMB also developed other metrics designed to measure if delivered IT systems would meet customers' needs. For example, the IT Dashboard incorporated an "Evaluation by Agency CIO" score and comment into every major IT investments' reporting. This allowed the CIO to provide feedback about the likely overall customer success, impact, and risk. Additionally, based on research showing that more rapid delivery allows IT project teams to learn from customer feedback and better meet customer needs, PortfolioStat began to measure how quickly IT systems made it from requirements gathering to delivery. Finally, beginning with PortfolioStat's 2015 sessions, OMB measured what percent of IT projects at each agency used agile or incremental development. Using these metrics allowed for evaluation of value delivered to the customer.

**TechStat.** TechStat Accountability Sessions used IT Dashboard cost variance, schedule variance, CIO evaluations, and CIO research to identify underperforming IT investments and hold data-driven reviews. OMB categorized the results of each OMB-led TechStat effort from the first year (2010) and tracked agency commitments for follow-through as "TechStat Action Items." Agencies reported the results of each of their agency-led TechStat efforts, but there was limited follow-up after a TechStat to evaluate the real impact of these sessions. FITARA restores and expands TechStat reporting requirements, but as of November 2016, OMB has not incorporated TechStat results into the current version of the IT Dashboard.

**PortfolioStat.** OMB has used PortfolioStat every year since 2012 to review each agency's IT performance. Each year, OMB crafts a number of KPIs to be used in PortfolioStat. These KPIs are revised each year, and only one KPI has been used in all five years from 2012-2016.<sup>25</sup> While these sessions have been the cornerstone of OMB oversight of agency performance, the impact and results of these sessions have not always been clear. While OMB has cited "cost savings" each year resulting from PortfolioStat, these savings are not always directly connected to the PortfolioStat process itself.

For example, the first year of PortfolioStat required each agency to develop "Commodity IT Consolidation Plans," which it announced would "save the government over \$2.5 billion."<sup>26</sup> In subsequent PortfolioStat sessions, however, OMB did not revisit these projects, evaluate their progress, or publish the results. Additionally, while each PortfolioStat session results in PortfolioStat Action Items for the agency to implement over the coming year, there is not a complete internal list of agency items and their status nor a measurement of overall agency progress. Finally, it is not always apparent that the KPIs selected for PortfolioStat match the Administration's IT priorities that year. For example, in 2015 and 2016 there were no KPIs measuring agency implementation of the FITARA Common Baseline.

***Role of the CIO and FITARA.*** As a part of FITARA implementation, OMB published a Common Baseline outlining 17 elements designed to improve IT management at an agency. Agencies annually self-assess their progress and send an update to OMB. OMB makes a visual dashboard of this progress, which is available to agencies through monthly FITARA implementation meetings coordinated on Management.cio.gov. In addition, a public update is posted quarterly. Based on agency self-assessments reported in April 2016, no single element of the Common Baseline had been completely implemented at all agencies and no agency had fully implemented all the elements of the Common Baseline.

## Lessons Learned

**Data Issues.** Data quality and completeness issues continue to exist. For example, the IT Dashboard relies on agencies reporting accurate data through the CPIC process. However, agencies discovered inaccuracies in their reported data, especially as they shifted from reporting progress once per year to making continuous monthly updates. In response, OMB worked with agencies and GAO to build “submission validations,” “submission warnings,” and a “data quality report” into the IT Dashboard to flag potential data issues and help agencies correct them.

In addition, following the release of the 25-Point Plan to Reform Federal IT, the CIO Council worked with OMB to modify IT project reporting requirements to more accurately handle in-progress projects without requiring agencies to invest in complex and costly earned-value management systems.<sup>27</sup> These improvements and dialogue between OMB and agencies led to more accurate, timely, and useful data in the IT Dashboard and PortfolioStat. OMB could further improve data quality by working with agencies to connect to agency budget and financial systems instead of relying on CIO staff at the agency to collect spending information. However, this may require significant data standardization to translate general financial information into IT project-specific data.

### **Executive Involvement in PortfolioStat.**

A significant shift in PortfolioStat began in 2015 when OMB stopped holding annual sessions with agency Deputy Secretaries and moved to a quarterly meeting with agency CIOs. It is difficult to evaluate

the impact of this shift, as it is difficult in general to evaluate the impact of PortfolioStat sessions, but much of OMB’s language explaining the importance of PortfolioStat from 2012-2014 mentioned the value of meeting with senior agency leadership. Senior leadership involvement allowed PortfolioStat to surface IT-related issues or opportunities involving resources, programs, and missions outside the CIO’s authority. Removing this in 2015 fundamentally changed the role of PortfolioStat in agency communication.

FITARA requires an annual review with each agency CIO, agency Deputy Secretary, and the Federal CIO, similar to the 2012-2014 PortfolioStat structure. OMB could help illustrate the impact of PortfolioStat by making agency KPI scores over the years and the status of all PortfolioStat Action Items assigned over the years publicly available.

**Next steps for FITARA.** OMB required agencies to develop plans to meet the FITARA Common Baseline, but has not incorporated oversight of these plans into PortfolioStat. It is unclear how OMB follows-up with agencies on FITARA, or what actions it plans to take to address persistent gaps in implementation. December 2016 will mark two years since Congress passed the law, but none of OMB’s Common Baseline elements have been implemented at all agencies. OMB could improve follow-up on agency progress and plans by making the scores summarized in the FITARA Visual Toolkit publicly available, using the same public pressure and transparency that OMB harnessed with the Federal IT Dashboard.

# Agency Observations and Findings

The power, prominence, and responsibilities of a CIO varies across government agencies. There are numerous stakeholders involved in the management and oversight of agency IT portfolios including the Office of the Federal CIO (OFCIO), OMB budget examiners (known as Resource Management Offices or “RMOs”), the President’s Management Council (PMC), and the CIO Council. As a result, centralized oversight and management of IT can be challenging. FITARA is the most recent effort that seeks to address and improve IT management and oversight.

## FINDING #1

### The Authority and Role of CIOs Varies Between Agencies.

The role of an agency CIO varies greatly by agency, typically due to:

- differences in mission,
- the historical growth of an agency,
- whether a CIO is a political appointee or career position, and
- the scale of direct budget control assigned to the CIO’s office.

For example, some CIOs report directly to the agency Under Secretary for Management, or equivalent, while others have reporting structures that place the CIO in a different organizational design.

*[PortfolioStat and FedStat were] all good attempts, but we chase symptoms rather than the core underlying problems.*

- Agency CIO

Oftentimes, significant IT decisions are made in the agency outside of the CIO’s direct control or involvement. A common theme reported by CIOs is that those who have built strong relationships with their executive counterparts and other leaders in their agency have reported being more successful. While the focus on FITARA has raised the profile of the CIO in a number of agencies, implementation has been uneven and many agencies still need to work towards bringing the CIO to a more visible role within the Executive leadership.

## FINDING #2

### Reaction to FITARA Implementation is Mixed.

A number of CIOs praised OMB’s outreach and planning for FITARA guidance, but identified shortcomings in implementation and oversight. While agencies devoted significant resources to preparing FITARA Common Baseline implementation plans and reporting information to OMB, they have not seen a strong continuing focus on follow-up and oversight of FITARA implementation. CIOs reported that continued OMB follow-up could help provide CIOs the necessary high-level cover to allow them to make progress on actions which depend on leaders outside of the CIO organization.

*Performance evals for component CIOs haven’t worked out quite as well – It’s what’s keeping us away from being perfect. The language in M-15-14 and in the statute is too vague on this. We have broad categories for evaluation, but the standardization isn’t complete.*

- Agency CIO

**FINDING #3****The FITARA Common Baseline is Only the First Step in a Much Longer Process.**

The completion and submission of the initial FITARA self-assessments and implementation plans, while important, is merely the first step in a much longer process. To be successful, the Common Baseline must not be viewed as a checklist for compliance purposes; rather, it must be used as a framework by which an agency's IT management practices can be measured.

*A lot of the work I need to get done is about building the right relationships in order to get the work done.*

- Agency CIO

Once an agency meets the Common Baseline requirements, the goal should be to further refine management practices to maximize the potential for positive IT outcomes. That is, agencies are not finished with FITARA implementation just because they give themselves a good rating on an element in the Common Baseline. Agencies must continue to conduct honest assessments of agency leadership, program managers, and stakeholders regarding the IT management practices throughout an agency and refine those practices accordingly.

**FINDING #4****Successfully Improving Agency IT Management Functions Requires the Participation of All Members of the Executive Suite.**

The transformational changes that must take place to improve a number of agencies' IT management functions will take time, resources, energy, and, most importantly, consistent engagement and oversight from agency leadership, OMB, and Congress. For example, integral to nearly every element of the Common Baseline is a strong partnership between CIOs and their peers at both the agency and bureau level. This ensures that management at all levels of the agency has visibility into how IT investments, processes, and resources are managed. However, based on the review of initial agency FITARA submissions, it is clear that close partnerships are not currently in place at many agencies. The establishment of these relationships and processes is necessary to drive change in technology related procurement, workforce development, and budget allocation.

**FINDING #5****Agency Operations Do Not Always Align With OMB Reporting.**

CIOs have mentioned that the data requested by OMB frequently differs from agencies' own operational data collection efforts. In order to satisfy OMB's requests, agencies have to utilize time intensive workarounds and manual processes. Additionally, once the data from these reporting mechanisms are reported to OMB, CIOs reported that they rarely receive feedback on how their data is used or the value resulting from its collection.

In addition, CIOs reported that data requests from Congress, OMB, and GAO,

*The reporting for OMB is different from the way I manage my business. OMB reporting doesn't drive my business decisions, but I've tried to avoid "gaming" the system. We need to align how we report based on our business practices.*

- Agency CIO

can often overlap or conflict, creating agency confusion and increasing the reporting burden. In a recent example, the Congressional FITARA scorecard emphasized themes and areas that were different from reporting required in OMB's FITARA Common Baseline self-assessments and milestones.

**FINDING #6****Agencies Struggle to Apply Government-wide Policies to Their Environments.**

As many CIOs noted, government-wide policies and metrics may not always fit for each agency, which vary in mission, structure, and environment. Consequently, many CIOs advocated for OMB policies which provide them the flexibility to define an approach to best fit their environment while advancing broader policy objectives. CIOs stated that OMB's seeking and incorporating feedback from agencies prior to issuing guidance resulted in policies which allowed greater flexibility and had clearer objectives. Moving forward, actively incorporating feedback from agencies may assist OMB in crafting policies that can be applied government-wide, but which contain flexibilities allowing individual agencies to better achieve the policy's objectives in their unique environment.

# Notes

1. Testimony of Tony Scott, Federal Chief Information Officer, Office of Management and Budget, before the Committee on Oversight and Government Reform, Subcommittee on Information Technology and Subcommittee on Government Operations, United States House of Representatives. 11/4/2015. <https://oversight.house.gov/hearing/the-federal-information-technology-reform-acts-fitara-role-in-reducing-it-acquisition-risk-part-ii-measuring-agencies-fitara-implementation/>
2. Computer Chaos: Billions Wasted Buying Federal Computer Systems. Investigative Report of Senator William S. Cohen, Ranking Minority Member, Subcommittee on Oversight of Government Management, Senate Governmental Affairs Committee. 10/12/1994. <https://acc.dau.mil/adl/en-US/22163/file/2121/Cohen%20Computer%20Chaos%201994.pdf>
3. Inadequate coordination between an agency CIO and the bureaus of an agency can also impede the implementation of cybersecurity initiatives. Several agency CIOs stated that the automated network scanning initiative EINSTEIN required them to direct bureaus to implement network scans, but many lacked visibility or influence on bureau CIOs, leading them to only apply the automated scanning in their own office, rather than the whole agency network. This limitation persisted until the 2009 Cyberspace Policy Review, also known as the 60-day Review, specifically clarified the expectation that bureaus implement this scanning. For more information on EINSTEIN and the 60-day Review, see *Policy Chapter E: Cybersecurity*, as well as “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”. 5/2009. [https://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)
4. Federal Information Technology Shared Services Strategy. 5/2/2012. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/shared\\_services\\_strategy.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf)
5. The Clinger-Cohen Act of 1996 was originally enacted as the Information Technology Management Reform Act of 1996 (Divisions D and E of Public Law No: 104-106). The law was renamed the Clinger-Cohen Act by Public Law No: 104-208, 110 Stat. 3009-393 (1996)
6. Public Law 107-347. *The E-Government Act of 2002*. 12/17/2002. <https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>
7. *Federal Information Technology Acquisition Reform Act*. 12/19/2014. Title VIII, Subtitle D of the *National Defense Authorization Act (NDAA) for Fiscal Year 2015*, Public Law No: 113-291: <https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148>
8. The GPRA Strategic Plan is primarily developed and managed outside of the CIO and IT functions, but all other components depend on policy and guidance from OFCIO
9. *Information Technology Management Reform Act of 1996*. 2/9/1996. Division E of the *National Defense Authorization Act for Fiscal Year 1996*, Public Law No: 104-106: <https://www.dol.gov/ocfo/media/regs/ITMRA.pdf>
10. These were described, respectively, in Exhibit 53 and Exhibit 300 of OMB Circular A-11: *Preparation, Submission, and Execution of the Budget*. 7/2016. [https://www.whitehouse.gov/sites/default/files/omb/assets/a11\\_current\\_year/a11\\_2016.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf)
11. OMB Circular A-11: *Preparation, Submission, and Execution of the Budget*. 7/1/2016. [https://www.whitehouse.gov/sites/default/files/omb/assets/a11\\_current\\_year/a11\\_2016.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf) and FY 2018 IT Budget – Capital Planning Guidance. 6/30/2016. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/fy18\\_it\\_budget\\_guidance.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy18_it_budget_guidance.pdf)
12. The PMA Scorecard was a precursor to PortfolioStat key performance indicators. The Scorecard was published quarterly for every agency and evaluated performance across all management areas, not just IT. OMB combined multiple IT policy areas into a single “E-Government” rating for each agency
13. George W. Bush Presidential Archives. “Budget Highlights: FY 2009 IT Budget Spring Update Reflects Sustained Commitment to Improved Service Delivery”. 9/7/2016. [https://georgewbush-whitehouse.archives.gov/omb/egov/g-9-budget\\_highlights.html](https://georgewbush-whitehouse.archives.gov/omb/egov/g-9-budget_highlights.html)
14. For more information on TechStat, see <https://cio.gov/what-is-techstat/>
15. A 2013 Report by the Government Accountability Office (GAO) summarized: “OMB reported conducting 79 TechStat reviews, with 59 reviews occurring in 2010, 8 in 2011, 11 in 2012, and one so far in 2013. OMB conducted fewer TechStats in recent years because it expected the agencies to increase the number of agency-led TechStats.” GAO-13-524. INFORMATION TECHNOLOGY: Additional Executive Review Sessions Needed to Address Troubled Projects. 6/13/2013. <http://www.gao.gov/products/GAO-13-524>
16. OMB described the impact of TechStat as “cost implications (e.g. cost avoidance, life cycle cost avoidance, and/or reallocation of funding)”. 11/4/2016. <https://cio.gov/drivingvalue/techstat/>
17. “Agency CIOs will take on responsibility for the ‘TechStat’ governance process within their agencies as of March 2011.” Vivek Kundra. *25-Point Implementation Plan to Reform Federal IT Management*. 12/9/2010. <https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf> The *25-Point Implementation Plan to Reform Federal IT Management* launched “agency TechStats”; OMB reported the results of agency TechStats in a December 2011 presentation. “Our Moment.”. 12/2011. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/december2011update.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/december2011update.pdf)
18. M-12-10. Implementing PortfolioStat. 3/30/2012. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10\\_1.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10_1.pdf)
19. M-15-14. Management and Oversight of Federal Information Technology. Page 21. 6/10/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>
20. Testimony of Tony Scott, Federal Chief Information Officer, before the Committee on Oversight and Government Reform, Subcommittee on Information Technology, Subcommittee on Government Operations, United States House of Representatives. 11/4/2015. <https://oversight.house.gov/wp-content/uploads/2015/11/Scott-OMB-Statement-11-4-FITARA.pdf>. The accuracy of this figure has been disputed by GAO. GAO-15-296. INFORMATION TECHNOLOGY: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked. 4/16/2015. <http://www.gao.gov/assets/670/669679.pdf>

21. M-15-11. Fiscal Year 2017 Budget Guidance. 5/1/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-11.pdf>
22. Performance.gov. "Cross-Agency Priority Goal: Benchmark and Improve Mission-Support Operations". Quarterly Progress Update. <https://www.performance.gov/node/3397/view?view=-public#progress-update>
23. GAO-11-634. Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management. Pages 29-30. 9/15/2011. <http://www.gao.gov/assets/590/585305.pdf>. See also GAO-04-823. Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges. 7/21/2004. <http://www.gao.gov/products/GAO-04-823>
24. M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>
25. The HSPD-12 "Strong Authentication" KPI has been included in all five years of PortfolioStat, though the labelling of the metric has varied: "Percentage of systems which require PIV card usage for logical access for all users"
26. PortfolioStat: Saving Billions in IT Spending. 10/24/2012. <https://www.whitehouse.gov/blog/2012/10/24/portfolio-stat-saving-billions-it-spending>
27. Vivek Kundra. *25-Point Implementation Plan to Reform Federal IT Management*. 12/9/2010. <https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>







# IT Infrastructure Modernization



“Many Federal departments and agencies rely on aging computer systems and networks running on outdated hardware and infrastructure that are expensive to operate and difficult to defend against modern cyber threats.”

— Federal CIO Tony Scott<sup>1</sup>

## Summary

 <p>Cost</p>	Federal spending on IT Infrastructure has been growing year-to-year, roughly at the same pace as other IT spending. Of the \$88.7 billion in Federal IT spending planned for fiscal year 2016, approximately \$34.7 billion (43%) is to be spent on IT infrastructure.” <sup>2</sup>
 <p>Accountability</p>	Inconsistent and changing metrics result in high compliance costs for agencies and make it difficult to measure and report the true cost of maintaining Federal IT infrastructure.
 <p>Risk</p>	Many CIOs cite their agency’s dated and obsolete IT infrastructure as an obstacle to meeting the rising expectations of citizens, employees, and other customers. Major transformative projects are needed to address these issues.
 <p>Policy</p>	IT policy and appropriations law currently does not allow agencies to redirect operations and maintenance funding to update the IT systems that directly support their mission and goals.

# IT Infrastructure Modernization

## Overview

Agencies rely on physical information technology equipment to provide them with direct operational support for their mission objectives. This equipment includes data centers, end user devices, cloud systems, and other infrastructure. IT infrastructure comprises a major portion of overall Federal IT spending (ranging from 30-50 percent)<sup>3</sup> and government-wide spending in this area continues to increase at a steady pace.<sup>4</sup> IT infrastructure underpins nearly all other IT policy areas, providing the physical and logical framework upon which a modern enterprise can be built. For example, without a modern IT infrastructure that includes systems which can easily be patched and updated, it is very difficult to develop a strong cybersecurity posture.

In addition, the increased cost of maintaining an older IT infrastructure can take away agencies' ability to embark upon new and innovative IT activities. CIOs across the government repeatedly cited aging infrastructure as a roadblock to innovation and as an obstacle to meeting expectations of citizens and agency employees. For example, as agency users access more bandwidth-intensive cloud-based services, aging agency network infrastructure can struggle to meet the demand. As a result, improved management of agency IT infrastructure has been a major focus for government-wide initiatives and policies in recent years to facilitate a transition to a less expensive, more secure, and customer-focused IT environment.

## Transition to IPv6

Legacy Internet Protocol version 4 (IPv4), which was first described in 1981, is no longer able to support the enormous growth of devices connected to the Internet.<sup>5</sup> In the late 1990s, engineers commenced designing the next generation Internet Protocol, version 6 (IPv6), which enabled multiple improvements such as:

- Increasing the number of available IP addresses
- Simplifying the way the addresses can be transmitted through the Internet
- Incorporating bandwidth optimization techniques
- Embedding cryptographic authentication for ease of use.

The Federal government is currently in the process of adopting IPv6 for all network-enabled devices.

Government-wide adoption of IPv6 everywhere is imperative to maintain and enhance service to the general public as well as sustaining communication with world partners. To ensure the success of IPv6 top down support and leadership from the Federal CIO and agency CIOs is critical.

Figure B1: IT Infrastructure Spend FY 2016 (Excluding DOD)<sup>6</sup>

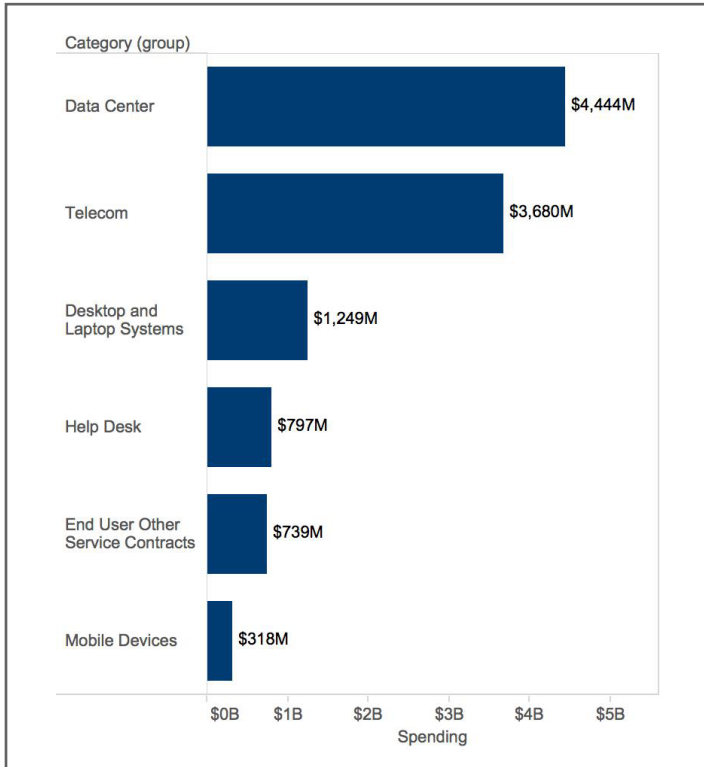
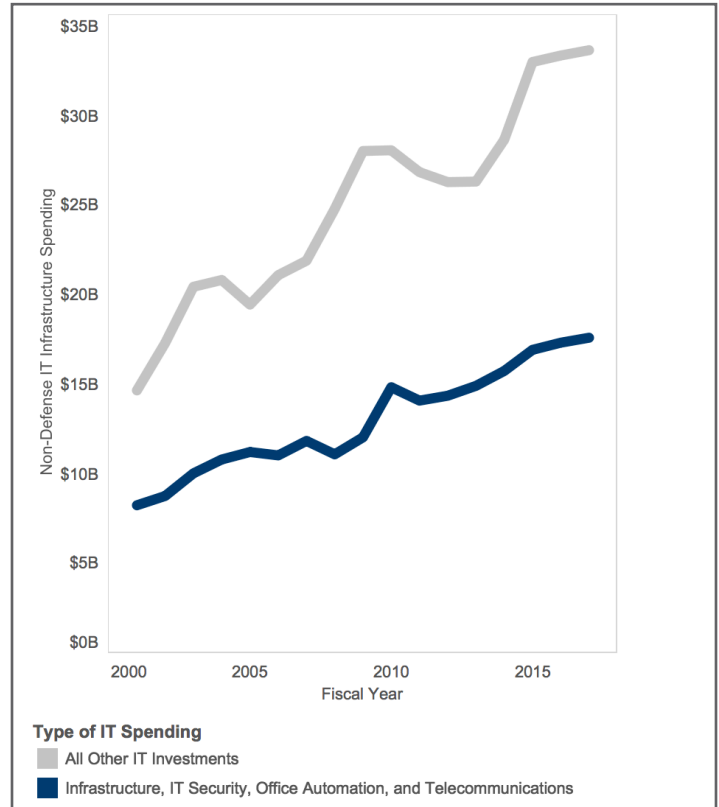


Figure B2: IT Infrastructure and all other IT Spending Over Time (Excluding DOD)<sup>7</sup>



Government spending on data centers represents a significant portion of the money spent on Federal IT infrastructure.<sup>8</sup> Agencies have to purchase hardware and software, pay for facilities, and pay the salaries of the employees who operate these centers, which typically run 24 hours a day, seven days a week. Over the years, the Federal Government’s demand for IT has led to a dramatic rise in the number of Federal data centers.<sup>9</sup> The Government Accountability Office (GAO) has cited “the growth in the number of Federal data centers, many offering similar services and resources” as a source of duplication that creates unnecessary expenditures.<sup>10</sup>

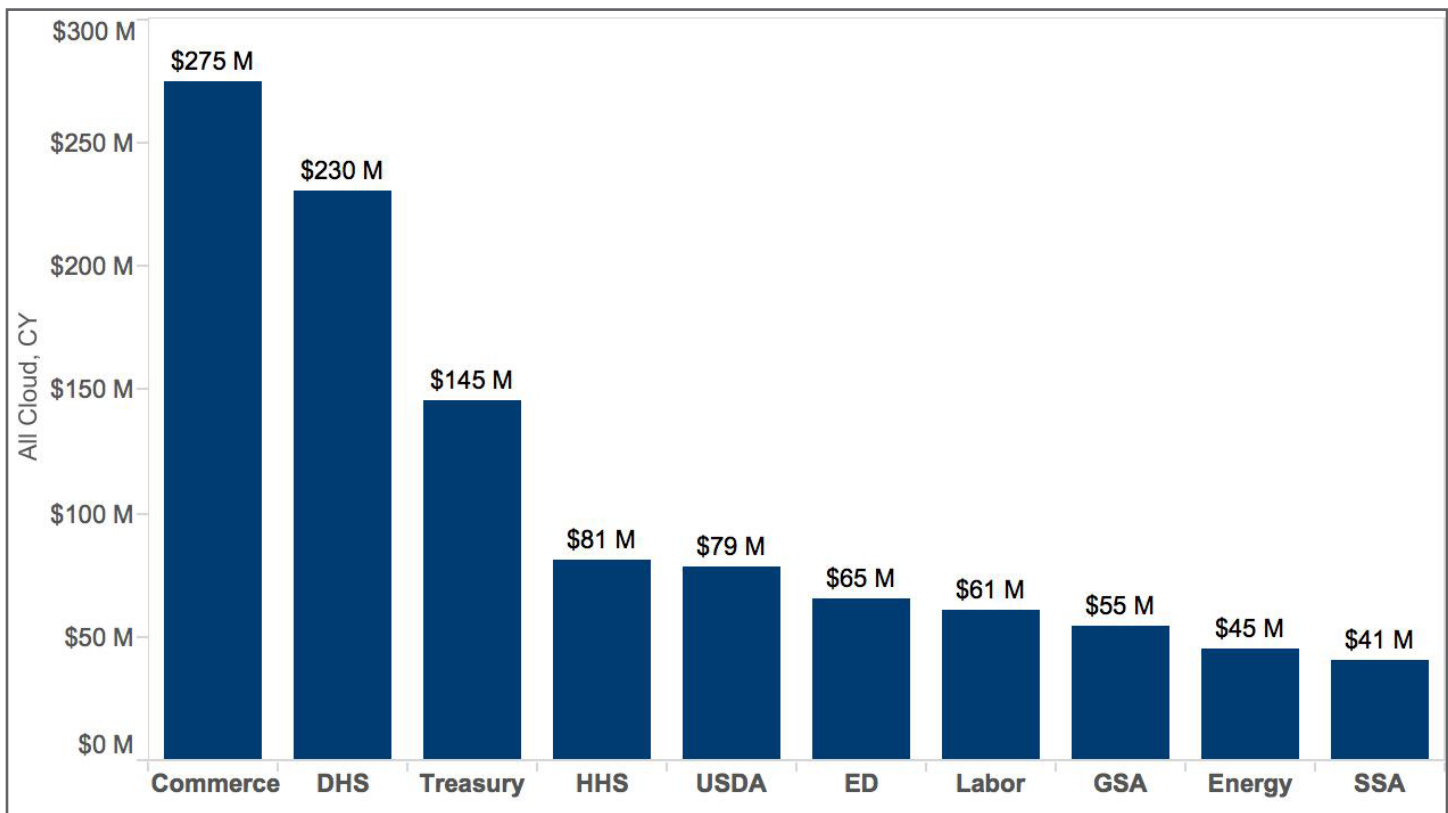
In recent years OMB pushed to move agencies to the cloud. With Federal agencies projected to spend over \$2 billion on cloud computing services out of a total of \$80 billion in IT spending in FY 2016, there are clearly more opportunities to adopt cloud-based solutions.<sup>11</sup> However, while agencies see value in adopting cloud-based solutions they continue to face challenges in doing so. Longstanding Federal procurement policies, geared towards long-term, large-scale investments, do not always support the more incremental, agile acquisition model (e.g., only buy additional

IT Infrastructure Modernization

capacity when it is needed) offered by cloud providers. Furthermore, there are a number of standing policies that may conflict with moving to a cloud-based environment. For example, the implementation of Trusted Internet Connections (TIC)<sup>12</sup> requires the usage of specific government and commercial access providers, with validation checks provided by the Department of Homeland Security. A number of agencies stated that it was unclear as to whether their cloud-based providers were TIC-compliant, and the issue was further complicated by uncertainty over which policy should take precedence. Additionally, the risk of vendor lock-in and concerns around multi-tenancy and data sovereignty continue to be issues.

Finally, the need for upfront capital planning and investment to adhere to Federal budget cycles does not align with the pace of innovation which, in turn, slows the pace of adoption. The creation of an IT Modernization Fund (ITMF) provides a possible path forward. By creating a central funding mechanism for IT modernization efforts, it can help agencies to work around long budget cycles, streamline procurements, and reprogram funding to modernize IT infrastructure. In combination with ongoing data center optimization and cloud computing initiatives, ITMF (as currently proposed) could help drive the modernization of aging IT infrastructure and achieve significant cost savings.

Figure B3: Total Cloud Spending for Top 10 Civilian Agencies, FY 2016 Spending<sup>13</sup> (Dollars in Millions)



## Policy Evolution

The modernization of legacy IT systems and the effective management of infrastructure investments has long been a focus for agencies and OMB. Earlier efforts included the usage of Enterprise Architecture roadmaps and consolidated business cases to take an enterprise-wide view of their IT infrastructure (versus a bureau-level view). Over the last several years, data center consolidation and optimization, and moving resources to the cloud have topped the IT modernization agenda.

## Key Initiatives

- 2006** IT Infrastructure Optimization (ITI) Line of Business

Develops common government-wide performance measures for service levels and costs, identifies best practices, and provides guidance for agency IT infrastructure transition plans.
- pre-2009** Enterprise Architecture and Centralizing Infrastructure

Defines the infrastructure major business case and use of Federal enterprise architecture to manage across the agency.
- 2010 – 2015** Federal Data Center Consolidation Initiative

**2010 Memo** - Directs agencies to inventory their data centers, develop a consolidation plan, and to evaluate virtualization and cloud alternatives.  
**2011 Memo** - Provides guidance on consolidating “core” data centers and the movement of operations into them. Specifies the closure of 800 data centers by 2015.
- 2011** Cloud First

Agencies should identify three services which “must move” to the cloud within 18 months and evaluate cloud for new/enhanced investments.
- 2011** Federal Risk and Authorization Management Program

Integrates standards and risk management with Cloud First, provides “a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.”
- 2016** Data Center Optimization Initiative

Updates the Federal Data Center Consolidation Initiative (FDCCI) based on requirements in FITARA. Refocuses on tiered data centers, PUE, CM, and other optimization metrics, in addition to cost savings and closures.

2006

## IT Infrastructure Optimization (ITI) Line of Business (LoB)

Established in 2006, the ITI LoB was designed to examine the government-wide opportunities for IT infrastructure consolidation and optimization in an effort to achieve cost savings.<sup>14</sup> This initiative defined common performance measures for provider service levels in infrastructure areas such as mainframe and server services and support, telecommunications systems and support, and end user systems. Through a central coordination mechanism at GSA, ITI LoB also assisted agencies with their migrations and the adoption of best practices.<sup>15</sup>

IT Infrastructure Optimization Line of Business	
Key Strengths	<ul style="list-style-type: none"> <li>Established government-wide assistance for agency migrations of IT infrastructure</li> <li>Defined common performance standards and metrics</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>Participation was optional, so impact was limited to agencies already proactively investing in infrastructure improvements</li> <li>Governance structure did not require significant buy-in from agency leaders, allowing effort to operate independently but diminishing the applicability and usefulness of standards developed</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>Established a baseline discussion of infrastructure services and performance models</li> <li>Early effort to capture consistent, standardized metrics relating to common infrastructure categories</li> </ul>

Pre-2009

## Enterprise Architecture and Centralizing Infrastructure

In addition to the government-wide efforts in the ITI LoB, OMB also encouraged more deliberate central planning for IT infrastructure at each agency in two primary ways:

- First, agencies were required to develop agency-wide Enterprise Architecture<sup>16</sup> plans that described how each agency currently operated, how it intended to operate in the future, and how it planned to transition to the envisioned future state.
- Second, agencies were required to create a single consolidated major business case for their entire IT infrastructure spending portfolio.

The goal was to improve visibility into an agency’s overall approach to acquisition, architecture, and business decisions regarding IT infrastructure across the agency’s portfolio. While enterprise architects were directed to support efforts to consolidate commodity IT as late as 2011,<sup>17</sup> other foundational policy documents are largely silent on the use of enterprise architecture.<sup>18</sup>

Enterprise Architecture and Centralizing Infrastructure	
Key Strengths	<ul style="list-style-type: none"> <li>• Creating an EA established processes, vocabulary, and a framework for building an IT enterprise, not just separate individual efforts</li> <li>• Provided a tool for identifying redundant and overlapping investments</li> <li>• Emphasized that infrastructure operations throughout each agency are relatively similar and could be managed in a cross-cutting manner</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• The enterprise architecture community had trouble communicating with other executives about the value of EA</li> <li>• EA efforts were seen as document- and compliance-oriented, rather than guided by the management objectives of the agency</li> <li>• Large consolidated IT infrastructure business cases may obscure the details of potential budget or performance issues</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Despite guidance from OMB to the contrary, many consolidated infrastructure investments remain in agency IT portfolios</li> <li>• OMB still houses the Chief Enterprise Architect, but EA has not been a major component of OMB management priorities in recent years</li> <li>• While OMB’s focus on EA has diminished, given that many of its policies and guidance are still active, agencies continue to spend significant effort on compliance</li> <li>• OMB has not connected current efforts to modernize IT infrastructure, such as the IT Modernization Initiative, with the existing EA community or EA policies</li> </ul>

2010 – 2015

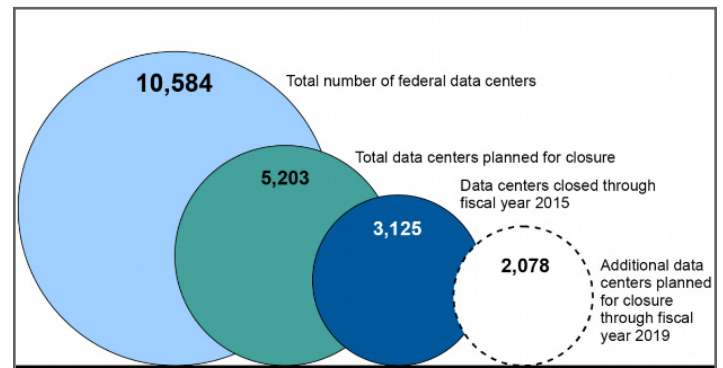
## Federal Data Center Consolidation Initiative (FDCCI)

In 2010, OMB launched the Federal Data Center Consolidation Initiative (FDCCI) to consolidate redundant Federal data centers, improve the government's cybersecurity posture, reduce Federal data center energy usage, and achieve cost savings.<sup>19</sup> OMB set a target goal of closing 40 percent of the Federal data centers agencies had previously identified (initial goal of consolidating 800 data centers), and estimated cost savings between \$3 and \$5 billion – both by the end of 2015.<sup>20</sup>

### FDCCI Goals

- Promote the use of green IT by reducing the overall energy and real estate footprint of government data centers;
- Reduce the cost of data center hardware, software, and operations;
- Increase the overall IT security posture of the government; and
- Shift IT investments to more efficient computing platforms and technologies.

Figure B4: From GAO, Agencies' Total Number of Data Centers, Completed, and Planned Closures through FY 2019 (As of November 2015)<sup>21</sup>



Under the FDCCI, agencies were required to:

- Submit an inventory of each agency's data centers;
- Develop a plan to consolidate data centers; and
- Annually update their asset inventory and report on the progress made toward implementing the agency consolidation plan.

*“With data centers that run as large as three and a half football fields, shutting down excess data centers will save taxpayers billions of dollars by cutting costs for infrastructure, real estate and energy. At the same time, it will improve the security of government data and allow us to focus on leveraging technology to make government services work better for the American people,”*

– Federal CIO Vivek Kundra, 2011



While progress was made in closing data centers, it is unclear what the impact of that progress was. This was due in large part to the fact that many agency data centers were actually small “server closets” containing localized telecommunications equipment, the closure of which might not result in cost savings. Furthermore, as the definition of data centers changed over time, it is unclear how precise agency closure counts are.

Despite these challenges, the FDCCI did kickstart an important conversation about IT infrastructure throughout the Federal IT community, a conversation that continues to this day due to the codification of many of the requirements in the original FDCCI memo. It is important to note that the Data Center Optimization Initiative (DCOI), discussed later in this chapter, was built upon the foundation laid by the FDCCI. While DCOI shifted some of the definitions and metrics used in FDCCI, it retained the central focus of consolidating data centers and achieving cost savings.

Federal Data Center Consolidation Initiative (FDCCI)	
Key Strengths	<ul style="list-style-type: none"> <li>• Consolidation targets provided agencies a clearly defined objective</li> <li>• Provided executive level attention on core IT infrastructure issues</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Debates over what to “count” as a data center hampered efforts to establish a meaningful baseline to measure progress</li> <li>• The focus on reducing the number of data centers distracted from the broader objectives of infrastructure modernization</li> <li>• Agencies do not track their spending on individual data center facilities, hampering efforts to project cost savings based on consolidation activities</li> <li>• Investment in a universal “total cost of ownership” tool to estimate agency spending on each data center was cancelled due to challenges related to data accuracy and completeness</li> <li>• Shifting metrics from simply counting closures to evaluating various optimization metrics in PortfolioStat<sup>22</sup> led to confusion amongst many agencies</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Successful in achieving agency cost savings due to consolidation or optimization of their data centers over the life of the effort</li> <li>• Agency CIOs looking to move to alternative IT infrastructure providers used FDCCI to justify investment in migration to new providers (e.g., cloud alternatives)</li> <li>• CIOs reported that they now favor a cost-benefit analysis of whether closing a facility was a sound business decision rather than simply reducing counts of facilities</li> </ul>

2011

## Cloud First

Along with the FDCCI initiative, the Administration issued a report in 2010 titled *State of Public Sector Cloud Computing*, that laid out the argument for agencies to focus on moving agency operations to the cloud.<sup>23</sup> The primary argument in the report was that cloud computing could allow Federal agencies to move away from owning and operating their equipment directly, and towards leasing equipment from external service providers, at reduced costs and on more modern IT infrastructure. It also asserted that, by using provisioned cloud computing services, agencies could more effectively deal with spikes in demand for key services. Agencies could then use the most modern infrastructure available within the government and private sector, allowing their staff to focus more time on agency mission goals.

In December 2010, the Administration launched the 25-Point Implementation Plan to Reform Information Technology Management.<sup>24</sup> A key initiative in the 25-Point Plan was the “Cloud First” policy which required agencies, for new IT deployments, to “default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.” OMB told agencies to identify three “must move” services, where “at least one of the services must fully migrate to a cloud solution within 12 months and the remaining two within 18 months.”<sup>25</sup>

Cloud First was reemphasized in the *Federal Cloud Computing Strategy*, released in 2011, which articulated the benefits, considerations, and tradeoffs of cloud computing for agencies.<sup>26</sup> This strategy also provided a decision framework, case examples, and other resources that could support agencies in their migration to cloud-based solutions.

Cloud First	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided CIOs with the necessary “top cover” to push for more cloud adoption</li> <li>• Change in mindset began to shift CIOs’ thinking away from traditional servers and mainframes to cloud-based services in a more systematic way</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Requirements were loosely defined - the requirement to shift three “must move” services did not provide sufficient guidance for how agencies might identify appropriate targets</li> <li>• There was no evidence of significant follow-through on the Cloud First policy requirements. For example, IT budget guidance for the next fiscal year did not require agencies to identify their “must move” services. As a result, it is unclear if agencies actually fulfilled the requirements of the policy</li> <li>• OMB continued to accept budget requests for agency expansion of non-cloud systems with no explanation or negative consequences, despite the “Cloud First” principle</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Agencies chose to prioritize cloud migrations for low impact services in order to meet OMB’s “three services” target</li> <li>• Agency CIOs faulted the policy for not providing sufficient follow-through to truly change their business practices</li> </ul>

2011

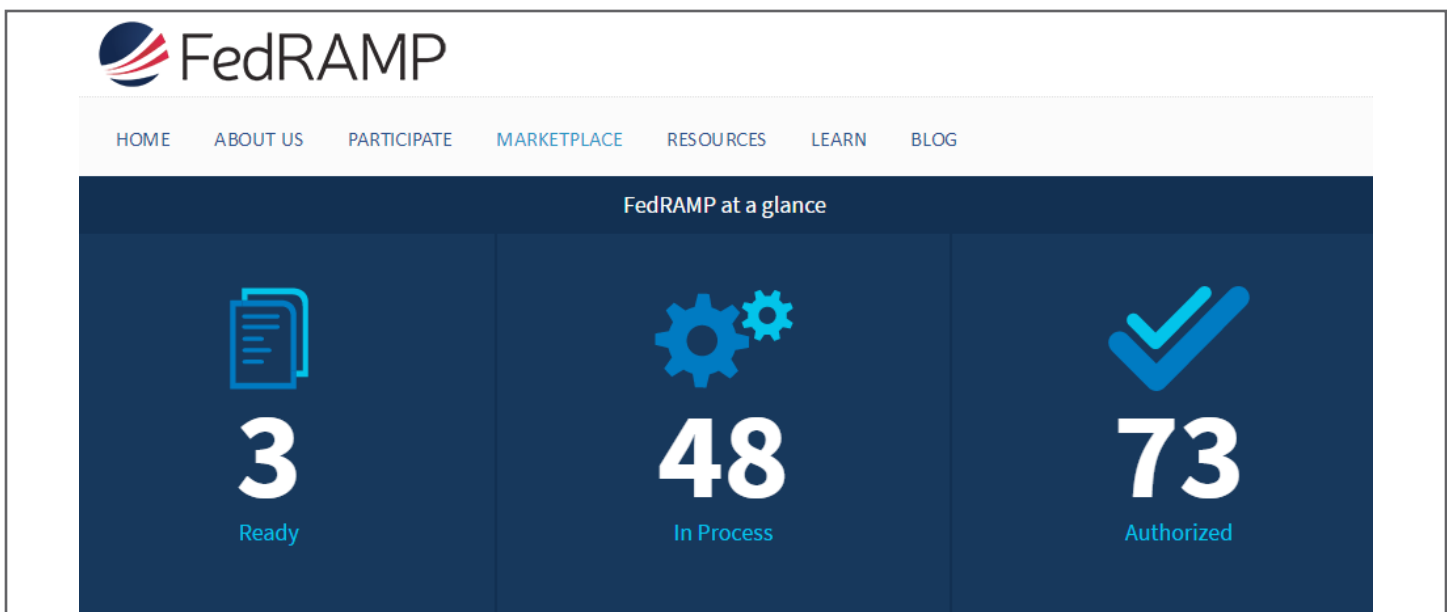
## Federal Risk and Authorization Management Program (FedRAMP)

In 2011, FedRAMP was launched to accelerate cloud adoption across the Federal Government while appropriately handling cybersecurity risks and Federal Information Security Management Act (FISMA) rules.<sup>27</sup> FedRAMP was set up to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.<sup>28</sup> The program is intended to facilitate the adoption of cloud computing services among Federal agencies by providing cloud service providers with a single accreditation that could be accepted by all agencies. The goal of FedRAMP is to reduce the time and money that individual agencies would otherwise have to spend on assessing a cloud provider’s cybersecurity posture. Certifications are based on a unified risk management process that includes security requirements agreed upon by the Federal departments and agencies.

Federal Risk and Authorization Management Program (FedRAMP)	
Key Strengths	<ul style="list-style-type: none"> <li>• Vision of providing a one-stop shop for identifying approved cloud providers gave agencies a framework for safely adopting cloud services</li> <li>• Unified risk management approach provides a common set of security standards and controls for cloud services</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• The average approval timeline is nearly 18 months, resulting in significant delays in adopting services</li> <li>• Agency CIOs must still conduct their own internal risk evaluations even on FedRAMP-approved services before adoption, negating some of the potential gains</li> <li>• Unclear path for maintaining approvals as technical and data management characteristics of approved providers change over time</li> <li>• Some agencies are unsure whether they may use cloud services which are not yet FedRAMP-approved</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• FedRAMP has successfully created a common security baseline for cloud-based services at the low, medium, and high levels</li> <li>• The program has currently [11/2/2016] authorized 77 cloud-based services, with another 49 “in process”</li> <li>• \$70 million per year in government-wide cost avoidance through the reuse of FedRAMP authorizations since the program’s launch<sup>30</sup></li> </ul>

IT Infrastructure Modernization

Figure B5: Example View of the FedRAMP Dashboard<sup>29</sup>



2016

## Data Center Optimization Initiative (DCOI)

In 2014, the Federal Information Technology Acquisition Reform Act (FITARA) was enacted, which, among other things, codifies and builds upon the requirements of the FDCCI. Under FITARA, agencies are required to submit annual reports that include: data center inventories, multi-year strategies to consolidate and optimize data centers, performance metrics and a timeline for agency activities, and yearly calculations of investment and cost savings.<sup>31</sup>

In August 2016, in an attempt to further clarify the data center objectives of FITARA, OMB launched the Data Center Optimization Initiative (DCOI).<sup>32</sup> The DCOI shifted the focus of the previous FDCCI efforts by:

- Moving from “core and non-core” data centers to industry-standard “tiered” data centers;
- Adding new optimization metrics, including a focus on power usage effectiveness and energy metering;
- Tasking GSA with the operation of a Data Center Line of Business and shared service; and
- Continuing efforts to close data centers and report cost savings.

Data Center Optimization Initiative (DCOI)	
Key Strengths	<ul style="list-style-type: none"> <li>• Implements FITARA’s statutory requirements for data center metrics, reporting, and management</li> <li>• Provides information to the public and Congress on progress and targets at a government-wide and agency level</li> <li>• Continues to shift the conversation from counting data center closures towards achieving performance improvements and cost savings</li> <li>• Begins to build the foundation for an internal Federal shared services market of interagency IT infrastructure services</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Some agencies have found that the characteristics of data centers most important to them are not well reflected in DCOI’s optimization metrics</li> <li>• It remains unclear whether high performance in DCOI’s optimization metrics will reliably translate into operating a modern infrastructure</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• It is still very early in the initiative’s lifecycle, so it is difficult to evaluate the impact thus far</li> </ul>

## Metrics and Oversight

### Primary Objective Emphasized in Metrics and Oversight

While IT Infrastructure efforts have a number of goals, such as improving security, streamlining operations, and providing better service, measurement efforts above primarily focused on cost savings with the overall intent of shifting funding from infrastructure to new development and/or mission-focused efforts.

OMB traditionally has used the CPIC process as the primary mechanism for tracking infrastructure spending – measuring the amount spent on IT Infrastructure (Part 2) versus the overall spend on IT. While this was included in the initial PortfolioStat (2012), it was replaced by spending per FTE in subsequent years.<sup>33</sup> Notably, while savings of \$8.1 billion have been reported through data center consolidation, PortfolioStat, and other reform initiatives, the portion of spending on IT Infrastructure versus overall Federal IT spending has remained relatively constant (34.6% in 2010 to 34.3% in 2017).<sup>34</sup>

### Examples

*Data center consolidation and optimization.* Through FDCCI, OMB sought to drive cost efficiencies by reducing the number of data centers government-wide. Initially, OMB tracked the number of planned and actual data center closures as a PortfolioStat Key Performance Indicator (KPI). However, discovery of additional data centers by agencies, and OMB modification of the definition of data center resulted in the government's overall inventory increasing, despite agency closures. Additionally, as the definition of data center was expanded to include smaller facilities, such as server closets, agencies were able to increase their closure rate but not necessarily in ways that generated additional cost reductions. OMB developed a Total Cost of Ownership tool to estimate the savings resulting from facility closures, but agencies had difficulty applying it to their environment.

Nonetheless, OMB has reported \$4.6 billion in savings due to data center closures, although GAO has questioned the accuracy and completeness of these estimates.<sup>35</sup> Over time, OMB has evolved the FDCCI approach to focus on optimization rather than consolidation, moving away from specific closure targets and more specifying overall performance goals, giving agencies more freedom as to how to achieve those goals.

**Commodity IT consolidation.** In 2011, OMB began to focus on consolidating and rationalizing the use of commodity IT, in part to reduce infrastructure spending. While this was tracked in PortfolioStat 2012-2014, ambiguity regarding the definition of the areas of commodity IT made it difficult to attribute savings to specific commodity IT efforts. OMB did emphasize mobile contract spending in particular as an area for potential savings, taking advantage of the relative similarity between agency cellular service contracts for comparison. Total savings of \$3.4 billion have been reported due to PortfolioStat and other reform initiatives since FY 2012.<sup>36</sup>

**Cloud computing.** OMB tracks the amount of IT spending on cloud computing investments, but does not report savings due specifically to migrations to cloud computing. Rather, the focus has been on driving agencies to cloud computing services, with the assumption that cloud-based services intrinsically yield benefits, primarily cost savings. As such, OMB tracks the percentage of each agency's IT spending using cloud computing as a PortfolioStat KPI. In the past, OMB instead measured the percentage of investments using cloud computing, and prior to that, the percentage of investments considering cloud computing. As a part of 2016 PortfolioStat, OMB set 15% as its government-wide target for cloud computing; currently no agencies meet that level. OMB also looked at FedRAMP utilization as a proxy for success adopting cloud computing solutions, but until the 2016 launch of the FedRAMP Dashboard, it was difficult to evaluate the level of agency re-use of FedRAMP packages for additional cloud provider authorizations.

## Lessons Learned

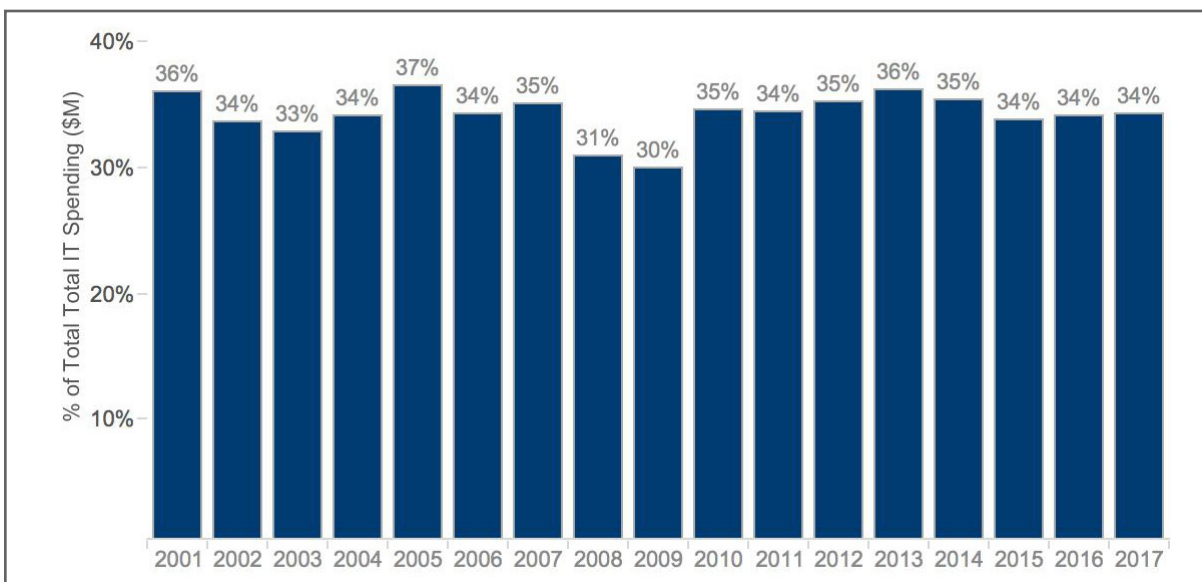
Notably, while savings of \$8.1 billion have been reported through data center consolidation, PortfolioStat, and other reform initiatives, efforts to measure cost savings have been challenged both by the lack of consistent baseline data as well as changes in definitions over time. As GAO summed it up, “Inconsistencies in OMB and agencies’ reporting make it difficult to reliably measure progress in achieving PortfolioStat savings.”<sup>37</sup> For example, agencies did not have complete inventories of their data centers prior to the start of FDCCI. Changes to definitions used in measurements of IT infrastructure have made it difficult to understand whether agencies have improved over time. Redefining data center multiple times over the years, creating a new IT infrastructure exhibit, and varying metrics between percentage of total spending versus per employee versus percentage of IT investments have contributed to this ambiguity.

Moreover, by focusing on metrics like percentage of cloud spending, infrastructure measurements have lacked

a strong connection to agency mission and objectives; agencies have been reluctant to invest in cloud computing simply to increase the percentage of their spending on cloud solutions, for example. OMB could develop a more outcome-oriented measure of modern IT infrastructure to use to evaluate whether agency environments are truly becoming more cost-efficient and mission-effective. Similarly, by focusing on selecting and defining processes, OMB runs the risk of signaling an approach to agencies which it then revises based upon new information. For example, many initial agency FDCCI consolidation plans focused on reducing the number of facilities, so when new optimization metrics were announced that emphasized server virtualization and power usage effectiveness, those original agency plans may have no longer been relevant.

Moving forward, the current DCOI model, which gives agencies greater control by setting higher-level, outcome-oriented goals centered around optimization, can provide a good example. Additionally, by focusing on outcomes, there is less need for precise definitions of terms and processes.

Figure B6: Federal Spending on IT Infrastructure (Percentage of Total IT Spending), 2001-2017<sup>38</sup>



# Agency Observations and Findings

Despite spending more money on IT infrastructure, including substantial sums on Federal data centers, many agencies reported that they have not seen a corresponding improvement in the functionality, effectiveness, capabilities, and efficiency of that infrastructure. CIOs across the government repeatedly cited aging infrastructure as a significant roadblock to innovation and as an obstacle to meeting the expectations of citizens, employees, and other customers of digital services. For example, some agencies have found it difficult to adopt agile development methodologies or use software-as-a-service collaboration tools because of Internet bandwidth constraints or deployment processes that are necessitated by aging IT infrastructure. In addition, inconsistent metrics have made it difficult for agencies to capture the necessary data required to evaluate progress.

*We had to increase the bandwidth four times in order to get to email as services. I don't have the bandwidth to support collaboration tools or VTC*

— Agency CIO

## FINDING #1

### Current Approach to Modernizing IT Infrastructure Does not Necessarily Align with Agency Needs.

Agency CIOs identified outdated IT infrastructure as an obstacle to progress, impacting operational and mission goals including: offering modern digital services to the public, meeting employees' expectations about mobile device use, providing modern collaboration tools, and enabling secure identity management.

*The reporting for OMB is different from the way I manage my business. OMB reporting doesn't drive my business decisions, but I've tried to avoid "gaming" the system. We should align how we report to OMB based upon our business practices*

— Agency CIO

However, several CIOs commented that current government-wide data collections and metrics in this policy area do not align with the business needs of their agency. According to CIOs interviewed, recent oversight efforts have focused on metrics that do not directly measure whether an agency's IT infrastructure enables modern services. Instead, these oversight metrics have varied from closures and cost savings, to physical and technical utilization, to energy efficiency. Yet as CIOs reported, these metrics do not necessarily measure progress toward replacing an outdated IT infrastructure with one which better supports agency needs. In the absence of a standard modern infrastructure to build toward, agencies have charted their own paths and have used mission and budget requirements to drive modernization.



**FINDING #2****Changes in Messaging and Oversight Metrics Can Discourage Agencies from Taking Action.**

Several CIOs expressed challenges in following government-wide guidance for infrastructure given what they considered to be frequent changes in metrics and reporting requirements. Because of the multi-year planning horizon for Federal budgeting and procurement processes, agencies must balance where they expect OMB's focus and priorities to be multiple years down the road with the agency's own opportunities and challenges. For example, the changes in the oversight metrics used to evaluate agency progress in data centers have often signaled different priorities to agencies. Agencies that began multi-year efforts to establish powerful modern "core" data centers (as encouraged in the FDCCI) may now be underperforming in new oversight metrics that focus on power utilization effectiveness and floor space utilization. Additionally, regardless of the specific metrics used, agencies report significant costs in developing and automating reporting. Nonetheless, in many cases there is good reason to update the metrics to better focus efforts government-wide on the right outcomes, especially given the rapid evolution of technologies. Going forward, OMB and agencies will need to strike the balance between consistency of metrics year-over-year and adapting to changing environment.

*I have to get 10 centers to give me their data. Every time OMB changes their metrics, I can't automate the data collection.*

*I need to go through an expensive and time-consuming manual process. Plus I can't do any trend analysis.*

— Agency CIO

**FINDING #3****Infrastructure Only Gets Leadership Attention When It Fails.**

Many CIOs indicated that agency leadership tends to focus on mission and customer-facing IT initiatives. While understandable, this can mean that IT infrastructure is not seen as priority until it fails, creating issues that affect mission performance, such as losing Internet access or email functionality. However, as infrastructure provides the backbone required for the operation and management of an enterprise IT environment, it enables agencies to deliver mission-critical services. For example, while PIV cards (a part of the infrastructure that supports Federal identity management efforts) have been around since 2005,<sup>39</sup> their issuance did not gain significant traction until the Cybersecurity Sprint in 2015.

**FINDING #4****FedRAMP Has Not Accelerated Safe Adoption of New Cloud Services.**

One CIO said, “even once FedRAMP has issued an approval, I still need to do my own [certification & accreditation] – where is the cost savings?” Others indicated that FedRAMP takes so long to authorize a provider that it is not in the agency’s interest to participate. Further, even if a FedRAMP authorization is in place, the agency must conduct its own complete ATO. Numerous CIOs mentioned that they have been unable to find other agencies’ ATOs and authorization packages through FedRAMP, though forthcoming improvements to FedRAMP.gov in 2016 are intended to address this issue.

*FedRAMP says “that platform is certified” or “that app is certified”, but each agency still has to have their own ATOs on top of it. If we can use some other agency’s ATO to start, that would be very helpful.*  
– Agency CIO

**FINDING #5****New Tools Have the Potential to Accelerate Cost Savings and Infrastructure Rationalization.**

The application of tools such as continuous monitoring and power metering have also led to significant savings in modern data centers. This can lead to significant improvements in economies of scale, procurement efficiencies, effective security controls, and application development and deployment schedules.

# Notes

1. Excluding the Department of Defense from the total, these numbers become \$50.7B total, \$17.3B in infrastructure, making up 21% of the total. Source: President's IT Budget for FY 2017. 2/25/2016. [https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17\\_agency\\_submission\\_topline.pdf](https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17_agency_submission_topline.pdf)
2. DigitalGov. "Laying the Foundation for a More Secure, Modern Government". 10/28/2016. <https://www.digitalgov.gov/2016/10/28/laying-the-foundation-for-a-more-secure-modern-government/>
3. Estimates are dependent on methods of data collection. For example, estimates and methods of collection included in this range: FY 2017 Federal IT Dashboard; investments reported since FY 2003 in the "IT Portfolio" portion of the agency's budget request (formerly known as the "Exhibit 53"); investments in the FY 2011-2012 budget requests including "End User Services and Support," "Mainframes and Servers Services and Support," and "Telecommunications Services and Support"; Commodity IT spending areas used in FY 2012 PortfolioStat; and IT infrastructure spending summary categories used in agency budget requests FY 2015-2016
4. "IT Infrastructure" historically includes spending on data centers, server equipment, network routers and switches, as well as other telecommunications equipment connecting these devices together. In addition, at times, OMB has also asked agencies to include spending on end user devices, office automation software (i.e., Microsoft Office applications), and IT security spending in the same budget reporting category
5. <https://www.icann.org/news/blog/ipv6-the-future-is-now-more-than-ever>
6. Source: Federal IT Dashboard, IT Infrastructure Spending Summary data feed. <https://www.itdashboard.gov>
7. Source: Historical Exhibit 53s and IT Portfolios of agencies, as provided by OFCIO; includes archived data from Federal IT Dashboard, IT Infrastructure Spending Summary data feed. <https://www.itdashboard.gov>
8. A data center is a room or building that houses computer systems and associated components that are used for the storage, management, and dissemination of data and information. OFCIO Memorandum. Implementation Guidance for the Federal Data Center Consolidation Initiative. 3/19/2012. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/cio\\_memo\\_fdcci\\_deliverables\\_van\\_roekel\\_3-19-12.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/cio_memo_fdcci_deliverables_van_roekel_3-19-12.pdf)
9. Since the 1990s, the number of data centers operated by the Federal Government has grown from several hundred to more than ten thousand as of November 2015. GAO-16-323. Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established. 3/4/2016. <http://www.gao.gov/assets/680/675592.pdf>
10. GAO-11-318SP. Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue. 3/1/2011. <http://www.gao.gov/new.items/d11318sp.pdf>
11. GAO-16-325. Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance. 4/2016. <http://www.gao.gov/assets/680/676395.pdf>. Original data source: <https://itdashboard.gov>
12. M-08-05. Implementation of Trusted Internet Connections. 11/20/2007. <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf>
13. Top 10 agencies by Sum of public cloud, hybrid cloud, and private cloud FY 2016 spending from Federal IT Dashboard. "Data Feed: Provisioned Services". <https://itdashboard.gov/drupal/data/datafeeds?format=csv>
14. OMB Memorandum. Launch of Information Technology (IT) Infrastructure Optimization, Geospatial, and Budget Formulation and Execution Lines of Business and Task Force Formations. 3/3/2006. <https://www.fgdc.gov/organization/coordination-group/meeting-minutes/2006/march/LOB%20Taskforce%20Memo.pdf>. For more detailed information about the Lines of Business, see Policy Chapter D: Federal Shared Services
15. The first round of metrics included: total cost per device, total cost per user, cost per help-desk contact, mission-critical service restoration percentage, help-desk speed-of-answer percentage, and help-desk first-contact resolution percentage. Jason Miller. FCW. "IT Infrastructure LoB Issues First Metrics". 11/16/2007. <https://fcw.com/articles/2007/11/16/it-infrastructure-lob-issues-first-metrics.aspx>
16. Enterprise architecture is defined as "a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy." Federation of EA Professional Organizations. Common Perspectives on Enterprise Architecture, Architecture and Governance Magazine. Issue 9-4. 11/2013. See also Technical Reference Model - Federal Enterprise Architecture Practice Guidance. 11/2007. [https://www.whitehouse.gov/sites/default/files/omb/assets/fea\\_docs/FEA\\_Practice\\_Guidance\\_Nov\\_2007.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_Practice_Guidance_Nov_2007.pdf)
17. M-11-29. Chief Information Officer Authorities. 8/8/2011. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf>
18. For example, the FDCCI, the Federal Cloud Computing Strategy, and the 25 Point Implementation Plan to Reform Federal Information Technology Management
19. OFCIO Memorandum. Federal Data Center Consolidation Initiative. 2/26/2010. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/federal\\_data\\_center\\_consolidation\\_initiative\\_02-26-2010.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal_data_center_consolidation_initiative_02-26-2010.pdf)
20. OFCIO Memorandum. Federal Data Center Consolidation Initiative Update Memo. 7/20/2011. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/fdcci-update-memo-07202011.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fdcci-update-memo-07202011.pdf)
21. GAO-16-323. Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established. 3/4/2016. <http://www.gao.gov/assets/680/675592.pdf>. GAO relied on OMB's FDCCI memo for their definitions of data centers (identified as "core" and "non-core")
22. For more information about PortfolioStat, see Policy Chapter A: Management and Oversight of IT
23. Vivek Kundra. State of Public Sector Cloud Computing. 5/20/2010. <https://cio.gov/wp-content/uploads/downloads/2012/09/StateOfCloudComputingReport-FINAL.pdf>





24. Vivek Kundra. 25-Point Implementation Plan to Reform Federal Information Technology Management. 12/9/2010. <https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>
25. Ibid. OMB told agencies to identify three “must move” services, where “at least one of the services must fully migrate to a cloud solution within 12 months and the remaining two within 18 months.” However, when OMB released IT budget guidance for the next fiscal year, there was no requirement for agencies to identify their “must move” services
26. Vivek Kundra. Federal Cloud Computing Strategy. 2/8/2011. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/federal-cloud-computing-strategy.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf)
27. Public Law No. 107–347. E-Government Act of 2002. 12/17/2002. <https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>
28. The Federal Risk and Authorization Management Program. For more about FedRAMP governance, see: <http://www.gsa.gov/portal/category/103271>. See also OFCIO Memorandum. Security Authorization of Information Systems in Cloud Computing Environments. 12/18/2011. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/fedrampmemo.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf). For more information about FedRAMP and securing the network, see Policy Chapter E: Cybersecurity
29. Full website available at: <https://marketplace.fedramp.gov>
30. FedRAMP.gov. “FedRAMP Forward”. [https://www.fedramp.gov/files/2015/08/FFSixMonthStatusReport\\_Infographic-2.pdf](https://www.fedramp.gov/files/2015/08/FFSixMonthStatusReport_Infographic-2.pdf)
31. Federal Information Technology Acquisition Reform Act. 12/19/2014. Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Public Law No: 113-291: <https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148>
32. M-16-19. Data Center Optimization Initiative. 8/1/2016. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m\\_16\\_19\\_1.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_19_1.pdf)
33. Part 3 in forthcoming FY 2018 CPIC reporting--previously Part 2
34. IT Dashboard. “Cost Savings”. <https://itdashboard.gov/drupal/cost-savings>
35. GAO-16-323. Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established. 3/4/2016. <http://www.gao.gov/assets/680/675592.pdf>
36. IT Dashboard. “Cost Savings”. <https://itdashboard.gov/drupal/cost-savings>
37. GAO-16-323. “Data Center Consolidation Agencies Making Progress, But Planned Savings Goals Need To Be Established”. 3/4/2016. <http://www.gao.gov/assets/680/675592.pdf>
38. Source: Historical Exhibit 53s and IT Portfolios of agencies, as provided by OFCIO; includes archived data from Federal IT Dashboard, IT Infrastructure Spending Summary data feed. <https://www.itdashboard.gov>
39. President George W. Bush. HSPD-12. Policy for a Common Identification Standard for Federal Employees and Contractors. 8/27/2004. <http://fas.org/irp/offdocs/nspd/hspd-12.html>. For more information about the 2015 Cybersecurity Sprint and PIV, see Policy Chapter E: Cybersecurity

# Open Data and Open Government

Information is a valuable national resource and a strategic asset to the Federal government, its partners, and the public. In order to ensure that the Federal government is taking full advantage of its information resources, executive departments and agencies...must manage information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguard systems and information.

OMB Open Data Policy – Managing Information as an Asset<sup>1</sup>

## Summary

 Stakeholders	Responsibilities and governance are widely distributed in this policy area. Some initiatives are led by the Federal CIO, while others come directly from The White House. GSA manages Data.gov and Project Open Data.
 Impact	To date, over 185,000 government datasets have been posted on Data.gov. However, it can be difficult to measure the broader economic and civic impacts of open data and open government efforts.
 Risk	While most CIOs reported interest in open government and open data initiatives, many expressed challenges in obtaining resources, navigating conflicts with existing policies, and balancing priorities against other efforts such as infrastructure modernization and cybersecurity.
 Policy	Efficiently managing government data and information can increase operational efficiencies, reduce costs, improve services, and better safeguard personal information. Making information resources accessible, discoverable, and usable by the public can help fuel entrepreneurship, innovation, and scientific discovery.

# Open Data and Open Government

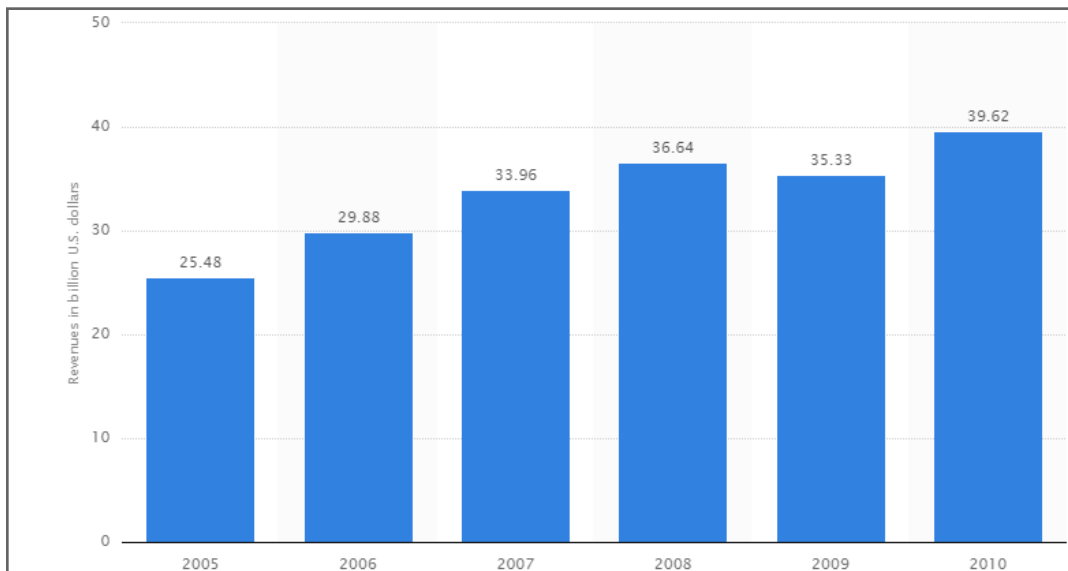
## Overview

The Federal government creates and collects a wide variety of valuable data and has long sought to provide citizens with the right and ability to access this information.<sup>2</sup> On the first full day of the Obama Administration, the President signed the Memorandum on Transparency and Open Government that recognizes information generated in the Federal government as a national asset. The memo established three central principles that set the tone for future efforts in this area: (1) transparency; (2) public participation; and (3) collaboration.<sup>3</sup> Making information and data accessible, discoverable, and usable by the public can transform citizen-facing services and help fuel entrepreneurship, innovation, and scientific discovery.<sup>4</sup> For example, the government's release of weather data and the Global Positioning System (GPS) allowed for the creation of navigation

systems (see Figure C1) and weather forecasting that fundamentally changed citizens lives and had a tremendous impact on the American economy.

Key to achieving both of these goals is the effective and efficient management of government information. Improving the management of government data and information can increase operational efficiencies, reduce costs, improve services, and better safeguard personal information. Furthermore, improved information management can allow for the efficient release and reuse of this data by others outside of an agency. The next section will discuss several of the strategies and initiatives that the Federal government has pursued to improve how agencies manage information and to provide more data to the public.

Figure C1: GPS Equipment Revenue in the United States between 2005 to 2010<sup>5</sup>



## Policy Evolution

Prior to 2009, government-wide efforts to bring government data into the public sphere were largely focused on meeting the requirements of the E-Government Act, which included establishing a public domain directory of Federal websites. This period also saw the creation of websites supporting a single business function or dataset (e.g., Regulations.gov in 2003),<sup>6</sup> and websites created as a result of other legislation (e.g., USASpending.gov in 2007).<sup>7</sup> Later efforts included the increased sharing of public resources which could become platforms for research, entrepreneurship, and innovation (e.g. the release of structured, machine-readable data pertaining to weather and climate).<sup>8</sup> In 2016, the primary government-wide strategy shifted “to focus more broadly on enterprise data governance and to emphasize the message that Open Data is an output of good data management and critical to success in areas like cybersecurity, customer service, and internal data-driven decisionmaking.”<sup>9</sup>

The recurring theme throughout all of these efforts was to improve transparency, accountability, and information management while providing the public with increased access to government information.

## Key Initiatives

- 2009** Transparency and the Open Government Directive
 

Lays out open government principles of being transparent, participatory, and collaborative. Establishes the Open Government Dashboard. Requires agencies to post information online in open formats, and to identify three high-value datasets to post on Data.gov.
- 2009 – present** Data.gov and the IT Dashboard
 

Citizen-facing websites designed to increase transparency and share government data directly with the public.
- 2011 – 2015** Open Government National Action Plans
 

Launches the “We the People” online petitions platform, promotes public participation, modernizes records and information management, improves FOIA administration.
- 2012** Digital Government Strategy
 

Directs the development and adoption of new open data, content, and web API policies. Requires agencies to identify two major customer-facing systems with information that can be exposed to the public via web-based APIs.
- 2013** Open Data Policy – Managing Information as an Asset
 

Requires standard machine-readable and open data formats, supports interoperability and information accessibility, establishes the Enterprise Data Inventory and public data listing.
- 2014** Open Data Action Plan and CAP Goals
 

Mandates collaboration with public and civil actors to identify and prioritize the release of new open data sets, incentivizes public outreach efforts such as challenges and industry roundtables, focuses Presidential Innovation Fellows on data innovation projects.

2009

## Transparency and the Open Government Directive

On President Obama's first day in office he issued a Transparency and Open Government memorandum based on three principles: transparency, public participation, and collaboration.<sup>10</sup> Later that year, an Open Government Directive was issued that, among other things, required the appointment of a senior agency official accountable for the quality of information presented via public-facing websites.<sup>11</sup> In addition, the Open Government Directive tasked agencies with creating an Open Government Plan, publishing agency information online in "open formats", and gave agencies a specific target of publishing three high-value data sets which were not previously publicly available, within 45 days. OMB later renewed agencies' focus on these approaches by updating instructions for Agency Open Government Plans in 2016.<sup>12</sup>

Transparency and the Open Government Directive	
Key Strengths	<ul style="list-style-type: none"> <li>• Jump-started the movement to release government datasets</li> <li>• Provided high-level executive support for government-wide efforts to improve transparency and accountability</li> <li>• Shared performance data with the public through web-based dashboards</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Like many other initiatives, raised expectations for agencies without providing additional resources</li> <li>• The focus of the initiative was frequently on counting the number of shared datasets rather than the data quality, value, or impact of released datasets</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Began the discussion of the potential value of open government and open data to customers</li> </ul>



2009-present

Data.gov and the IT Dashboard

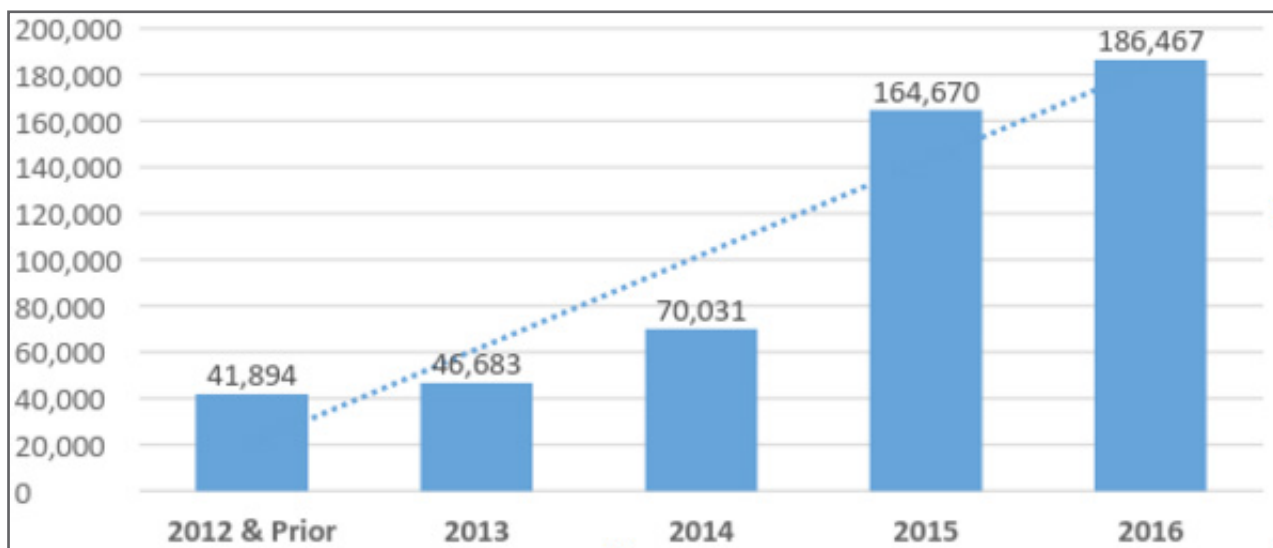
The Obama Administration launched several additional initiatives to improve the transparency of government spending on major IT investments and to provide a one stop shop for government datasets ranging from census data to public health information.

**Data.gov:** Data.gov, launched in May 2009, made an early push to publicize a broad range of agency datasets, ranging from consumer complaint data to information about 911 emergency service areas.<sup>13</sup> Currently, Data.gov lists 14 different sectors for which data is available.<sup>14</sup> However, in many cases the datasets are not available in open formats or easily machine-readable (e.g., PDF versus XML) or are not updated more often than once per year, limiting the usefulness of the data provided on the site.<sup>15</sup> Finally, Agencies maintain their data listings (publicly) and Enterprise Data Inventory (usually not posted publicly) as structured data files which can be read by Data.gov and OMB. The “impact” section of the Data.gov website includes a number of anecdotal examples of how these datasets are being used by private sector companies and the public.<sup>16</sup>

Data.gov	
Key Strengths	<ul style="list-style-type: none"> <li>Provides a one stop shop for government datasets</li> <li>Made government data more easily discoverable and searchable</li> <li>Supported the Obama Administration’s open government objectives</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>As the number of datasets increased, improved navigation, discovery, and search tools became necessary</li> <li>Efforts such as the Enterprise Data Inventory introduced a high degree of burden (cost), making it difficult for agencies to fully implement without additional support</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>Signaled a new government-wide approach to opening up data to the public</li> <li>Created a public-facing portal for government datasets to spark innovation (e.g., weather data)</li> </ul>

Open Data and Open Government

Figure C2: Data Sets Available on Data.gov increased by over 400% from 2012 - 2016<sup>17</sup>



**IT Dashboard:** In 2009, OMB publicly launched the Federal IT Dashboard with information as to whether major IT investments were on schedule and within budget, as well as an assessment by the agency CIO of the investment’s overall level of risk.<sup>18</sup> Currently, the IT Dashboard displays cost, schedule, and performance data for over 770 major federal IT investments accounting for \$81.5 billion in IT spending for FY 2016.

Federal IT Dashboard	
Key Strengths	<ul style="list-style-type: none"> <li>Improves transparency into major IT investments</li> <li>Makes data available so the public could see how agencies spend taxpayer dollars</li> <li>In 2015, the Dashboard began displaying whether agencies use agile or incremental development practices on IT projects</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>Variances both over budget and under budget are reported as negative conditions (as well as ahead of schedule and behind schedule), leading to some confusion</li> <li>The IT Dashboard draws from data that is self-reported by agencies, leading to questions about data quality and completeness</li> <li>Not all agencies have provided detailed, regular, up-to-date “Evaluations by Agency CIO” for all major investments</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>The IT Dashboard represents a major shift away from the static, document-driven approaches, toward live data visualizations</li> <li>The public can download and analyze the data themselves, increasing citizen engagement and oversight</li> <li>The IT Dashboard and TechStat sessions helped agencies, OMB, and Congress identify at-risk IT projects and implement corrective measures</li> </ul>

2011 – 2015

**Open Government National Action Plans**

In 2011, as part of the international Open Government Partnership, the Obama Administration launched the first in a series of National Action Plans (NAPs).<sup>19</sup> Many of the initiatives in the NAPs focused on enabling public participation and citizen engagement in government (e.g., the “We The People” online petitioning platform). The initiatives proposed in the last NAP (2015) continue to be implemented today and are connected with a number of other open government, open data, and citizen-facing digital service strategies, such as the CAP Goals.<sup>20</sup>

The special focus placed on improving Challenge.gov is an example of a NAP initiative from 2015. The Challenge.gov portal is designed to publish innovative opportunities for the public to engage in providing solutions to government challenges (e.g., providing veterans with better access to health services).<sup>21</sup> The NAP’s focus on Challenge.gov centered around making it easier for the average person to find the prizes and challenges that interested them by increasing both the accessibility of the available data and the number of participating agencies.

Open Government National Action Plans	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided additional support from the Obama Administration for open government efforts, both in project support and public communications</li> <li>• Created synergies with Administration focus on increasing government usage of digital tools and services</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Makes a number of “grand challenge” commitments where results are difficult to track</li> <li>• Engagement of offices outside of CIO organization have made it sometimes difficult for CIOs to focus on open government and open data efforts</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Led to the development of the “We the People” online petitioning platform</li> <li>• Improved the “Challenge.gov” platform to engage the public in providing solutions to solve government’s “mission-centric” problems</li> <li>• Initiated the development of the Federal Source Code Policy on reusable and open source software</li> </ul>

Open Data and Open Government

**NAP Grand Challenge Commitments**

- Improving Public Services
- Increasing Public Integrity
- More Effectively Managing Public Resources
- Creating Safer Communities
- Increasing Corporate Accountability

2012

## Digital Government Strategy

In May 2012, the Administration launched a Digital Government Strategy that sought to improve the delivery of citizen-facing digital services.<sup>22</sup> A primary focus of the strategy was to make the vast quantities of government data more easily available to the public.<sup>23</sup>

The strategy’s data-driven components emphasized both interoperability and accessibility. This involved the application of metadata tagging in order to make published datasets more easily searchable and the adoption of an API-first mindset to allow developers to create highly accessible mobile applications to draw upon those datasets. In addition, pursuant to the Digital Strategy, Data.gov was expanded to include a web API catalog for all Federal agencies to centrally aggregate agency APIs. Since August of 2013, the public has been able to access the features of these APIs in order to receive automatic data feeds. These feeds are particularly useful for IT software developers.<sup>24</sup> In addition, agencies were required to:

- Ensure all new IT systems follow the open data, content, and web API policy and operationalize agency.gov/developer pages.
- Engage with customers to identify at least two existing major customer-facing services that contain high-value data or content as first-move candidates to make compliant with new open data, content, and web API policy.
- Make high-value data and content in at least two existing major customer-facing systems available through web APIs.

- Apply metadata tagging and publish a plan to transition additional high-value systems.
- Establish new websites which hosted human-readable (HTML) and machine-readable (JSON) descriptions of their progress implementing each action and milestone.<sup>25</sup>

While there were a number of clear implementation outcomes that came from the Digital Government Strategy (e.g, the development of a web performance guidance<sup>26</sup> and customer experience metrics<sup>27</sup>), there is no available information about the overall impact of these initiatives and their success.

Digital Government Strategy	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided clear guidance (e.g., identify 2 high-value data sets)</li> <li>• Emphasized open data concepts such as accessibility and interoperability through metadata tagging</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• The strategy did not contain metrics to assess quality or accuracy of information released. As a result, it is unclear if agencies actually fulfilled the requirements of the policy</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• PortfolioStat reviews in 2013 and 2016 included the number of APIs developed by each agency in its key performance indicators (KPIs)</li> <li>• Agency compliance with the creation of the HTML and JSON files was never measured in PortfolioStat KPIs</li> </ul>

2013

## Open Data Policy – Managing Information as an Asset

On May 9, 2013, President Obama issued an Executive Order titled “Making Open and Machine Readable the New Default for Government Information” with the simple principle that “openness in government strengthens our democracy, promotes the delivery of efficient and effective services to the public, and contributes to economic growth.”<sup>28</sup> That same day, OMB issued an Open Data Policy highlighting the need to “manage information as an asset” and to “improve the discoverability and usability of existing datasets by making them “open.”<sup>29</sup> Under the Open Data Policy agencies were directed to:

- Use machine-readable and open formats;
- Use data standards;
- Ensure information stewardship through the use of open licenses;
- Use common core and extensive metadata;
- Build information systems to support interoperability and information accessibility;
- Create and maintain an Enterprise Data Inventory;
- Create and maintain a public data listing; and
- Create a process to engage with customers to help facilitate and prioritize data release.

A significant component of this policy was the establishment, maintenance, and use of an Enterprise Data Inventory. This requirement is based on the concept of if you cannot inventory your asset, you cannot manage or protect your asset.

OMB and the Office of Science and Technology Policy (OSTP) also launched Project Open Data as a clearinghouse for definitions, best practices, tools, case studies, and community interaction.<sup>30</sup> While obstacles to widespread adoption remain (e.g., limited agency budgets, competing policy priorities),<sup>31</sup> the policy helped shift agency focus in open data from simply releasing datasets to improving dataset usability.

Additionally, the Project Open Data Dashboard was launched to track metrics and OMB comments related to the completeness, accuracy, and use of agency open data materials across the following goals: Enterprise Data Inventory, Public Data Listing, Public Engagement, Privacy & Security, Human Capital, and Use & Impact.<sup>32</sup> Many of these metrics also appear at a government-wide aggregate level in the Open Data CAP Goal on Performance.gov.

Open Data Policy – Managing Information as an Asset	
Key Strengths	<ul style="list-style-type: none"> <li>• Reemphasized that data should be “open” by default</li> <li>• Expanded the meaning of “open data” to encourage more accessible and usable formats, licenses, and descriptions of datasets</li> <li>• Launch of Project Open Data</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Efforts such as the Enterprise Data Inventory introduced a high degree of burden (cost), making it difficult for agencies to fully implement without additional support</li> <li>• Open data efforts in some cases have a tension with existing policies</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• It is difficult to measure the impacts of open data policies because it is hard to quantify concepts such as data usability, transparency, and downstream innovation</li> <li>• Focused agency attention on the usability of datasets released</li> <li>• The Project Open Data Dashboard is used to publicly track a number of metrics for open data efforts</li> </ul>

2014

## Open Data Action Plan and CAP Goals

**Open Data Action Plan.** In May 2014, the Federal government released the Open Data Action Plan which summarized many of the Federal government’s accomplishments to date, while committing to new initiatives.<sup>33</sup> These commitments included expanding agencies’ use of “Data Jams” (workshops) and “Datapaloozas.”<sup>34</sup>

Numerous other approaches were also promoted by the Action Plan, including sector-specific feedback sessions with groups outside of government, incentive prizes, challenges, open-data-dedicated Presidential Innovation Fellows, appropriate licenses, and a list of detailed enhancements to specific datasets and data programs. Agencies were also tasked with a greater level of outreach to public, civil society, and private organizations in order to solicit input on what datasets should be prioritized for release. This effort was intended to increase both the usefulness of released government datasets and to spur additional opportunities for innovation within the private sector.<sup>35</sup>

**Open Data CAP Goal.** In 2014, the Open Data Cross-Agency Priority (CAP) goal was created to provide more comprehensive implementation and oversight mechanisms for open government and information management efforts.<sup>36</sup> Progress on these actions and measures have been published quarterly on the publicly-available Performance.gov website.<sup>37</sup> Agency progress has also been evaluated through the Project Open Data Dashboard, but those measures are not tightly integrated with other IT management processes (e.g., PortfolioStat). Summarizing performance across many of the aforementioned

strategies and initiatives, the CAP goal includes many of the metrics calculated on Project Open Data Dashboard at a government-wide level, in addition to updates from related initiatives. For example, one sub-goal describes actions agencies have taken to improve the overall usage of government datasets through outreach activities such as Datapaloozas, code-a-thons, and roundtables.

Open Data Action Plan and CAP Goals	
Key Strengths	<ul style="list-style-type: none"> <li>• Focused on public outreach through innovative techniques such as incentive prizes and “Datapaloozas”</li> <li>• Introduced a more comprehensive oversight mechanism for open data efforts through Performance.gov</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Many Open Data CAP sub-goals have shown a lack of agency progress or a decline from baseline levels<sup>38</sup></li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• 17% of agencies reported holding a datapalooza or other public outreach data event in FY 2016 Q3<sup>39</sup></li> </ul>

## Metrics and Oversight

### Primary Objective Emphasized in Metrics and Oversight

The primary objective of OMB's efforts in open data and open government has been to improve transparency, enable external innovation based on government resources, and increase public engagement. Because of the nature of these goals, directly measuring outcomes can be difficult. Therefore, OMB adopted a series of qualitative anecdotes as well as tracking key outputs of efforts along the way.

### Examples

Early efforts focused on counting datasets. Over time, OMB introduced more nuances to this approach, focusing on "high priority" datasets and developing a baseline of all datasets managed internally at each agency (enterprise data inventories). This count of datasets or percentage of datasets released became a KPI used in a number of years of PortfolioStat. Additionally, OMB established an Open Data CAP Goal which emphasized the importance of agency outreach to external organizations to understand how they are using publicly released datasets. Anecdotes based on dataset usage and counts of hackathon and Datapalooza events held by agencies became important parts of tracking public engagement. Finally, the Project Open Data Dashboard evaluates each agency based on dozens of calculations drawn from their public datasets, enterprise data inventories, and other agency reporting, such as how many bureaus at the agency had shared datasets. However, between PortfolioStat, the Open Data CAP Goal, and the Project Open Data Dashboard, there was no single place or metric to evaluate the complete picture of the government's progress on open data and open government across these different efforts and priorities.

### Lessons Learned

After the launch of Data.gov, OMB focused on the number of datasets released by each agency. It was quickly realized, however, that additional context to understand such a count was an important part of the story. With M-13-13, OMB required agencies to establish a baseline of all unreleased datasets against which the public count could be compared.

Realizing that simply creating more datasets may not match the objective of the policy area, agencies began to focus on soliciting and measuring feedback from the public through electronic means on their webpages or through in-person events such as hackathons and Datapaloozas. Though this was motivated by a recognition that measuring the impact and value of datasets would be important, these metrics still focus on counting events rather than gathering satisfaction and results information from external users of agency datasets.

These metrics have been augmented by anecdotes about private sector uses of public data posted to Data.gov's "Impact" page. These anecdotes, however, are difficult to compare between agencies, do not always make clear what the contribution of public data was to overall value, or how the anecdote connects to data available on Data.gov or agency websites. The Federal government is still looking for effective ways to measure the value and impact of released datasets, realizing that it is difficult to translate these concepts into quantifiable impact.

# Agency Observations and Findings

Although agency CIOs see value in open government and open data initiatives, they often have to focus their limited resources on other policy goals that may be more urgent. These efforts are further complicated by a large group of stakeholders that drive government-wide open government and open data efforts both simultaneously and independent of each other. Additionally, there are a number of existing laws and policies that can sometimes directly conflict with the principles of openness in government, including those dealing with records management, public information access, and cybersecurity. This has led to some uncertainty in agencies about the prioritization, measurement, and impact of open government and open data policies and initiatives.

## FINDING #1

### Agency CIOs Expressed Difficulty in Dedicating Resources to Open Government and Open Data Initiatives.

While many CIOs stated that they support the principles behind open government and open data efforts, they face challenges dedicating resources to these initiatives. Given limited budgets, support of mission activities takes precedence (e.g., modernizing agency IT infrastructure, strengthening cybersecurity protections). Finally, there are limited consequences should an agency decide not to implement open government initiatives, especially compared to the consequences from a public data breach or a disruption in network services.

*Everyone loves the concepts of open government and open data, but we don't get extra funding for it. To accurately collect this data requires hundreds of millions of dollars..."*

— Agency CIO



**FINDING #2**

**The Broad Range of Stakeholders Complicates Governance.**

Open government and open data tools and applications are widely available and accessible by stakeholders outside the traditional CIO community. Program offices, mission leads, and other agency officials can independently carry out open data initiatives, without needing the support of the agency CIO organization.

Our enterprise architect is working on open data efforts, and we release limited public data sets... but I'm not personally focused on it. Right now, open data is not a high-value initiative for our agency, but I think there will be more focus on this policy area in the future.

— Agency CIO

In addition, GSA, OSTP, and the White House lead numerous open government and open data efforts, often without significant engagement from the OFCIO or the CIO Council.

Implementation of the Digital Accountability and Transparency Act (DATA Act)<sup>40</sup> of 2014 follows a similar pattern. While this statute contains a significant number of IT-related open data provisions relevant to CIOs, current efforts are being driven primarily by the CFO community.

The ownership of open government and open data initiatives outside of the agency CIO organization can lead to conflicts between agency leadership and the CIO. Overall, the wide range of stakeholders can make it difficult for CIOs to engage in these efforts and ensure compliance with broader agency IT requirements (e.g., cybersecurity, privacy) and other policy initiatives. In addition, the recent appointments of Chief Data Officers at many agencies only adds to the complexity.

Key Organizations in Government-wide Open Government and Open Data Initiatives	
Lead Organization	Key Initiatives and Projects
OMB - Office of the Federal Chief Information Officer (OFCIO)	Open Government Directive, Open Data Policy, IT Dashboard, Open Data CAP Goal with GSA and OSTP
General Services Administration (GSA)	Data.gov, Project Open Data, Challenge.gov, Open311, Open Data CAP Goal with OMB and OSTP
The White House Office of Science and Technology Policy (OSTP)	Open Government National Action Plans (NAPs), Roundtables, Datapaloozas, "My Data" Initiatives, <sup>41</sup> Open Data CAP Goal with OMB and GSA
The White House Office of Administration	We The People
OMB - Office of Federal Financial Management (OFFM)	Digital Accountability and Transparency Act (DATA Act)

**FINDING #3****Existing Policies and Statutes Can Conflict with Open Data Efforts.**

Existing statutes and policies such as the Paperwork Reduction Act (PRA) of 1995, the Freedom of Information Act (FOIA) of 1966, the Privacy Act of 1974, and various records management policies and requirements were established prior to the advent of modern technologies and did not necessarily account for the ease of collecting, sharing, and connecting data sources in a digital government. This tension can complicate agency implementation of open data initiatives. For instance, agency CIOs expressed concern that the release of datasets could inadvertently create vulnerabilities or expose confidential information. Furthermore, as more datasets are released, new challenges can emerge – such as the “mosaic effect”, which allows sensitive information to be derived from the combination of multiple public datasets, despite the fact that each individual piece of data does not contain sensitive information. Ultimately, CIOs are struggling to balance adherence to legacy policies and laws in the context of open government and open data efforts.

**FINDING #4****Outcomes of Open Government and Open Data Efforts Can Be Hard to Gauge.**

Another challenge to the adoption of open government and open data initiatives is the difficulty in directly assessing their economic and civic impacts.<sup>42</sup> It is inherently difficult to directly measure outcomes as well as broader economic and social impacts of releasing data sets and other government information. As such, the primary focus has been on measuring leading indicators (e.g., number of datasets released on Data.gov) and highlighting success stories and anecdotes across the public and private sectors.<sup>43</sup> While open data progress is tracked via CAP Goals and various Government-wide public-facing websites such as the Project Open Data dashboard, they have not been a primary focus of PortfolioStat. As such, CIOs do not see measurement of these efforts as a priority for OMB, even as the number of requirements and initiatives in this policy area has expanded.

# Notes

1. M-13-13. Open Data Policy – Managing Information as an Asset. 5/9/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>
2. One of the earliest and most well-known efforts in this area is the Freedom of Information Act (FOIA) of 1966, which provides the public with access to the records of their government leaders. 5 U.S.C. § 552. Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings. 2012 edition. <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/html/USCODE-2012-title5-partI-chap5-subchapII-sec552.htm>
3. President Barack Obama. “Transparency and Open Government”. 1/21/2009. [https://www.whitehouse.gov/the\\_press\\_office/TransparencyandOpenGovernment](https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment)
4. According to a 2013 private sector report, “Open data can help unlock \$3 trillion to \$5 trillion in economic value annually across seven sectors.” The diverse sectors listed were: “Education, Transportation, Consumer products, Electricity, Oil and gas, Healthcare, and Consumer finance”. McKinsey Global Institute. “Open data: Unlocking innovation and performance with liquid information”. 10/2013. <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information>
5. Source: NPD Group. “Statistics”. <https://www.statista.com/statistics/199890/revenues-of-gps-equipment-in-the-united-states-since-2005/>
6. Regulations.gov was created pursuant to Section 206 of the E-gov Act of 2002. Public Law 107-347. The E-Government Act of 2002. 12/17/2002. <https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>. The site makes all proposed rules available online in a single location and allows the public to comment on proposed rules. As of 11/1/2016, the five most-commented regulations posted on Regulations.gov had received 704,531 public comments since the beginning of the year. Source: Regulations.gov. “Site Data.” <https://www.regulations.gov/siteData>
7. USASpending.gov was created under the Federal Funding Accountability and Transparency Act of 2006. Public Law 109-282. Federal Funding Accountability and Transparency Act of 2006. 9/26/2006. <https://www.gpo.gov/fdsys/pkg/PLAW-109publ282/pdf/PLAW-109publ282.pdf> and provides details regarding spending on Federal contracts and grants. The site was recently transferred from GSA to the Department of the Treasury pursuant to the Digital Accountability and Transparency Act (DATA Act). The DATA Act also greatly expanded the information contained on USASpending.gov to include nearly all federal expenditures. Public Law 113-101. Digital Accountability and Transparency Act of 2014. 5/9/2014. <https://www.gpo.gov/fdsys/pkg/PLAW-113publ101/content-detail.html>
8. In one example of data-driven entrepreneurship and innovation, the Climate Corporation utilizes data from the National Oceanic and Atmospheric Administration, National Weather Service, U.S. Geological Survey, Natural Resources Conservation Service, National Aeronautics and Space Administration. Source: Open Data 500. “Climate Corporation”. <http://www.opendata500.com/us/climate-corporation/>
9. Performance.gov. “Cross-Agency Priority Goal: Open Data”. FY 2016 Q3 Update. [https://s3.amazonaws.com/app\\_performance\\_prod\\_ahwdtloxscy/s3fs-public/FY%2016%20Q3%20Open%20Data%20FINAL.pdf](https://s3.amazonaws.com/app_performance_prod_ahwdtloxscy/s3fs-public/FY%2016%20Q3%20Open%20Data%20FINAL.pdf)
10. President Barack Obama. “Transparency and Open Government”. 1/21/2009. [https://www.whitehouse.gov/the\\_press\\_office/TransparencyandOpenGovernment](https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment)
11. M-10-06. Open Government Directive. 12/8/2009. [https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda\\_2010/m10-06.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf)
12. M-16-16. 2016 Agency Open Government Plans. 7/14/2016. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-16.pdf>
13. Peter Orszag. The White House Blog. “Democratizing Data”. 5/21/2009. <https://www.whitehouse.gov/blog/2009/05/21/democratizing-data>
14. These sectors are: Agriculture, Business, Climate, Consumer, Ecosystems, Education, Energy, Finance, Health, Local Government, Manufacturing, Ocean, Public Safety, and Science & Research. Source: Data.gov. “Browse Topics”. <https://www.data.gov/>
15. Data.gov has 36,529 (or 20%) of the total of 186,467 datasets are in PDF format. Source: Data.gov. “Data Catalog”. [http://catalog.data.gov/dataset#sec-res\\_format](http://catalog.data.gov/dataset#sec-res_format)
16. Data.gov. “Impact”. <https://www.data.gov/impact/>
17. Source: Data.gov. “Metrics”. <https://www.data.gov/metrics>
18. IT Dashboard. “Cost Savings”. <https://itdashboard.gov/drupal/cost-savings>
19. Whitehouse.gov. “Open Government National Action Plans”. Retrieved 11/4/2016. <https://www.whitehouse.gov/open-partnership/national-action-plans>
20. Anecdotal data (success stories, initiative highlights) can be found on Data.gov (<http://www.data.gov/impact/>). Additional measures can be found on Project Open Data Dashboard and the quarterly CAP Goals updates as reported on Performance.gov
21. GSA, in consultation with OSTP, developed the site and administers the approximately 700 challenges currently available. Challenge.gov. “Newest Challenges”. <https://www.challenge.gov>.
22. Whitehouse.gov. “Digital Gov”. <https://www.WhiteHouse.gov/DigitalGov>. See also, “Digital Government: Building a 21st Century Platform to Better Serve the American People”. 5/23/2012. <https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>
23. In addition to data and APIs, the strategy also emphasized mobile device usage and improving development to support the mobile experience.
24. Office of Management and Budget. FY 2012 Report to Congress on the Implementation of The E-Government Act of 2002. 3/2013. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/fy12\\_e-gov\\_act\\_report.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_e-gov_act_report.pdf)





25. OMB's IT Dashboard then aggregated agencies' reporting in real-time and summarized government-wide progress and each agency's performance, however this summary was removed from the IT Dashboard in 2015. Available through archive.org at: <https://web.archive.org/web/20130417085852/http://www.itdashboard.gov/digitalgov>. This method of publicly-transparent real-time automated reporting would be used later by OMB to measure agency progress implementing FITARA and the Data Center Consolidation Initiative. For more information about government-wide data center consolidation and optimization policies, see Policy Chapter B: IT Infrastructure Modernization
26. Digital.gov. "DAP: Digital Metrics Guidance and Best Practices". <https://www.digitalgov.gov/services/dap/dap-digital-metrics-guidance-and-best-practices/>
27. Digital.gov. "DAP: Digital Analytics Program". <https://www.digitalgov.gov/services/dap/>
28. President Barack Obama. Executive Order 13642: Making Open and Machine Readable the New Default for Government Information. 5/9/2013. <https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government>
29. President Barack Obama. "Making Open and Machine Readable the New Default for Government Information". 5/9/2013. <https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government>
30. Project Open Data. "Open Data Policy – Managing Information as an Asset". <https://project-open-data.cio.gov/>
31. For a more detailed explanation of these obstacles, see the finding below: "Agency CIOs Expressed Difficulty in Dedicating Resources to Open Government and Open Data Initiatives"
32. Data.gov. "Dashboard". <https://labs.data.gov/dashboard/offices>
33. The White House. "U.S. Open Data Action Plan". 5/9/2014. pp. 2-6. [https://www.whitehouse.gov/sites/default/files/microsites/ostp/us\\_open\\_data\\_action\\_plan.pdf](https://www.whitehouse.gov/sites/default/files/microsites/ostp/us_open_data_action_plan.pdf)
34. Datapaloozas are informational events intended to highlight innovation within the private, nonprofit, and academic sectors who have utilized the government's datasets to build useful and creative products, services, and applications. Data.gov. "Safety". <https://www.data.gov/safety/white-house-safety-datapalooza>
35. In 2016 alone, the White House and OSTP have highlighted a variety of public data-related initiatives occurring in partnership with agencies, including: the Police Data Initiative, the Precision Medicine Initiative (and Summit), Open Data Day DC, the Open Data Summer Camp Open House, Datapaloozas, and various open data roundtables with industry leaders. Source: The White House. Fact Sheet: Data by the People, for the People – Eight Years of Progress Opening Government Data to Spur Innovation, Opportunity, & Economic Growth. 9/28/2016. <https://www.whitehouse.gov/the-press-office/2016/09/28/fact-sheet-data-people-people-eight-years-progress-opening-government>
36. Ownership of the Open Data CAP Goal is shared by by OFCIO, OSTP, and the Department of Transportation
37. Performance.gov. "Cross-Agency Priority Goal: Open Data". FY 2016 Q2 Update. <https://www.performance.gov/content/open-data#supporting-info>
38. Performance.gov. "Cross-Agency Priority Goal: Open Data". FY 2016 Q3 Update. [https://s3.amazonaws.com/app\\_performance\\_prod\\_ahwdtloxcxcy/s3fs-public/FY%2016%20Q3%20Open%20Data%20FINAL.pdf](https://s3.amazonaws.com/app_performance_prod_ahwdtloxcxcy/s3fs-public/FY%2016%20Q3%20Open%20Data%20FINAL.pdf)
39. "Cross-Agency Priority Goal: Open Data". FY 2016 Q3 Update. [https://s3.amazonaws.com/app\\_performance\\_prod\\_ahwdtloxcxcy/s3fs-public/FY%2016%20Q3%20Open%20Data%20FINAL.pdf](https://s3.amazonaws.com/app_performance_prod_ahwdtloxcxcy/s3fs-public/FY%2016%20Q3%20Open%20Data%20FINAL.pdf)
40. Public Law 113-101. Digital Accountability and Transparency Act of 2014. 5/9/2014. <https://www.gpo.gov/fdsys/pkg/PLAW-113publ101/pdf/PLAW-113publ101.pdf>
41. "My Data" initiatives, such as the Blue Button (for healthcare) and Green Button (for energy usage), are designed to give Americans secure electronic access to their own personal data
42. Júlia Keserű. "A new approach to measuring the impact of open data". The Sunlight Foundation. 5/5/2015. <https://sunlightfoundation.com/blog/2015/05/05/a-new-approach-to-measuring-the-impact-of-open-data/>
43. See: <https://data.gov/impact> for examples

# Federal Shared Services

To become more efficient, government needs to reach the point where sharing or merging functions is routine, making use of scarce but critical expertise and building high-quality capacity through economies of scale. It requires agency leaders to make critical choices about what their organization does well and what makes sense to obtain from others who can provide best-in-class services.

— Partnership for Public Service - A Call to Action on Shared Services<sup>1</sup>

## Summary

 <p>Cost</p>	<p>The use of shared services is estimated to generate between \$21.0 billion and \$47.2 billion in cost savings between 2015 and 2025. Once fully utilized, total savings and cost avoidance are estimated at \$47 billion per year.</p>
 <p>Policy</p>	<p>The goal of shared services is to efficiently aggregate resources and systems to improve the quality, timeliness, and cost effectiveness of service delivery to customers. The Unified Shared Services Management (USSM) office was created to drive shared service adoption and establish a high-performing marketplace that leverages proven best practices in service delivery and performance.</p>
 <p>Risk</p>	<p>Sporadic agency adoption of shared services continues due to concerns about quality and expertise of providers, the lack of standard, government-wide requirements, and the challenges of transferring funds between agencies.</p>
 <p>Accountability</p>	<p>USSM recently launched ProviderStat to measure performance and drive accountability across shared service providers to improve customer satisfaction, transparency, and, ultimately, increase shared service adoption.</p>

# Federal Shared Services

---

## Overview

A shared service is a business or mission function that is provided for consumption by multiple organizations within or between Federal agencies. There are approximately 300 Executive Branch organizations of various magnitudes and missions, and over 10,000 IT systems across the Federal government. Through the use of shared services, there is tremendous opportunity to drive efficiencies and cost-savings in many functions such as Human Resources and Financial Management. For example, a 2012 review of Federal agency IT investments revealed significant redundancies and identified billions of dollars in potential savings that could be achieved by adopting a shared approach to IT service delivery both inside and across agencies.<sup>2</sup>

The goal of shared services is to efficiently aggregate resources and systems to improve the quality, timeliness, and cost effectiveness of service delivery to customers. By leveraging government-wide economies of scale, agencies can reduce administrative burdens and increase collaboration, allowing more time to focus on core mission functions. Furthermore, *intra-agency* shared services can also be impactful in improving mission function, reducing costs, and increasing collaboration across an agency.

Federal shared services continue to evolve. While some challenges in shared service implementation have already been addressed, the government will only begin to benefit from economies of scale in technology if agencies agree on baseline common requirements that satisfy

*We have a culture of every agency doing 100 percent of its own work most of the time, absent of a few shared services...And not just at the agency level, but sometimes well below that. There's tons and tons and tons of uniqueness."*

— Federal CIO Tony Scott<sup>3</sup>

agencies of all sizes. Recognizing that agencies will have their own requirements based on existing business processes, gathering customer requirements on a systematic basis will help identify a more appealing shared service solution. By empowering shared service providers and their associated change management boards, these customer requirements can be built, as appropriate, into their service offerings. Potential cost savings are not insignificant. For example, “for government-wide back-office operations, the conservative range of cost savings over 10 years is estimated to be between \$21.0 billion and \$47.2 billion. Once shared

services are implemented, total savings and cost avoidance from the annual budget would be approximately up to \$47 billion per year”<sup>4</sup> (see Figure D1).

Recent fiscal pressures, cyber vulnerabilities, rising customer expectations, hiring limitations, and the need to deliver IT solutions more efficiently provide significant incentives for agencies to share services government-wide.<sup>5</sup> Agency adoption of shared services has historically proven to be an arduous task. Successful adoption government-wide will require sustained executive leadership and support from within the agency itself and from the next Administration.

Figure D1: Projected Cost Savings Through the Use of Shared Services (2015-2025)<sup>6</sup>

CALCULATION INPUTS	CUMULATIVE ESTIMATED COST SAVINGS PROJECTED OVER 10 YEARS <sup>7</sup>	
	COST SAVINGS (LOW)	COST SAVINGS (HIGH)
Cost savings	\$24.8 billion	\$55.9 billion
Migration and transition costs	-\$6.5 billion	-\$14.5 billion
Continuous improvement	\$2.6 billion	\$5.8 billion
<b>TOTAL COST SAVINGS AND COST AVOIDANCE</b>	<b>\$21.0 billion</b>	<b>\$47.2 billion</b>

# Policy Evolution

The benefits of shared services are well known to the Federal government. Though hurdles still need to be overcome for broad adoption, sharing responsibilities for common tasks both within an agency and among agencies can reduce duplicative investments, thus conserving resources and achieving efficiencies.

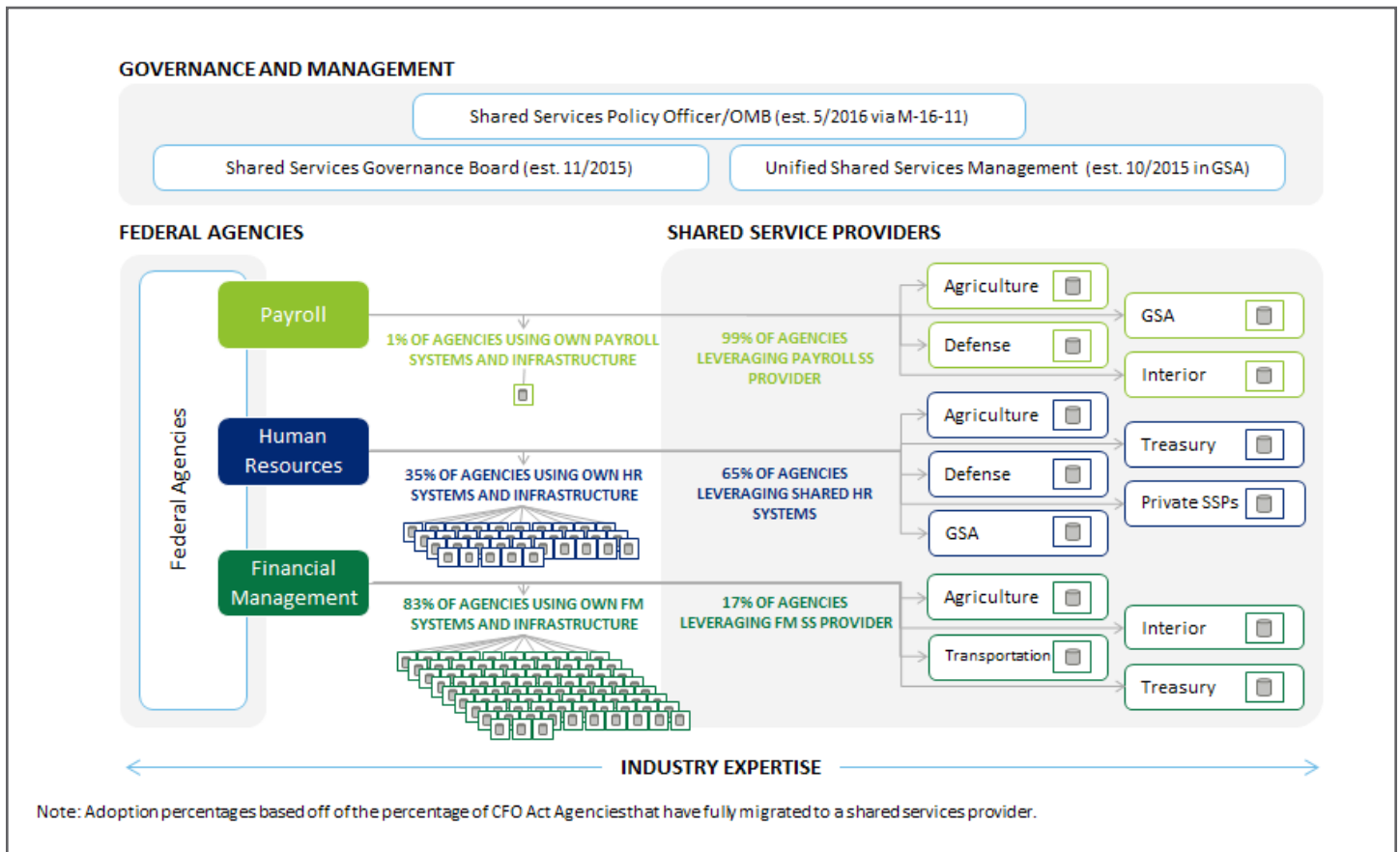
Currently, there are five Federal agencies offering shared services across two lines of business (LoBs) - Human Resources (encompassing Payroll and other services) and Financial Management. As shown in the figure below, the Human Resources

LoB has the highest rate of adoption across government, 99 percent for Payroll and 65 percent for core Human Resources systems. Given the potential for further cost savings and cost avoidance, significant opportunities remain for additional adoption of these shared services.

### Key Stakeholders

- Unified Shared Services Management (USSM) – GSA
- Federal Acquisition Service (FAS) – GSA
- Office of Financial Innovation and Transformation (FIT) – Treasury

Figure D2: Shared Service Providers<sup>7</sup>



Federal Shared Services



## Key Initiatives

Over time, government-wide policies and initiatives to encourage and increase shared services have shifted from a top-down mandatory approach towards building a shared services marketplace. For example, the new Unified Shared Services Management Initiative (USSM) at GSA lays out a comprehensive organizational structure for shared services efforts across the Federal government. This shift is discussed in the next section of this paper, including a summary of key government-wide strategies and initiatives.

**2001**

### E-Government Initiatives

Sets up cross-agency initiatives to provide services to citizens, business, and government through Internet-based tools and technologies. Initiatives included Benefits.gov, Grants.gov, and USAJOBS.gov.

**2004**

### Lines of Business

Designates managing partner agencies and task forces to address areas of shared government-wide business support functions (e.g., human resources management, financial management, grants management).<sup>8</sup>

**2011**

### Intra-Agency Commodity IT Services

Directs agency CIOs to leverage their agency's purchasing power to eliminate duplication of IT investments. Instructs agency CIOs to show a preference for the use of shared services, either as a customer or as a provider.

**2012**

### Shared-First

Requires the adoption of shared services whenever applicable, identifies provider agencies and delivery models, and the identification of two IT areas for migration to a shared service.

**2013  
– 2015**

### Uncle Sam's List

Implements the market research component of the Shared-First strategy, provides a location for users to find and connect with service providers, and supplies additional implementation guidance to agencies.

**2013  
– present**

### Financial Management Shared Services

Mandates the use of shared service solutions for future modernizations of core accounting systems, provides an analysis process for existing Federal shared service providers, and outlines communities to facilitate shared service adoption.

**2015**

### Unified Shared Services Management

Created at GSA to foster a Federal shared services environment that emphasizes good government, consumer satisfaction, and service provider innovation.<sup>9</sup>

Supporting OMB memo M-16-11<sup>10</sup> establishes a review process for new financial management, human resources, or acquisition system investments and their alignment with shared service options, establishes USSM as the managing partner for ProviderStat, and provides new implementation and oversight guidance.

2001

**E-Government Initiatives**

In 2001, OMB established an E-Government Task Force to examine opportunities for government-wide common service solutions, many of which were citizen-facing.<sup>11</sup> The resulting projects became known as the E-Government Initiatives and focused on four general service areas: service to individuals, service to businesses, intergovernmental services, and internal efficiency and effectiveness.

E-Government Initiatives	
Key Strengths	<ul style="list-style-type: none"> <li>• Led to initial improvements in the way that citizens interact with the government using the Internet</li> <li>• Focused on specific government-wide service offerings, such as one-stop websites and payroll consolidation</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Mandating use of a shared service can lead to lower quality service levels if governance does not adequately incorporate customer feedback</li> <li>• Services addressed by this initiative did not necessarily prioritize the highest potential value opportunities</li> <li>• Requiring interagency funding transfers to pay for services can draw additional scrutiny or oversight</li> <li>• Migrations took a long time to complete</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Paved the way for future shared service offerings</li> <li>• Many of the citizen-facing websites originally created by E-Government Initiatives are still active today: Grants.gov, Benefits.gov, Recreation.gov, and USAJobs.gov</li> </ul>

## 2004

### Lines of Business

In 2004, the initial shared services Lines of Business (LoBs) were established to improve the internal operations of Federal agencies and further reduce duplicative IT spending. Cross-agency teams identified Financial Management, Human Resources Management, and Grants Management as key opportunities for integration and consolidation.<sup>12</sup> The LoB approach then designated government-wide service providers and sought to drive customer agency migrations to those providers. At present, the Shared Services CAP Goal highlights the Lines of Business for Human Resources Management (HR LoB) and Financial Management (FM LoB) which illustrates the continued commitment to these efforts.<sup>13</sup>

Lines of Business	
Key Strengths	<ul style="list-style-type: none"> <li>Early exploration of the value of interagency collaboration on standardizing common business processes</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>Required strong and consistent engagement by OMB and agency leadership to drive use of services provided by the Lines of Business</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>There are a number of active LoBs still in existence today, such as the Human Resources LoB, Budget Formulation and Execution LoB, and Financial Management LoB</li> </ul>

### Initial Lines of Business

- Case Management (CM)
- Financial Management (FM)
- Human Resources Management (HR)
- Grants Management (GM)
- Federal Health Architecture (FHA)

2011

## Intra-Agency Commodity IT Services

The difficulties surrounding adoption of shared services within agencies led the Administration to include a shared services effort in its 2010 IT Reform Plan, the 25-Point Implementation Plan to Reform Federal IT Management.<sup>14</sup> As it relates to shared services, the focus was on consolidating intra-agency commodity IT services. Commodity IT includes areas of common functionality such as e-mail, desktop computers, mobile devices, financial systems, human resources systems, and other administrative systems.<sup>15</sup> To accelerate the adoption of shared services in commodity IT, OMB directed agencies to first examine the possibility of adopting shared services either as a provider or consumer before considering the adoption of one-off independent licenses or agreements.

Intra-Agency Commodity IT Services	
Key Strengths	<ul style="list-style-type: none"> <li>Required agencies to establish plans to replace redundant commodity IT services with consolidated or enterprise services</li> <li>Developed cost savings targets used to track future PortfolioStat-related savings</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>While examples of commodity IT were listed, no formal definition was provided, leading to ambiguity and potential confusion</li> <li>Encouraged agencies to consolidate but did not offer significant solutions to policy, legal, and management challenges</li> <li>PortfolioStat efforts after the first year did not follow-up on the progress of commodity IT consolidation plans</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>Provided cover for agencies to replace disparate systems and services with consolidated and enterprise approaches</li> <li>Established cost savings targets for new investments</li> </ul>

2012

**Shared-First**

Shared-First<sup>16</sup> was an effort to consolidate and improve upon the shared services developed in the E-Government Initiatives, Lines of Business, and commodity IT. Shared-First, as described in the 2012 Federal Information Technology Shared Services Strategy, sought to improve return on investment and close productivity gaps through the use of shared services.<sup>17</sup> Key requirements for agencies included:

- Identification of two IT areas for migration to a shared service approach; and
- Submission of an enterprise roadmap that included the agency’s Commodity IT Consolidation Plan and LoB Service Plan.<sup>18</sup>

Shared-First	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided agencies with standardized vocabulary and guidance on business models</li> <li>• Identified responsibilities for various shared services stakeholders, identified available funding models, and defined critical factors for success</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Policy requirements were a good start, but did not go beyond basic guidance (e.g. “two IT areas for migration to a shared service approach”)<sup>19</sup></li> <li>• Despite the “Shared-First” principle, OMB continued to accept budget requests for agency expansion of non-shared systems with no negative consequences</li> <li>• Agencies often did not have the IT infrastructure<sup>20</sup> necessary to provide efficient and effective shared services to the Federal community</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• Agencies chose “low-hanging fruit” when selecting services to meet OMB’s “two IT areas for migration to a shared service approach”</li> <li>• There is no evidence of follow-up on the success or failure of each agencies selected “two areas for migration” or to determine whether agencies progressed to more advanced services over time</li> </ul>

2013 – 2015

## Uncle Sam's List

Another key challenge facing shared services adoption has been the difficulty that agencies encounter when trying to identify providers and solutions. To address this issue, OMB launched Uncle Sam's List (USL) in 2013 as an online marketplace that cataloged available shared service providers, contracts suitable for use by multiple agencies, and other opportunities for agency collaboration.<sup>21</sup>

The goal of USL was to connect government service providers with potential customers the way popular commercial sites like Craigslist did so for housing, jobs, and professional services. Providers could post available services and contracts. Potential customers could post requests for services that matched their needs. Though the service offerings were centralized, continued rates of low adoption led OMB to pivot toward the broader-scoped USSM program and terminated USL in 2015.

Uncle Sam's List	
Key Strengths	<ul style="list-style-type: none"> <li>Explored a "marketplace" approach to connecting service providers with potential customers</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>Ambiguous service level agreements, competitive offerings from commercial providers, and low trust between potential customers and Federal providers resulted in low customer interest</li> <li>Limited agency outreach, accessibility challenges, and lack of breadth in service offerings reduced adoption potential</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>Voluntary adoption of offered services was low</li> <li>Uncle Sam's List was not widely used and was eventually discontinued</li> </ul>

2013 – present

**Financial Management Shared Services**

In 2013, OMB’s Office of Federal Financial Management (OFFM) looked to shared services as a means to reduce costs and improve the state of government-wide financial management. OMB required CFO Act agencies to halt all financial system modernization projects with \$20 million or more in planned development or modernization spending, pending an agency re-evaluation of shared services alternatives and a further review by OMB.<sup>22</sup>

In order to mitigate risks and decrease costs, the Department of the Treasury’s Office of Financial Innovation and Transformation (FIT) was established as a pilot office for new shared service solutions in the area of financial management systems. Some of the approaches attempted in this initiative were later applied in the Unified Shared Services Management effort discussed below.

Financial Management Shared Services	
Key Strengths	<ul style="list-style-type: none"> <li>• Provided standards, migration guidance, implementation frameworks, and other tools designed to assist agencies in selecting government or commercially-based financial management shared services</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>• Difficult to customize provider service offerings for diverse agency business process needs</li> <li>• Potential customer agency business processes were often difficult to reengineer to match available offerings</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>• The effort acted as a pilot program for other shared services adoption government-wide, focusing on a mission-critical system to start</li> </ul>

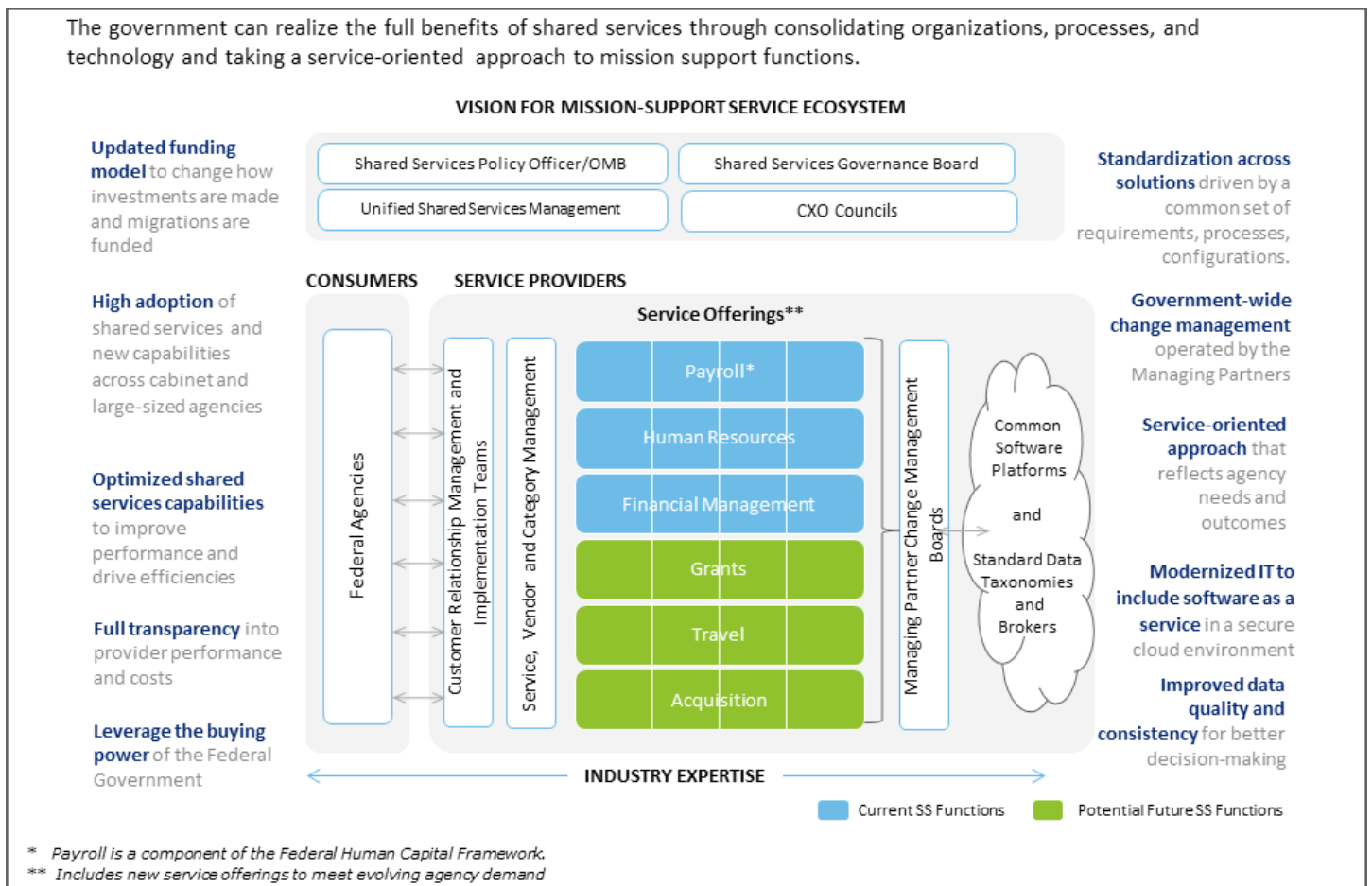
2015

## Unified Shared Services Management (USSM)

In late 2015, the push for broad adoption of Federal shared services was renewed once more with the establishment of USSM.<sup>23</sup> USSM was placed within the Office of Government-wide Policy at GSA, providing management of the Federal shared services ecosystem. USSM's government-wide perspective includes efforts related to the original LoBs, commodity IT, the Shared-First Initiative, and financial systems modernization. At present there is a strong focus on cross-administrative functions, Financial Management, and Human Resources, as reflected in the current Shared Services CAP Goals. Much of USSM's role was defined in OMB Memorandum M-16-11.<sup>24</sup>

Primarily, USSM is charged with establishing a long-term vision to optimize a service delivery model for the Federal government that addresses capacity, funding, and technology challenges of today and creates a balanced marketplace of commercial and Federal providers. USSM also aligns agency demand to the possible expansion of supply, creates best practices to ensure successful implementation, and establishes a performance management framework for transparency into FSSP operations and metrics. The figure below depicts this future state of shared services operations for mission support functions.

Figure D3: Future Concept of Operations for Mission-Support Functions<sup>25</sup>



Federal Shared Services



Unified Shared Services Management	
Key Strengths	<ul style="list-style-type: none"> <li>Provides guidance and support to both shared service providers and customers, as well as management and oversight from an enterprise-wide perspective</li> </ul>
Key Challenges	<ul style="list-style-type: none"> <li>Previous challenges experienced with other shared services efforts still exist including different approaches to Service-Level Agreements (SLAs), migration timing, customer service burdens, concerns over the assumption of risk, and provider performance management</li> </ul>
Policy Impact	<ul style="list-style-type: none"> <li>USSM has worked with the Shared Service Governance Board, providers, and customers to craft a 10-year vision for service delivery of administrative functions</li> <li>Over the long-term, USSM will help agencies realize the full benefits of shared services through consolidating organizations, processes, and technology and taking a service-oriented approach to mission support functions</li> <li>Creating a centralized support office should help agencies manage their migrations and can help mitigate regulatory and policy barriers to implementation</li> </ul>

## Metrics and Oversight

### Primary Objective Emphasized in Metrics and Oversight

OMB and GSA have promoted shared services because agencies can leverage commonly-skilled resources to perform transaction work at lower costs, focus less on maintaining and modernizing systems and more on data analytics and mission work, and benefit from standardized processes that produce efficient outcomes.

Though the shared services marketplace is generally thought of as comprising the four designated Financial Management providers, there are actually more agencies offering niche services across the government. In 2016, the director of USSM, Beth Angerman, observed that, “[t]he market for Federal shared services is more than \$1 billion a year and growing as agencies struggle to sustain their own systems and hire the right resources. Because we have an expansive marketplace, it’s important that the government expects cost and pricing transparency, coupled with consistent performance metrics, to ensure that the solutions are meeting customer demand.”<sup>26</sup>

### Examples

*Report to Congress on the Benefits of the E-Government Initiatives and Lines of Business.* While OMB’s focus on shared services was based on both operational efficiencies and cost savings, the limited availability of such measures led to a focus on qualitative anecdotes. As these initiatives progressed, additional metrics and assessments evaluated adoption and performance of shared services. Some inconsistencies across these metrics made it difficult to accurately compare data from year to year.

*PortfolioStat 2012.*<sup>27</sup> To promote adoption of Federal shared services, OMB directed agencies to identify opportunities to consolidate commodity IT functions – including both intra-agency and government-wide shared services. In the 2012 PortfolioStat process, OMB identified potential savings of \$2.5B over 3 years through the reduction of duplicative investments; however, those savings were not solely attributable to the use of shared services.<sup>28</sup> While shared services savings have been reported by individual managing partner agencies (e.g., OPM reported \$1.3B in cost savings and avoidance for HR LoB through FY 2014),<sup>29</sup> savings achieved through the use of shared services have not been measured in the aggregate through either PortfolioStat or CAP Goal Quarterly Progress Updates. In addition, the 2013 PortfolioStat process shifted the focus away from the consolidation of commodity IT.<sup>30</sup> Although agencies established Commodity IT Consolidation Plans as a part of PortfolioStat 2012, there is no evidence OMB followed-up on these plans in subsequent years or asked agencies to send updated status of in-progress projects or results of completed projects.

**GSA Benchmarking Initiative.** Beginning in 2013, GSA's Benchmarking Initiative built on the commodity spending areas originally identified in the first PortfolioStat. Agencies reported to GSA on their total and per-head spending in a variety of back-office or management areas for each of their bureaus and overall. This included the areas of human resources and financial management as well as a few sub-categories of IT.

In future years, the Benchmarking Initiative added more customer satisfaction and operational efficiency metrics. Together, these cost, satisfaction, and operations metrics helped OMB and agencies identify which agencies were leaders in common management functions and direct underperforming agencies toward those

leaders. In some cases, OMB focused on expanding the ability of those leaders to directly serve other agencies as shared service providers, a focus elaborated on in the Financial Management LoB, HR LoB, and FedStat efforts.

**Shared Services CAP Goal.** OMB helped to expand and support these management services through efforts reported under the Shared Services CAP Goal on Performance.gov.<sup>31</sup> This CAP goal publishes quarterly updates of the progress of the FM LoB and HR LoB, as well as overall metrics evaluating government use of shared services. Like other CAP Goals, the agency and government-wide leaders of this Goal meet regularly and OMB leadership conducts a "deep-dive" into the plans and progress of the Goal.

### *USSM M3 Framework and ProviderStat.*

In August 2016, USSM released the Modernization and Migration Management (M3) Framework, a process for agencies to follow when planning for the replacement of administrative IT solutions or services. M3 helps guide agencies through the planning, selection of a provider, and implementation of shared services. This framework includes an Investment Review Process, with OMB, provider, and customer involvement, to assess the health of the migrations in a repeatable and consistent way.<sup>32</sup> It is too early to evaluate the impact of USSM's use of this framework, but according to its website "all agencies evaluating an administrative (e.g. financial management, human resources, or acquisition) system and/or service modernization or migration must comply with M3."

Another component of the USSM approach is ProviderStat, a performance management framework that demands transparency into provider costs and pricing, performance metrics, and a maturity assessment based on provider best practices established by the Shared Service Governance Board. ProviderStat will identify common challenges that providers face today, opportunities for USSM and OMB to assist in resolution of those issues, and data to compare the overall performance of the marketplace. This data will assist agencies in making informed decisions about possible providers and will inform USSM and OMB where supply may not be adequate.

### **Lessons Learned**

Attempts to increase government-wide adoption of shared services and measuring their impact has changed over time from a top-down mandate requiring the use of certain shared services (as used in the E-Government Initiatives and, to some degree, the FM LoB) to more of a marketplace approach. Previous efforts have led to the establishment of USSM as a centralized entity focused on the management of these services to facilitate the goal of increased adoption.

Currently, USSM is focused on establishing a performance framework for evaluating and promoting shared services. One goal of USSM's performance framework is to establish objective data and information so an agency can evaluate the suitability of a shared service provider. This requires making reliable, understandable, and accurate satisfaction and service quality measures available for each service. This marketplace model allows the existing decision-making of a potential customer agency to validate the cost savings or other business case for shared services, but may lead to less overall adoption than the mandatory model. However, this approach could also lead to more substantive adoption of valuable services.

# Agency Observations and Findings

The opportunities and benefits of shared services within agencies and more broadly across the Federal government are clear. The increased use of shared services can save money and improve service delivery with the added benefit of replacing or retiring outdated infrastructure and legacy systems.<sup>33</sup> However, this will require the full attention of senior management as well as sustained engagement with key stakeholders outside of the executive branch – in particular, the legislative branch and the vendor community.

## FINDING #1

### Providing Shared Services Increases Agency Risk and Burden and Can Lead to Lower Quality of Service.

Agencies who offer shared services face challenges scaling to meet the needs of a growing customer base and to remain competitive versus other providers, especially those from the private sector. Becoming a provider entails additional costs and risks, and agencies must carefully evaluate the business case before agreeing to become a provider. In some instances,

becoming a provider may not align explicitly with the agency's own mission, further

*Providing a shared service can be a potential liability... It becomes your fault if something goes wrong. There's lots of responsibility that goes beyond your agency's mission if you are a shared services provider.*

— Agency CIO

increasing these costs and risks. In addition, the range of costs and risks in providing a shared service depends in part on the variety of mission objectives of customer agencies. Differences in those agencies' missions can affect requirements (e.g., the level of security and privacy controls required for data storage), not to mention that shared service providers may receive conflicting direction from home agencies and USSM's Shared Services Governance Board.

In addition, Federal shared service providers face different constraints relative to those in the private sector around basic operational considerations. For example, Inter-Agency Agreements (IAAs) such as Service Level Agreements (SLAs) are not as easily enforceable as business to business contracts. This is in part due to the fact that government agencies do not

have access to the same legal recourse for addressing breaches of interagency agreements as private sector organizations do for contracts.

*There's no accountability (via SLAs) for providing cost-effective and reliable services.*

– Agency CIO

Additionally, government agencies must comply with a number of hiring and retention laws and policies that are not found in the private sector. Federal agencies also typically face highly constrained annual budgets, reducing their ability to make long-term investments in service improvements. As such, mandating shared service usage across government can actually lead to lower levels of customer satisfaction. For example, as reported in Federal Shared Services CAP Goal KPIs, customer satisfaction with value of services (for the HR LoB) was relatively low.<sup>34</sup> Fixing these constraints should be part of the conversation around positive changes in government operations, which could increase shared service adoption as well as facilitate other improvements.

## FINDING #2

**Intra-agency shared service offerings may not effectively scale to other agencies.**

Strong agency performance in providing a specific service to its own bureaus does not automatically make that agency a good candidate to provide that service across government. In some cases, small agencies may have difficulty scaling up services to larger Federal agencies, and agencies with a low cybersecurity risk may find it hard to provide certain services to agencies which are more likely to be the target of a major cyber attack. In order to drive better performance in Federal shared services, agencies must carefully evaluate all of the risks and benefits when deciding whether to become a service provider.

**FINDING #3****Transfer of Funds Between Agencies Present Challenges.**

Interagency financial agreements can be challenging due to a variety of policies and laws governing how Federal appropriations can be spent and for what purposes. For example, shared service providers and customers typically rely on IAAs to transfer funds.<sup>35</sup>

*Most department CIOs will tell you it takes about a year to move money between departments. The typical vehicle is the Economy Act, but it's not efficient for the task – the justification process is too long. Maybe we need a Shared Services Act to facilitate that process.*

– Agency CIO

However, the laws that underpin these IAAs, such as the Economy Act of 1932,<sup>36</sup> have strict requirements as to what constitutes an allowable transfer.

The barriers are even higher when moving funds across agencies.<sup>37</sup> Agencies may be required to submit reprogramming requests or otherwise notify Congress. In some cases, different funding rules apply within the same agency, requiring provider agencies to enter into multiple IAAs with a single customer agency to support some or all of that agency's bureaus. This may be further complicated by varying requirements for basic needs like service uptime and security across bureaus. Collectively, these issues both complicate and delay funding. As many CIOs reported, these legal, institutional, and cultural barriers can cause year-long delays for funding transfers, significantly curtailing the adoption of shared services.

**FINDING #4****Increasing accountability could increase adoption.**

Moving forward, many agency CIOs noted that standard accountability measures for shared service providers could improve customer confidence and increase Federal shared service adoption. They stated that providing information, flexibility, and choice for shared service customers improves the competitiveness and quality of Federal shared service offerings.

USSM is also setting up new ProviderStat accountability sessions, designed to foster transparency in the shared service marketplace and to provide a performance review process for Federal shared services.<sup>38</sup> USSM, working with shared service providers, customers, and OMB, seeks to utilize ProviderStat to identify shared challenges, establish common metrics, develop reporting mechanisms, and measure customer satisfaction.<sup>39</sup>

# Notes

1. Available at <https://ourpublicservice.org/publications/download.php?id=758>
2. Federal Information Technology Shared Services Strategy. 5/2/2012. pp 3-4. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/shared\\_services\\_strategy.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf)
3. Tony Scott: "Cyber means sharing more than just info" 11/17/2015. <http://fedscoop.com/tony-scott-wants-to-see-more-sharing-among-agencies>
4. Partnership for Public Service. "Building a Shared Services Marketplace: Recommendations from the Shared Services Roundtable." 05/2015. pp 24. <https://ourpublicservice.org/publications/viewcontentdetails.php?id=470>
5. For further information on cybersecurity shared services and programs, such as the EINSTEIN program, see Policy Chapter E: Cybersecurity
6. Partnership for Public Service. "Building a Shared Services Marketplace: Recommendations from the Shared Services Roundtable." 05/2015. pp 22-24. <https://ourpublicservice.org/publications/viewcontentdetails.php?id=470>
7. Graphic provided by Unified Shared Services Management
8. For a complete listing of Lines of Business, see page 48 of the FY 2018 IT Budget – Capital Planning Guidance. 6/30/2016. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/fy18\\_it\\_budget\\_guidance.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy18_it_budget_guidance.pdf)
9. Unified Shared Services Management. "About Unified Shared Services Management". <https://www.ussm.gov/why/about-ussm/#.V9BqnCgrKM8>
10. M-16-11. Improving Administrative Functions Through Shared Services. 5/4/2016. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-11.pdf>
11. M-01-28. Citizen-Centered E-Government: Developing the Action Plan. 7/18/2001. [https://www.whitehouse.gov/omb/memoranda\\_m01-28](https://www.whitehouse.gov/omb/memoranda_m01-28); and E-Government Strategy: Simplified Delivery of Services to Citizens. 2/27/2002. <https://www.whitehouse.gov/sites/default/files/omb/inforeg/egovstrategy.pdf>
12. George W. Bush Presidential Archives. "Lines of Business". <https://georgewbush-whitehouse.archives.gov/omb/egov/c-6-lob.html>
13. Performance.gov. "Cross-Agency Priority Goal: Shared Services". FY 2016 Q3 Update. <https://www.performance.gov/node/3398/view?view=public#progress-update>
14. 25-Point Implementation Plan to Reform Federal IT Management. Point A.6: "Develop a strategy for shared services". 12/9/2010. <https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>
15. The initial focus on commodity IT (i.e., desktop, mobile devices) was due to the relatively low complexity of such items when compared to business support services (e.g., human resources) and mission support services (e.g., geospatial). Nonetheless, agencies and OMB faced challenges in determining common definitions of commodity IT. A subsequent OMB memo provided examples of Commodity IT, but did not provide a specific definition of the term. M-11-29. Chief Information Officer Authorities. 8/8/2011. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf>
16. The "Shared-First" concept was first articulated in the 25-Point Implementation Plan to Reform Federal IT Management (<https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>) in action item #6
17. Federal Information Technology Shared Services Strategy. 5/2/2012. [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/shared\\_services\\_strategy.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf)
18. Ibid
19. Ibid
20. For more information about IT infrastructure and its underlying role in many other IT policy areas, see Policy Chapter B: IT Infrastructure Modernization
21. CIO Council. Federal Shared Services Implementation Guide. 4/16/2013. <https://cio.gov/wp-content/uploads/downloads/2013/04/CIOC-Federal-Shared-Services-Implementation-Guide.pdf>
22. The previous mandate to apply a shared service solution in financial management systems modernization held over from the Financial Management Line of Business (FMLoB) was removed. M-13-08. Improving Financial Systems Through Shared Services. 3/25/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-08.pdf>
23. David Mader and Denise Turner Roth. The White House Blog. "Scaling Implementation of Shared Services". 10/22/2015. <https://www.whitehouse.gov/blog/2015/10/22/scaling-implementation-shared-services>
24. M-16-11. Improving Administrative Functions Through Shared Services. 5/4/2016. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-11.pdf>
25. Graphic provided by Unified Shared Services Management
26. Elizabeth Angerman, comments to author, December 2016
27. For more detailed information about PortfolioStat, see Policy Chapter A: Management and Oversight of IT
28. GAO-13-796T. Information Technology: OMB and Agencies Need to More Effectively Implement Major Initiatives to Save Billions of Dollars. 7/25/2013. <http://www.gao.gov/assets/660/656191.pdf>
29. Office of Personnel Management. Human Resources Line of Business Strategic Framework. 4/14/2015. <https://www.opm.gov/services-for-agencies/hr-line-of-business/strategic-framework/hr-lob-strategic-framework.pdf>







30. M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. 3/27/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>
31. Performance.gov. "Cross-Agency Priority Goal: Shared Services". Quarterly Progress Update. <https://www.performance.gov/content/shared-services#overview> and Performance.gov. "Cross-Agency Priority Goal: Benchmark and Improve Mission-Support Operations". Quarterly Progress Update. <https://www.performance.gov/node/3397/view?view=public#overview>
32. General Services Administration. "Introduction to Modernization and Migration Management (M3)". <https://www.usssm.gov/m3/#.WByCOuErKVu>
33. In 2014, the Department of the Interior's Interior Business Center negotiated 1,202 agreements with a mix of non-profit organizations as well as Indian tribal, state, and local governments. These efforts resulted in \$24 million in potential government-wide savings. Source: <https://www.doi.gov/ibc/about-us/success-stories>
34. While overall customer satisfaction with providers in the HR LoB was close to the target (73% versus a target of 80%), customer satisfaction with value of services was well below the target (52% actual versus a target of 80%). Performance.gov. "Cross-Agency Priority Goal: Shared Services". FY 2016 Q2 Update. <https://www.performance.gov/node/3398/view?view=public#progress-update>
35. OFPP Memorandum. Improving the Management and Use of Interagency Acquisitions. 6/6/2008. [https://www.whitehouse.gov/sites/default/files/omb/assets/procurement/iac\\_revised.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/procurement/iac_revised.pdf)
36. 31 U.S.C. § 1535. The Economy Act (and amendments). <https://www.gpo.gov/fdsys/pkg/USCODE-2009-title31/html/USCODE-2009-title31-subtitle11-chap15-subchapIII-sec1535.htm>
37. Agencies cannot transfer funds between appropriations accounts unless expressly permitted in law or with approval of the House and Senate appropriations committees
38. Unified Shared Services Management. "Improving Mission Support through ProviderStat". <https://www.usssm.gov/providerstat/#.V9b305MrIUE>
39. Performance.gov. "Cross-Agency Priority Goal: Shared Services". Quarterly Progress Update. <https://www.performance.gov/content/shared-services#progress-update>

# Cybersecurity

Our cybersecurity goal is simple: To support an Open and Transparent Government where the People’s Information is protected and Privacy, Civil Rights, and Civil Liberties are preserved.

– Gen. Gregory Touhill, U.S. Chief Information Security Officer, Office of Management and Budget, in a November 2016 CIO.gov blog post

## Summary

 Cost	The proposed FY 2017 President’s Budget requests \$19 billion for cybersecurity, a 35 percent increase over FY 2016 funding levels. Sustained public attention and funding is needed to make progress in this key policy area.
 Accountability	A number of Chief Information Officers (CIOs) said they often do not have the flexibility to quickly incorporate safeguards to address newly-discovered vulnerabilities due to lengthy and complex Federal procurement and hiring processes and competing priorities.
 Risk	High-profile incidents such as the Office of Personnel Management (OPM) data breaches highlighted the vulnerability of the government’s IT systems and prompted greater attention on Federal cybersecurity initiatives and progress.
 Policy	Recently, Federal cybersecurity efforts have shifted from compliance-oriented, documentation-driven processes to continuous, automated tools and processes. Federal cybersecurity efforts span six key areas: managing cybersecurity throughout the enterprise; understanding data assets and threats, building the Federal cyber workforce and budget processes; promoting the use of standardized, centralized IT; securing the network; and securing authentication and authorization.

# Cybersecurity

## Overview

### What is Cybersecurity?

Cybersecurity is often used interchangeably with the term “information security” and is defined by the Office of Management and Budget (OMB) as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and
- Availability, which means ensuring timely and reliable access to and use of information.<sup>1</sup>

Federal initiatives and performance metrics related to cybersecurity have evolved over time to focus on six key areas:

1. *Managing Cybersecurity Throughout the Enterprise*: Efforts to improve how agencies budget for, plan for, and implement and oversee cybersecurity related activities throughout the agency enterprise. This includes government-wide reporting and oversight initiatives such as agency reporting on Federal Information Security Modernization Act (FISMA) implementation, CyberStat Reviews, and the President’s Management Council (PMC) Cybersecurity Assessment.

### Transition to IPv6

The transition from IPv4 to a more modern IPv6 does more than just enable an expansion of internet devices due to the exhaustion of IPv4 addresses, it can enable agencies to improve their cybersecurity posture. Specifically, native, end-to-end IPv6 environments enable cybersecurity staff to have an unobstructed view of network infrastructure directly supporting both the Cybersecurity National Action Plan “Secure by Design” approach and the DHS Continuous Diagnostic Mitigation (CDM) initiative. The Federal CIO and CISO should continue emphasizing agencies implement IPv6 to ensure business continuity, strategically decommission the legacy IPv4 protocol to remove this attack vector from their infrastructure, and enable secure innovations such as the Internet of Things.

2. ***Understanding Data Assets and Threats:*** The prioritized identification and protection of high value information and systems. High Value Assets (HVAs) are government systems, facilities, data, and aggregate datasets that may be of particular interest to potential adversaries. These assets may contain sensitive controls, instructions, or other information that is critical to national security or operational functionality.<sup>2</sup>
3. ***Building Federal Access to Cybersecurity Talent:*** A series of actions to identify, recruit, develop, retain, and expand the cybersecurity skill set of the Federal workforce, while recognizing that contractors also play vital roles in Federal cybersecurity.
4. ***Promoting the Use of Standardized, Centralized IT:*** The federated IT management approach that is prevalent across the Federal government today presents challenges to improving cybersecurity and delivering IT capabilities in an efficient, cost effective manner. Under this model, all agencies, regardless of size or mission, are responsible for maintaining their IT and information security resources, and many organizations struggle to maintain adequate capabilities. This problem necessitates both a further consolidation of the Federal government IT footprint and an expansion of shared, centralized services to better leverage Federal buying power, standardize IT capabilities, and realize economies of scale from aggregating data.

Government-wide shared services can augment or supplement existing agency services, while providing new services for agencies without existing capabilities. For example, both the Continuous Diagnostics and Mitigation (CDM) Program Tools and the Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreement (BPA) provide a consistent set of government-wide asset, identity, and event management tools that can provide capabilities and data needed to strengthen the security posture of agency networks.<sup>3</sup>

## Key Stakeholders

- White House Cybersecurity Coordinator
- Office of the Federal Chief Information Officer (OFCIO)
- Federal Chief Information Security Officer (FCISO)
- Office of Management and Budget, Cyber and National Security Unit (OMB Cyber)
- The President's Management Council (PMC)
- Federal CIO Council
- Federal Chief Information Security Officer Council
- National Security Council (NSC)
- Office of the Director of National Intelligence (ODNI)
- Department of Commerce, National Institute of Standards and Technology (NIST)
- Department of Homeland Security (DHS)
- General Services Administration

5. *Securing the Network*: Modernization of the Federal government's IT infrastructure through upgrades to insecure and inefficient systems, data center consolidation, and transition to cloud services, offers a path to a more efficient and secure IT portfolio. Cloud-based solutions, for instance, offer convenient, on-demand network access to a shared pool of IT resources that can be rapidly provisioned. However, while cloud-based services offer many benefits for Federal computing, they have also raised important questions about the protection of data in this new environment. Efforts like the Federal Risk and Authorization Management Program (FedRAMP), can help agencies leverage the promise of cloud by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. FedRAMP and other government-wide efforts to provide common capabilities to secure Federal networks, such as CDM and EINSTEIN, allow CIOs to focus on building new applications and services with the confidence that the network and infrastructure are appropriately secure.
6. *Securing Authentication and Authorization – Identity, Credential, and Access Management (ICAM)*: Securing information systems and networks by better understanding and controlling which users access which resources and the rights of those users. This includes efforts to strengthen identity, credential, and access management, secure mobile devices and remote access, address insider threats, prevent data loss, and manage user permissions.

## Background

Cybersecurity has taken on greater importance in recent years, driven by the continuing efforts to replace legacy government services with electronic and digital services and the rapid growth in the sensitivity, size, and variety of information held in the government's databases that support those services. Several high-profile incidents have highlighted the need to address longstanding vulnerabilities in Federal IT systems. Most notably, the 2015 breach at the Office of Personnel Management (OPM) involving the compromise of personally identifiable information (PII) and security clearance background details put approximately 21.5 million Federal employees at risk of identity theft.<sup>4</sup>

The early cornerstone of today's Federal cybersecurity efforts is the *Federal Information Security Management Act (FISMA) of 2002*. Congress enacted this law to improve the effectiveness of security controls for Federal information systems and to ensure adequate oversight of such activities. FISMA identified the role agencies, OMB, DHS, and the National Institute of Standards and Technology (NIST) play in government-wide efforts.<sup>5</sup> In 2014, Congress updated this law in the *Federal Information Security Modernization Act of 2014*.

Since 2009, a number of policy initiatives were undertaken to improve the government's cybersecurity posture. The most notable of these are the:

- 2009 Cyberspace Policy Review (60-day Review),
- 2015 Cybersecurity Sprint (Cyber Sprint),
- 2015 Cybersecurity Strategy and Implementation Plan (CSIP), and
- 2016 Cybersecurity National Action Plan (CNAP).

*Cybersecurity is much more than just a technology fix—rather it is a risk management issue. When we focus exclusively on the technology we sometimes miss the real goal, which is managing the risk to the confidentiality, integrity and availability of the information the technology supports.*

- Gen. Gregory Touhill,  
U.S. Chief Information Security Officer,  
Office of Management and Budget,  
in a November 2016 CIO.gov blog post

*Cyberspace Policy Review (60-day Review) and Resulting Actions.* In 2009, the new Administration conducted a 60-day Review of cybersecurity policies and structures inside and outside of the Federal government. The Review's findings were published in a May 2009 report to the President,<sup>6</sup> and include a number of recommendations which the White House implemented:<sup>7</sup> appointing a White House Cybersecurity Coordinator in the National Security Council, establishing a Cybersecurity Cross-Agency Priority (CAP) Goal<sup>8</sup> as a part of the President's Management Agenda, defining performance metrics for cybersecurity, establishing a mechanism for holding agencies accountable for their performance through OMB's CyberStat Review process,<sup>9</sup> and announcing other related national cybersecurity documents, strategies, and plans.<sup>10</sup>

### *30-day Cybersecurity Sprint and CSIP.*

While strengthening the cybersecurity of Federal networks, systems, and data continued to be an important challenge post-2009, agencies often struggled to ensure cybersecurity was resourced and prioritized on par with program delivery. The OPM cybersecurity breach in 2015 sharply refocused the attention of agency heads on the criticality of supporting CIO and Chief Information Security Officer (CISO) function within their agencies.

Capitalizing on this spotlight, OMB initiated a Cybersecurity Sprint. This effort identified a set of critical actions for Federal agencies to take within 30 days<sup>11</sup> and established a Sprint Team to lead an intensive review of the Federal government's cybersecurity policies, procedures, and practices.<sup>12</sup> The recommendations resulting from the Sprint Team's review led to an October 2015 OMB memorandum titled "Cybersecurity Strategy and Implementation Plan" (CSIP).<sup>13</sup> This plan:

- Reiterates agencies' responsibilities for a number of ongoing cybersecurity initiatives;
- Assigns new actions, such as agencies must identify their high value assets (HVAs) and critical system architecture, and designate a "security operations center" at each agency;
- Requires new plans and documents, such as an OMB cybersecurity shared services plan, an Improving the Security of Consumer Financial Transactions Implementation Plan, and new NIST guidance on how to recover from incidents;
- Extends actions emphasized during the Cybersecurity Sprint, such as tightening privileged user policies, practices, and procedures and addressing critical vulnerabilities identified through scanning within 30 days; and
- Designates the PMC to oversee the implementation of the CSIP, in an effort to ensure agency leadership stayed engaged in supporting CIO and CISO functions within their organizations.

*CNAP and FY 2017 President's Budget.* Building on the CSIP, in 2016, the White House published a fact sheet announcing a set of near-term actions to improve cybersecurity, and pave the way for a longer-term strategy to enhance cybersecurity awareness and protections. The Cybersecurity National Action Plan (CNAP):<sup>14</sup>

- Establishes the Commission on Enhancing National Cybersecurity;
- Creates the Federal Chief Information Security Officer (FCISO);
- Proposes the Information Technology Modernization Fund (ITMF);
- Commits to work with industry to encourage multi-factor authentication throughout public-facing Internet services and to release a new action plan for government use of multi-factor authentication;
- Highlights a number of new initiatives with expanded funding in the FY 2017 President's Budget, including a focus on expanding the cybersecurity workforce by enhancing student loan forgiveness programs for cybersecurity experts joining the Federal workforce and catalyzing investment in cybersecurity education as part of a robust computer science curriculum through the President's Computer Science for All Initiative;<sup>15</sup>
- Highlights new and continued privacy and security initiatives, such as the 2014 BuySecure Initiative and the re-launch of IdentityTheft.gov, together designed to protect Americans from credit card fraud and identity theft; and
- Highlights new and continued initiatives to "enhance critical infrastructure security and resilience," such as establishing a National Center for Cybersecurity Resilience, developing the Cybersecurity Assurance Program to improve the security of "internet of things" devices, and doubling the number of Department of Homeland Security (DHS) cybersecurity advisors available to assist private sector organizations involved in critical infrastructure.

The FY 2017 Budget proposes more than \$19 billion for Federal cybersecurity efforts.<sup>16</sup> A 35 percent increase over the funding level of 2016, these resources are intended to help agencies improve their cybersecurity posture, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents. Many of the initiatives described in the CNAP would use this expanded funding.

The CNAP also established a new cybersecurity leadership position, Federal Chief Information Security Officer (FCISO). This position drives government-wide cybersecurity policy, planning, and implementation across the Federal government. In addition, the CNAP directed implementation of the first-ever Federal Cybersecurity Workforce Strategy<sup>17</sup> to identify, recruit, develop, and retain talent for Federal service, and proposed an IT Modernization Fund (ITMF) to provide \$3.1 billion in dedicated funding to encourage agencies to replace or otherwise modernize critical systems and equipment.

Initiatives spearheaded by the Federal CIO under the direction of the White House and the PMC, such as the Cyber Sprint, have yielded positive results. A sustained focus from the highest-ranking officials in government can serve to drive the cyber risk management process, leading to better-protected Federal data and information systems. Additionally, revisiting the role and relationship of agency CISOs to program leaders and other senior management leaders such as CFOs could help ensure that agencies are setup to integrate information security concepts, practices, and initiatives throughout agency decisions at a senior level.



# Current State of Key Initiatives

## Managing Cybersecurity Throughout the Enterprise

Guides how agencies budget for, plan for, and oversee cybersecurity. Includes, for example, CyberStat Reviews, FISMA reporting, Cybersecurity CAP Goal Performance Updates, and PMC reporting and oversight.

## Understanding Data Assets and Threats

Requires agencies to identify and protect high value information and systems that may be of particular interest to potential adversaries.

## Building the Federal Cyber Workforce

Directs a series of actions to identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service.

## Promoting the Use of Standardized, Centralized IT

Provides common services available to all agencies to consistently and cost-effectively implement aspects of cybersecurity initiatives, such as CDM, the CMaaS BPA, and EINSTEIN.

## Securing the Network

Improves the security of external and internal infrastructure and network options for agencies. Includes initiatives to secure both external providers' networks, such as FedRAMP, and internal Federal networks, such as TIC.

## Securing Authentication and Authorization – Identity, Credential, and Access Mgmt.

Provides a variety of initiatives to improve logical and physical security across agencies, including but not limited to the issuance and use of Personal Identity Verification (PIV) cards.

*The themes consist of numerous efforts and actions which took place over a broad period of years, and many are ongoing today. As such, specific years are not included.*

## Managing Cybersecurity Throughout the Enterprise

Overall government-wide reporting and oversight initiatives help ensure a common management approach to implementing cybersecurity capabilities across the Federal government. In early 2016, the White House created a new cybersecurity leadership position, the FCISO. Established in the CNAP, this position is responsible for driving government-wide cybersecurity policy, planning, and implementation across the Federal government. The initiatives listed below are all led by the Federal CISO:

- **Annual FISMA Reporting.** Common processes that originated in FISMA and are defined by NIST<sup>18</sup> publications include regular reporting on a standard set of cybersecurity capabilities by Federal agencies, an annual FISMA report from OMB to Congress summarizing performance metrics from all the agencies, the categorization of systems by risk level (these guidelines are typically referred to as “FISMA High,” “FISMA Moderate,” and “FISMA Low”)<sup>19</sup> and the procedures by which an agency authorizes the operation of a system in its environment.<sup>20</sup>

After twelve years, an amendment to FISMA was signed into law – the Federal Information Security Modernization Act of 2014. This update provides several modifications, such as clarifying OMB’s government-wide cybersecurity oversight role and DHS’s responsibility to administer the implementation of cybersecurity policies and practices by Federal agencies (the original FISMA had been passed before DHS was established). FISMA 2014 also led to OMB issuing the first revision of Circular A-130 “Management of Information as a Strategic Resource” since 2000.<sup>21</sup>

- **CyberStat Reviews.** CyberStat Reviews are deep-dive, evidence-based, face-to-face engagements with Federal CIOs and CISOs, built around comprehensive reviews of agency-specific cybersecurity postures and select government-wide cybersecurity programs. Through these targeted, high-level engagements, OMB and agency leaders are able to frankly discuss persistent cybersecurity concerns and collaborate to make sure challenges are adequately addressed and resourced. The number conducted per year increased from eight in FY 2014 to 24 in FY 2016. Reviews in FY 2016 focused on information security governance, strong authentication, and agency protections of HVAs. In general, OMB leverages the CyberStat process to uncover best practices and common challenges across the Federal enterprise in areas such as CDM implementation, rationalization of the TIC and cloud policies, and common needs for cybersecurity workforce and training. OMB's CyberStat Review process was established in January 2011<sup>22</sup> and updated in 2015.<sup>23</sup>
- **PMC Cybersecurity Assessment.** Since 2015, OMB has conducted quarterly engagements with agencies regarding their progress implementing Federal policies and priorities. The executive visibility gained by using the PMC to connect the Federal CIO with Deputy Secretaries is a critical factor in improving the state of Government-wide cybersecurity. PMC members discuss the status of their cybersecurity efforts and recommendations for improving performance using a maturity model based on the five function areas of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. These updates can factor into OMB's cybersecurity budgeting process, where agency performance in specific function areas can be matched to both previous and projected spending to identify opportunities for investments to support critical capabilities.

## Understanding Data Assets and Threats

Agencies' efforts to identify, prioritize, and protect their most sensitive assets and data are a major component of government-wide cybersecurity. These assets may contain sensitive controls, instructions, or other information that is critical to national security or operational functionality.

- **High Value Assets.** In 2015, OMB published the Federal Information Security and Privacy Management Requirements to identify and assess security risk around HVAs and to align current processes with the NIST Cybersecurity Framework.<sup>24</sup> However, agencies struggled to settle on a common definition for HVAs. OMB brought agency CIOs together to agree upon a common understanding of policies to identify, manage, and protect HVAs. OMB was then able to apply these policies in subsequent guidance, such as the CSIP,<sup>25</sup> and further codify them in the CNAP. OMB plans to take further steps to formalize these approaches through additional memoranda in FY 2017.

## Building the Federal Cyber Workforce

The Federal Cybersecurity Workforce Strategy, released in 2016, focuses on improving how agencies identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service.<sup>26</sup> It identifies actions for OPM, the National Initiative for Cybersecurity Education (NICE), and other Federal agencies to improve cybersecurity workforce planning.

The Strategy establishes four key initiatives:

- **Identify Cybersecurity Workforce Needs.** Seeks to improve the government-wide understanding of cybersecurity workforce needs by identifying key capability and capacity gaps in order to enhance workforce planning;
- **Expand the Cybersecurity Workforce through Education and Training.** Entails working with educational institutions, professional organizations, training organizations, and other experts on cybersecurity program guidance from P-12 through university-level education to significantly expand the pipeline of skilled cybersecurity talent;
- **Recruit and Hire Highly Skilled Talent.** Establishes government-wide and agency-specific efforts to expand the cybersecurity workforce through recruitment of highly skilled talent. Streamlines the hiring and security clearance process while still meeting applicable law and standards; and
- **Retain and Develop Highly Skilled Talent.** Promotes an enterprise-wide approach to retention and development to support the continued enhancement of the Federal cybersecurity workforce.

## Promoting the Use of Standardized, Centralized IT

The federated nature of agencies' IT management – distributing responsibilities across many agencies, bureaus, and programs – can be a significant impediment to improving cybersecurity. Under this model, all agencies, regardless of size or mission, are responsible for maintaining their own IT, and many organizations struggle to maintain adequate security capabilities.

One approach to addressing this disparity is to develop common, centrally-managed services to better leverage Federal buying power, cybersecurity skillsets, and standardize security capabilities. These efforts help agencies better secure their own networks and accelerate their access to secure external solutions. For example, both the CDM Program Tools and the CMaaS BPA provide government-wide capabilities that enable Federal agencies to strengthen agency networks.<sup>27</sup> The goal of the CDM program is to bring consistency to the security capabilities used by agencies for basic cyber hygiene functions, while also procuring these tools in a cost effective manner. Similarly, DHS's EINSTEIN program was designed to protect agencies' unclassified networks through shared situational awareness across the government, as threats detected at one agency are shared with all others.

Other efforts to ensure agencies have access to modern systems and services include taking steps to centralize IT for small agencies, using a Small Agency Network as a proof of concept. Other potential areas for greater centralization and standardization include: mobile security services, network segmentation services, identity, authentication, and authorization services, digital rights management, and encryption services.

- ***Continuous Diagnostics and Mitigation (CDM) program.*** CDM enhances the government's ability to collect and act on automated information regarding Federal IT assets. The first phase of CDM, currently being deployed, allows agencies to identify assets on a continuous basis. CDM also allows for information to be fed to a Federal-level dashboard, which provides government-wide visibility into the current state of Federal assets. Phases 2 and 3 will extend the visibility of these tools into additional aspects of Federal assets, users, devices, and intrusions.<sup>28</sup> Agencies are in the process of deploying to their own dashboards but have not yet connected to the Federal dashboard.
- ***EINSTEIN.*** The DHS National Cybersecurity Protection System, commonly known as EINSTEIN, offers a consistent suite of tools for network boundary protection to agencies. All major Federal agencies have adopted the intrusion detection services of EINSTEIN. The next phase of services offers a capability to disable attempted intrusions before harm is done, which would address approximately 85% of the cybersecurity threats affecting Federal civilian networks. As a shared service, EINSTEIN has encountered some resistance from agencies seeking to retain greater control over their tools, delaying full deployment.

## Securing the Network

Modernization of the Federal government's IT infrastructure, such as through upgrades to insecure and inefficient systems, data center consolidation, and transition to cloud services, offers a path to a more efficient and secure IT portfolio. Greater agency interest in cloud-based solutions has raised important questions about the protection of data in this new environment. Several key initiatives are currently underway to transition Federal agencies to more secure and efficient platforms which would allow CIOs to focus on building new applications and services with the confidence that the network and infrastructure are appropriately secure.

- *IT Modernization Fund.* Of the \$82 billion in Federal IT spending planned for 2017, approximately 78 percent (\$63 billion) is dedicated to maintaining legacy IT investments. These systems may pose security risks, such as the inability to utilize current security best practices, including data encryption and multi-factor authentication, as well as operational risks, such as rising costs and inability to meet mission requirements.

To help address these challenges, the President proposed the creation of a \$3.1 billion Information Technology Modernization Fund (ITMF) as part of the FY 2017 President's Budget and the Cybersecurity National Action Plan (CNAP). Federal agencies would use this revolving fund at GSA "to retire, replace or upgrade hard-to-secure legacy IT systems and transition to new, more secure, efficient, modern IT systems, while also establishing long-term mechanisms for Federal agencies to regularly refresh their networks and systems based on up-to-date technologies and best practices."<sup>29</sup> Envisioned as a revolving fund which agencies would reimburse based on the cost savings they achieve by replacing legacy IT systems with more efficient alternatives, the ITMF is intended to enable not only improvements to agencies' cybersecurity posture, but also to lead agencies to a modernized IT infrastructure which supports modern digital services.

- **Secure Cloud Adoption.** Cloud-based solutions offer convenient, on-demand network access to a shared pool of IT resources that can be rapidly provisioned. This allows agencies to get out of the business of managing the full stack of IT services themselves and to avoid overhead costs by paying only for those resources they use.

To help realize the benefits of cloud computing, OMB issued the Federal Cloud Computing Strategy in 2011. The strategy encouraged agencies to use cloud-based services in order to improve resource utilization, increase service responsiveness, and accrue meaningful benefits in efficiency, agility, and innovation. While cloud-based services offer many benefits for Federal computing, they have also raised important questions about the protection of data in this new environment. For this reason, in 2011, OMB established the Federal Risk and Authorization Management Program (FedRAMP).<sup>30</sup> The program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services in order to allow cloud service providers to achieve a single authorization for a given service that may then be used by other agencies to establish their own authorizations, providing efficiencies, cost savings, and a common security baseline. FedRAMP includes a Joint Authorization Board (JAB) composed of the CIOs of the Department of Homeland Security (DHS), Department of Defense (DOD), and the General Services Administration (GSA), and is operated by a GSA-based Program Management Office (PMO).

As agencies adopt cloud services, they have begun to experience difficulties complying with the Trusted Internet Connection (TIC) initiative, which lays out an architecture for consolidating and protecting agency connections to the public internet in order to ensure these connections are secure. Since its initiation in 2008, the government has reduced the number of Federal connections to the Internet from several thousand to 65 in 2015, and has helped provide a secure internal network infrastructure for CIOs to access. However, because TIC relies on a centralized access point (while cloud is based on a decentralized model), complying with both policies has created problems for agencies and industry alike. Given the growing importance of protecting Federal data whether hosted in a cloud, a data center, or traversing the internet, OMB has launched an effort to align existing policies related to TIC and cloud service adoption.

- **Continuous Diagnostics and Mitigation (CDM).** A key component of this effort is CDM, which continues to be a Federal priority in making real-time data on an agency's risk posture available to decision makers.<sup>31</sup> CDM assists agencies in maintaining continuous awareness of prioritized risks and security vulnerabilities at an enterprise level. While this program is a part of the effort to establish standardized, centralized IT for CIOs to build off of, it is also a basic component of identifying gaps in securing the network. By improving agency awareness of what is running on their networks, CDM makes it easier to target patch updates and address software vulnerabilities that may be weakening the resilience of the network.

## Securing Authentication and Authorization – Identity Credential and Access Management

A number of efforts focus on better understanding and controlling which users access which resources. These include efforts in Federal Public Key Infrastructure (PKI), Federal Identity, Credential, and Access Management (FICAM), securing mobile devices, improving citizen authentication to government and private sector services, as well as broader strategies to narrowly define privileged user permissions. An overall summary of the FICAM topic area can be found at [IDManagement.gov](http://IDManagement.gov).

- PIV Cards and HSPD-12.* One of the recommendations from the 9/11 Commission Report from 2004 was to ensure that only appropriate people are accessing Federal facilities (“physical access”) and IT systems (“logical access”).<sup>32</sup> Many cybersecurity threats gain unauthorized access to a system and its data by falsely claiming to be a user who has those privileges or access. Ensuring that someone is who they say they are and that only authorized people have access to the appropriate Federal facilities and systems became a major initiative in Federal cybersecurity efforts, beginning with the release of “Policies for a Common Identification Standard for Federal Employees and Contractors,” more commonly known as “HSPD-12.”<sup>33</sup> This set in motion a series of actions to develop a PIV card and to work with all agencies to issue the PIV card to employees, contractors, and others who require its use for physical and logical access, and to increase interoperability between agencies.
- National Strategy for Trusted Identities in Cyberspace (NSTIC) and other efforts.* Recognizing that Federal leadership could also play a role in strengthening identity verification and transactions outside of government, Commerce published the NSTIC in April 2011. This established the NSTIC program at Commerce to coordinate the Federal government and private sector to “increase adoption of trusted digital identity solutions” inside and outside of government.<sup>34</sup> Relatedly, the MyUSA and Connect.gov initiatives were also launched to expand government online citizen-facing services’ ability to accept credentials issued from other providers, such as Google accounts or State drivers’ licenses. In 2016, GSA consolidated these efforts into a new initiative led by 18F with similar goals called Login.gov.<sup>35</sup>

# Metrics and Oversight

## Primary Objective Emphasized in Metrics and Oversight

Government-wide reporting for cybersecurity focuses on agency progress implementing key government-wide initiatives to address critical vulnerabilities, identify emerging threats and vulnerabilities, and evaluate agency responses to incidents.

## Examples

The primary data collection for cybersecurity is that collected under FISMA each year (largely submitted through the DHS Cyberscope data collection tool). The data collected under FISMA each year can be varied and extensive, with one agency describing the requirement as “120 metrics quarterly.” OMB has made efforts to pare down the reporting over time, but the requirements are still significant. OMB strives to use the concept of “report once, use many times,” leveraging the FISMA data to inform PortfolioStats, CyberStat Reviews, the PMC Cybersecurity Assessment, and Cybersecurity CAP goal reporting. Additionally, OMB analyzes agencies’ HVA submissions, data collected by DHS under its “binding operational directive” activities, US-CERT incident reporting data, and data provided by the FedRAMP Program Management Office.

While cybersecurity-related KPIs have been included in PortfolioStat for every year of its operation, cybersecurity oversight is conducted in greater depth through the PMC Cybersecurity Assessments, and CyberStat Reviews. Additionally, the Cybersecurity CAP Goal reports progress on implementing priority cybersecurity capabilities publicly. The PMC Cybersecurity Assessments are quarterly and include Deputy Secretaries of major Federal agencies and the Federal CIO. The CyberStat Reviews currently assess 2-4 agencies per month, and include DHS and NSC leaders as well as OMB officials.



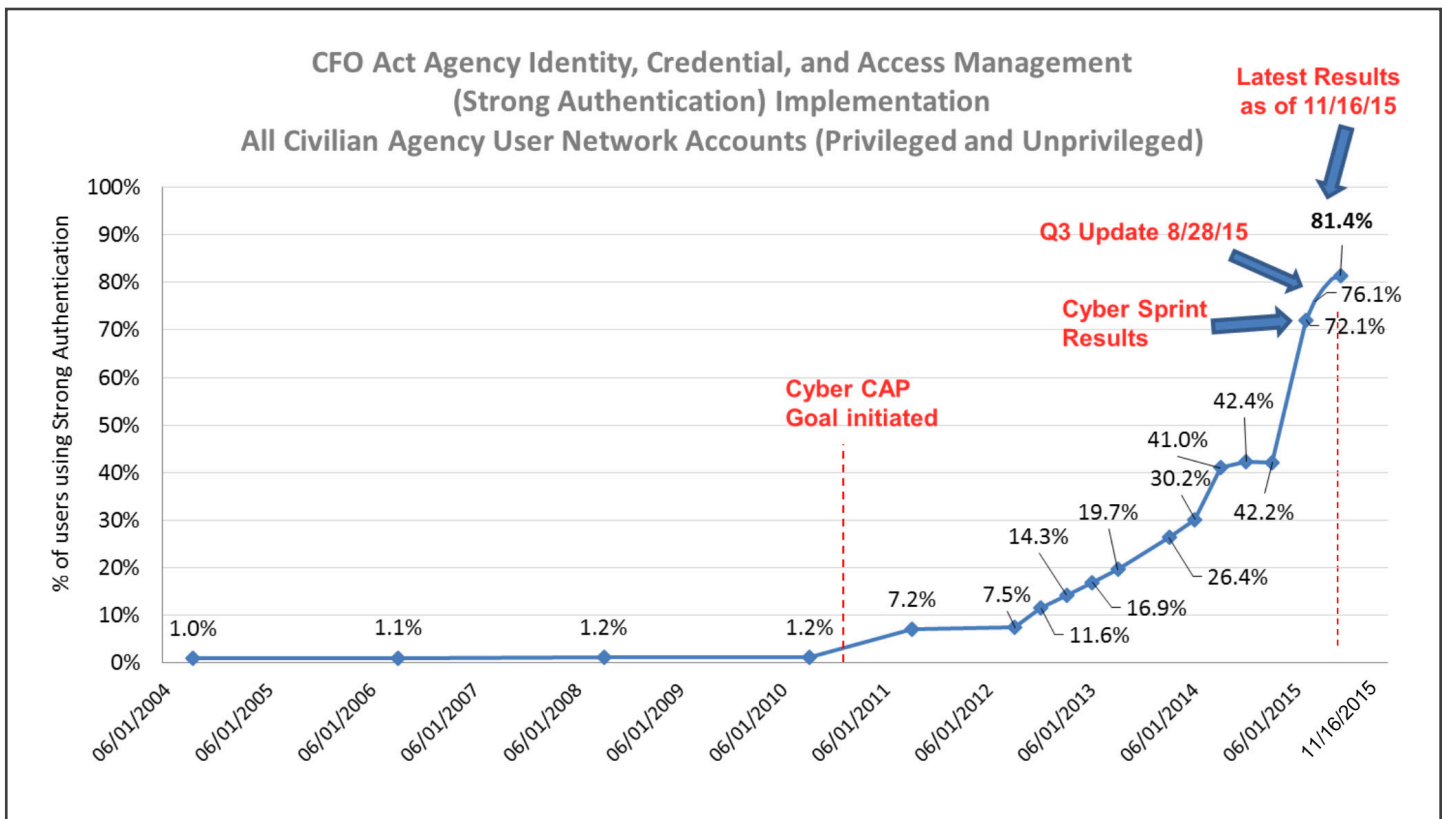
## Lessons Learned

Continued efforts to remove less valuable metrics and survey questions from FISMA have made progress year to year, though new vulnerabilities, initiatives, and threats have applied continued pressure to expand the reporting requirements.

One of the successful aspects of the Cyber Sprint was its focus on a small number of actions, allowing leadership to focus on a compact set of priorities rather than the large number of FISMA metrics, which represent diverse requirements. A key opportunity, therefore, is to explore more efficient oversight methods which help agencies and others focus on the most relevant aspects of this complex topic.

The Cyber Sprint rapidly improved agencies' implementation of the HSPD-12 initiative and is a model for future oversight. HSPD-12 required agencies to use two-factor authentication for physical and logical access by 2008.<sup>36</sup> However, PIV card issuance historically lagged behind targets and was inconsistent across agencies.<sup>37</sup> In fact, many agencies continued to require PIV cards for network access at or below a rate of just 1% for their civilian network accounts through 2010.<sup>38</sup> As indicated in the figure below, government-wide PIV compliance increased from 42 percent to 72 percent as a result of this concerted leadership attention.<sup>39</sup> This was a major success, and has been cited by many agency CIOs as a key example of effective policy implementation and oversight from OMB.

Figure E1: PIV Compliance Sprint Results, 2015 Q4 Update<sup>40</sup>



# Overall Findings

This sections presents key findings based on review of policy documents, CIO interviews, and analysis of OMB key metrics and oversight over the years. These findings are focused on government-wide activities rather than the circumstances in any particular agency.

## FINDING #1

### Government Procurement Processes Lack the Flexibility to Adapt to Evolving Cyber Threats.

A number of CIOs stated that the Federal procurement process is lengthy and complex, and does not provide them with the flexibility needed to respond quickly to cybersecurity threats. New cybersecurity vulnerabilities are discovered every day, and the tools required to mitigate those vulnerabilities may change just as quickly. The current Federal procurement process cannot adapt at that pace, leaving agencies with limited options in defending themselves against emerging cyber threats. With potential adversaries operating with access to the newest technologies, and focusing more of their efforts on compromising government systems, agencies need to be timely and flexible in their defenses. If a new vulnerability is discovered in an existing

*It sometimes takes too long to procure things especially when it comes to Cyber. A year to procure, 4 months to install and implement, too long to address the issue.*

- Agency CIO

vendor's system, the agency's contract agreement may make it difficult for agencies to switch to a different provider. The ability to respond to newly-discovered vulnerabilities in a more agile manner could improve the ability of agencies to respond to evolving threats. Agencies can also benefit from the additional testing and patching of software-based vulnerabilities that can come from open public review of Federal source code.<sup>41</sup> Efforts to address broader challenges in the IT acquisition and contracts area could improve the agility of agencies' to respond to cybersecurity threats or address vulnerabilities.<sup>42</sup> For example, GSA is adding a set of Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) to IT Schedule 70 "to better enable GSA to provide agencies quick, reliable access to key cybersecurity services before, during, and after cyber threats occur."<sup>43</sup>

**FINDING #2****The Federal IT Workforce Must Be Expanded and Strengthened in Order to Adequately Address Challenges in Cybersecurity.**

The Cyber Sprint highlighted the need to improve recruitment, retention, and training for the Federal IT workforce at large and, in particular, the Federal cybersecurity workforce. For example, many CIOs explained that they had identified well-qualified candidates for cybersecurity positions, but those candidates ended up taking other jobs—often in the private sector. CIOs attributed this to multiple issues with the Federal hiring environment: the process takes too long, relies on a confusing website/application procedure, and agencies cannot offer competitive salaries. For example, the hiring process for Federal agencies often takes significantly longer than that in the private sector and requires candidates to navigate the USAJobs process, which can be more difficult than applying for a private sector job. Even if a candidate does go through the whole process, HR selection officials with limited cybersecurity subject matter expertise may misevaluate candidates' capabilities, leading to under-qualified candidates advancing ahead of well-qualified ones.

Moreover, CIOs repeatedly mentioned that it is difficult for agencies to offer well-qualified candidates a salary that is competitive with the private sector. This salary issue also creates problems in retaining talented government employees. Internal reviews by OMB have identified additional potential issues, such as job candidates' concern that a private sector position may give them more autonomy and a more flexible work culture than a Federal information security position.

Finally, Federal hiring practices frequently rely on traditional career development models. However, many of today's information security professionals may take non-traditional career paths less focused on obtaining secondary education degrees, making it difficult for Federal hiring strategies to identify them.

Despite government-wide initiatives such as the cyber direct hire authority, some CIOs related concerns that the Cybersecurity Workforce Strategy focuses too heavily on long term solutions rather than helping CIOs with their immediate needs. However, other policy ideas being explored by OMB may address these issues, such as having OPM organize a cybersecurity recruitment fair for all Federal agencies that showcases hiring authorities and new cybersecurity career paths.

Facing significant obstacles to hiring new cybersecurity workforce, agencies have invested in training to improve the cybersecurity subject matter expertise of existing IT staff. Recent investments in workforce training have been implemented around cybersecurity concepts such as phishing and malware, including agency-wide trainings for non-experts, and expert-focused enrichment opportunities like the course on malware reverse engineering offered through US-CERT.<sup>44</sup> Similar Federal training programs and courses have augmented the adoption of modern automated practices such as CDM and tools like EINSTEIN.

**FINDING #3****Cybersecurity Sprint Demonstrated a Highly-Effective Model of OMB-to-Agency Policy Formulation and Implementation.**

The Cyber Sprint was praised by most CIOs as a success in accomplishing its goals, and provided a valuable set of lessons learned in how OMB and the White House could involve agencies in a collaborative effort. CIOs suggested that the Cyber Sprint was successful due to two key factors: ongoing involvement by high-level White House and OMB leadership, as well as early collaboration between government-wide policy makers and agency CIOs to design implementation plans that allowed agencies the flexibility to choose an approach that worked with their specific needs. CIOs listed some lessons learned from the Cyber Sprint: the need for continuous engagement between OMB and agency leadership and between agency leadership and CIOs; providing agencies with verifiable and achievable objectives and timeframes; allowing agencies some latitude within a policy framework to execute strategies that work within their structural constraints, and obtaining agency buy-in prior to the start of a new policy initiative.

Another factor cited for the Cyber Sprint's success was that it asked agencies to focus on a small number of actions. This is compared to the broader, high number of FISMA metrics — many with unclear causal relationships to each other — that create a perception that “everything is important,” which runs the risk of some leaders concluding “nothing is important.”

*The Cyber Sprint was helpful because it allowed us to focus on privileged users. The Deputy Secretary and CIO were in charge and it was very focused/scoped with a lot of follow-up.*

- Agency CIO

**FINDING #4****High Visibility in Cybersecurity Leads to Multiple Policy Messages, Metrics, and Priorities.**

CIOs have stated that they face an increasing number of reporting requirements in relation to their cybersecurity efforts, even while OMB has tried to reduce the requirements. The required reporting used in annual FISMA reports, CAP goal reporting, PMC meetings, and West Wing reviews of cybersecurity has led to a large number of varied metrics and information, according to agencies. Although many agency CIOs agree that there is some alignment of metrics across oversight mechanisms, they still note that reporting could benefit from streamlining and centralization.

Cyber-related metrics, especially those used in PortfolioStat, are some of the most consistent year-to-year of any IT policy area. Despite this consistency,

*300% more metrics (120 metrics quarterly) are being asked for us to report in regards to FISMA. Too many requirements, hard to tell what is a priority. Our challenge is to convince Tony and others [to streamline]. I only have time for 4 things and you are asking for 40.*

- Agency CIO

agencies did not mention PortfolioStat as a major channel for cybersecurity discussions. Instead, agencies pointed to CyberStat Reviews and the PMC Assessment as the driving force for cybersecurity discussions. The proliferation of cybersecurity efforts has led to an environment where agencies seek guidance in identifying immediate priorities. While OMB and other government-wide IT leaders in cybersecurity policy have taken steps to reduce the variety and burden of these reporting requirements, continued efforts to better align agency attention with the highest impact actions could be valuable.

# Notes

1. Circular A-130: Managing Information as a Strategic Resource. <https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>
2. M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>
3. For more information on Continuous Diagnostics and Mitigation (CDM) Program, see: <http://www.gsa.gov/portal/content/177883>
4. For more information about the OPM breach, see: <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>
5. Public Law No. 107–347. E-Government Act of 2002. 12/17/2002. <https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>
6. White House Press Release. “Cybersecurity event fact sheet and expected attendees” 5/29/2009. <https://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees> and “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”: [https://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)
7. White House Press Release. “Fact Sheet: The Administration’s Cybersecurity Accomplishments”. 5/12/2011. <https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments>
8. “Cybersecurity” became one of the original “interim CAP goals” announced in 2012 in the FY 2013 President’s Budget, as described in GAO report on CAP Goals. GAO-14-526. Managing For Results: OMB Should Strengthen Reviews of Cross-Agency Goals. 5/20/2014. <http://www.gao.gov/assets/670/664022.pdf>
9. CyberStat was established in the January 2011 OMB memorandum M-11-33 and DHS FISM 11-02 message. M-11-33. FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. 9/14/2011. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf>
10. Other documents include: a publicly-releasable summary of the “Comprehensive National Cybersecurity Initiative” (CNCI)--an internal guiding cybersecurity policy document, the “International Strategy for Cyberspace” (May 2011), the “National Cyber Incident Response Plan” (NCIRP), OSTP’s “Cyber Research and Development Framework,” and the “National Strategy for Trusted Identities in Cyberspace” (NSTIC) (April 2011)
11. Enhancing and Strengthening the Federal Government’s Cybersecurity. 6/11/2015. [https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact\\_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf](https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf)
12. The Sprint Team, led by OMB was comprised of representatives from the National Security Council (NSC), the Department of Homeland Security (DHS), the Department of Defense (DOD), and other Federal civilian and defense agencies
13. M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>
14. White House Press Release. “Fact Sheet: Cybersecurity National Action Plan.” 02/09/2016 <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>
15. White House Press Release. “Fact Sheet: President Obama Announces Computer Science For All Initiative”. 01/30/2016. <http://www.whitehouse.gov/the-press-office/2016/01/30/fact-sheet-president-obama-announces-computer-science-all-initiative-0>
16. White House Press Release. “Fact Sheet: Cybersecurity National Action Plan”. 02/09/2016. <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>
17. M-16-15. Federal Cybersecurity Workforce Strategy. 06/12/2016. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf>
18. FISMA requires agencies to follow certain instructions from organizations such as OMB and NIST. For example, FISMA requires agencies to comply with NIST’s Federal Information Processing Standards (FIPS) and OMB FISMA reporting requirements, which in turn reference other NIST documents called Special Publications (SPs), such as those describing how to conduct certification and accreditation procedures. See “Page iv” of NIST SP 800-37 for a summary of this framework: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
19. This requirement is described in FIPS 199. Standards for Security Categorization of Federal Information and Information Systems. 2/2004. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> and NIST SP 800-60. Guide for Mapping Types of Information and Information Systems to Security Categories. 8/2008. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf>
20. NIST SP 800-37. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. 2/2010. <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
21. Circular A-130 Managing Federal Information as a Strategic Resource. July 2016. <https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>
22. M-11-33. FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. 9/14/2011. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf>
23. M-16-03. Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements” 10/30/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf>





24. M-16-03. Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements. 10/30/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf>
25. M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>
26. M-16-15. Federal Cybersecurity Workforce Strategy. 6/12/16. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf>
27. For more information on Continuous Diagnostics and Mitigation (CDM) Program, see: <http://www.gsa.gov/portal/content/177883>
28. M-14-03. Enhancing the Security of Federal Information and Information Systems. 11/18/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf>
29. FY2017 Budget of the United States. "Analytical Perspectives: Information Technology." Available at: [https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/ap\\_17\\_it.pdf](https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/ap_17_it.pdf)
30. For more detailed information about efforts related to FedRAMP, see Policy Chapter B: IT Infrastructure Modernization. Also see: Office of Management and Budget. "Security Authorization of Information Systems in Cloud Computing Environments". 11/08/2011. <https://www.fedramp.gov/files/2015/03/fedrampmemo.pdf>
31. M-14-03. Enhancing the Security of Federal Information and Information Systems. 11/18/2013 <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf>
32. "9/11 Commission Report". 2004. <https://9-11commission.gov/report/911Report.pdf>
33. President George W. Bush. HSPD-12. Policy for a Common Identification Standard for Federal Employees and Contractors. 8/27/2004. <http://fas.org/irp/offdocs/nspd/hspd-12.html> and M-05-24. Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors. 8/5/2005. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>
34. NIST. "National Strategy for Trusted Identities in Cyberspace (NSTIC): Our Focus". <https://www.nist.gov/itl/nstic/our-focus>
35. 18F blog post. "Building a modern shared authentication platform". 5/10/2016. <https://18f.gsa.gov/2016/05/10/building-a-modern-shared-authentication-platform/> and see Login.gov homepage: <https://pages.18f.gov/identity-intro/>
36. President George W. Bush. HSPD-12. Policy for a Common Identification Standard for Federal Employees and Contractors. 8/27/2004. <http://fas.org/irp/offdocs/nspd/hspd-12.html>
37. GAO-11-751. Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards . 9/20/2011. <http://www.gao.gov/new.items/d11751.pdf>
38. Performance.gov. "Cross-Agency Priority Goal: Cybersecurity". FY 2015 Q4 Update. <https://www.performance.gov/content/cybersecurity#progress-update>
39. Performance.gov. "Cross-Agency Priority Goal: Cybersecurity". FY 2015 Q4 Update. <https://www.performance.gov/content/cybersecurity#progress-update>
40. Ibid
41. For more information about government-wide efforts to encourage public review of Federal source code, see: M-16-21. Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. 8/8/2016. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m\\_16\\_21.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf)
42. For more information about the IT Acquisition and Contracts policy area, see Policy Chapter F: IT Acquisition and Contracts Management
43. General Services Administration. "GSA IT Schedule 70 to Incorporate Highly Adaptive Cybersecurity Services SIN". 08/17/2016. <https://interact.gsa.gov/document/gsa-it-schedule-70-incorporate-highly-adaptive-cybersecurity-services-sins>
44. National Initiative For Cybersecurity Careers And Studies. "Malware Reverse Engineering". 10/4/2016. <https://niccs.us-cert.gov/training/search/anrc/malware-reverse-engineering>

# IT Acquisition and Contracts Management

With more than one out of every six dollars of federal government spending going to contractors, it is imperative that the federal government leverages its buying power, drives more consistent practices across federal agencies, shares information, and reduces duplication while providing better results for the American taxpayers.

– Anne Rung, Former Administrator, Office of Federal Procurement Policy, OMB

## Summary

 <p>Talent</p>	Category management efforts <sup>1</sup> and the Acquisition Gateway could greatly improve agency access to acquisition staff with modern IT expertise.
 <p>Accountability</p>	The Federal IT Acquisition Reform Act (FITARA) provides agency CIOs with significantly increased visibility and oversight into all IT acquisitions, requiring the CIO or a delegate to approve all purchases.
 <p>Risk</p>	Due to the complexity and slowness of the Federal acquisition process, CIOs cited numerous concerns with the ability to procure effective and innovative technology solutions, especially for cybersecurity related technology. <sup>2</sup> 82% of IT projects larger than \$2M do not have managers with Federal Acquisition Certification for Project or Program Managers. <sup>3</sup>
 <p>Policy</p>	Acquisition in the Federal government is considerably more complex and cumbersome than the private sector due to requirements to ensure fair competition and avoid frivolously spending taxpayers' dollars. Efforts have been made to expand awareness of how to leverage flexibilities within the Federal Acquisition Regulations to better support agile and other modern IT development practices; however significant barriers in the acquisition workforce remain.

# IT Acquisition and Contracts Management

---

## Overview

The Federal acquisition environment is often inefficient, cumbersome, and complex. In addition, current acquisition processes do not necessarily incentivize the use of agile or other innovative and modern information technology development and purchasing practices. The slowness, limitations, and uncertainties of the acquisition process were frequently cited during CIO interviews as major challenges in purchasing IT. Agencies face significant challenges in updating legacy IT systems given the long development and lead times, and the increased costs due to maintaining the existing systems and developing a new modern system alongside.

The Federal Acquisition Regulation (FAR) governs the acquisition process. For a variety of reasons, the FAR contains specific rules that can lengthen the amount of time it takes for the Federal government to acquire goods and services. As an example, the FAR mandates the use of small, minority-owned, or disadvantaged businesses in a certain percentage of Federal contracts.<sup>4</sup> While encouraging entrepreneurship and supporting small businesses is an important goal, the additional requirements needed to meet small-business set asides can add months

to the acquisition process for larger investments. Moreover, complying with the processes and reporting requirements stemming from the FAR can make doing business with the government expensive for businesses, reducing the pool of potential vendors for agencies to work with. Another unique attribute of the Federal acquisition process is the protest process which allows losing bidders to protest the government's purchasing decisions. Agencies face the potential for vendor protests if regulations or agency policies are not followed correctly. Protests can result in significant delays in beginning work, and if sustained, may result in a new competition or cancellation of a contract.<sup>5</sup>

Agency CIOs sometimes anticipate that potential acquisitions will take up to two years to ultimately select a vendor. A result of this delay is that technologies that are considered state-of-the-art when a new procurement is envisioned are often outdated by the time a contract is awarded. The lengthy procurement process can also create significant barriers to improving the cybersecurity posture of an agency because of difficulties in rapidly procuring and deploying innovative, cutting-edge cybersecurity technologies.



Best practices in the acquisition and development of IT favor agile development principles that should enable Federal agencies to accomplish their missions more efficiently, effectively, and economically. However, managing and procuring these projects in such a way requires a fundamental shift in how program managers and contracting officers work with vendors to obtain services. Typically, agencies define as many requirements as possible at the outset of the procurement process. These practices often lead agencies towards more traditional waterfall style development cycles, building large, complex systems over the course of years rather than using more agile development principles.

The principal policy leader for government-wide acquisition initiatives is the Office of Management and Budget's (OMB) Office of Federal Procurement Policy (OFPP), often acting in partnership with the Office of the Federal Chief Information Officer (OFCIO) and the General Services Administration (GSA). There have been numerous efforts to update and improve the acquisition process to better accommodate the specifics of IT purchases, ranging from empowering the CIO, improving the speed of acquisitions, enhancing innovation, and buying commonly acquired goods or services at an enterprise level.

The recently enacted Federal IT Acquisition Reform Act (FITARA) requires agencies to increase their use of agile development, and OMB oversight mechanisms such as the Capital Planning and Investment Control were modified to better track agency agile projects.<sup>6</sup> In addition, OFPP has been working to improve the agility and speed by which the Federal government can buy goods and services, especially for IT. These represent positive steps towards improving IT acquisition practices, but more work remains to be done.

A full treatment of all government acquisition procedures and issues is outside the scope of this document. Instead, this document focuses on several initiatives and efforts that have been undertaken to improve the ability of Federal agencies to successfully procure IT. These efforts sought to:

- Leverage the Federal government's ability to buy as an enterprise;
- Strengthen acquisition training and certification;
- Increase awareness of contract flexibilities and outreach to the contractor community; and
- Increase CIO oversight into the IT procurement process.

# Policy Evolution

One of the first efforts to improve IT acquisitions began with adopting performance-based acquisitions. A performance-based acquisition differs from conventional government procurements by changing the requirements documents. Instead of mandating specific actions, workflow or actions by a contractor, the government outlines objectives that it would like to be met, and allows companies to propose their own approach to meet those objectives. The government then monitors their performance in line with the objectives, evaluating them on a set of agreed-upon metrics. By focusing on objectives, and not process, the government enables companies to provide best-in-breed or more innovative solutions, focusing on the outcomes that the government desires. As early as 2001, agencies were mandated to improve their use of performance-based service contracts.<sup>7</sup> IT projects are excellent targets for performance-based contracts given the rapid evolution of technology and the ability to enhance digitized processes to shorten timeframes. However, performance-based acquisitions require additional time investment from program staff and more deliberative proposal reviews, which has slowed their adoption.

The Federal IT Acquisition Reform Act (FITARA)<sup>8</sup> represents the latest effort to improve the ability of Federal agencies to successfully procure IT. In particular, FITARA seeks to increase the CIO's awareness, oversight and authority over IT-related procurements by requiring all agency procurements that include IT be approved by the CIO, or via a delegated individual such as a bureau CIO. By providing this visibility into IT procurements, lawmakers sought to ensure that the agency CIO is fully integrated,

from the start, into the agency's processes for developing and delivering IT investments right.

## Key Initiatives

- Buying as an Enterprise: Sharing Contract Agreements**

Provides access to multi-agency contract agreements to increase the government's purchasing power while simultaneously decreasing costs.
- Buying as an Enterprise: Strategic Sourcing and Category Management**

Facilitates access to expertise offered through Federal Strategic Sourcing Initiative analysts, GSA's Category Managers, TechFAR Hub, or agency buyer's clubs and acquisition innovation labs.
- Buying as an Enterprise: Consolidating IT Procurement Authority Under the CIO**

Empowers CIOs around commodity IT responsibilities, expands CIO approvals across all IT acquisitions.
- Buying as an Enterprise: Standardizing Requirements & Configurations**

Rationalizes and reduces duplication in commodity IT, software licenses, desktops and laptops, and other mission-support areas.
- Acquisition Training and Certification**

Improves acquisition workforce skills through Specialized IT Acquisition Cadres, acquisition focus in Agency Human Capital Plans, and expanded FAC P/PM requirements.
- Awareness and Outreach**

Helps IT professionals navigate and better apply procurement procedures through publications such as acquisition Mythbusters materials, TechFAR Handbook, and contracting guidance for modular development.
- Federal IT Acquisition Reform Act (FITARA)**

Further empowers CIOs as the key IT leaders at their agencies by requiring all agency procurements that include IT to be approved by the CIO.

*The strategies consist of numerous efforts and actions which took place over a broad period of years, and many are ongoing today. As such, specific years are not included.*

## Buying as an Enterprise

A common theme of government-wide acquisition initiatives has been trying to improve the ability to make decisions and agreements as an enterprise rather than as thousands of separate unrelated offices. By pooling acquisition requirements, contracts, and expertise, Federal agencies can generate economies of scale and realize significant savings. This can happen both within an agency and amongst agencies. Buying as an enterprise is more than simply “buying in bulk” – the ultimate goal is to make smarter decisions at an aggregate level rather than many fragmented, isolated decisions. Additionally, these efforts can create opportunities to accelerate acquisition timelines (critical given expectations in today’s marketplace) and ensure broader competition. The discussion below focuses on improving the Federal government’s attempts to buy as an enterprise through:

- Sharing Contract Agreements,
- Strategic Sourcing and Category Management,
- Consolidating IT Procurement Authority Under the CIO, and
- Standardizing Requirements and Configurations.

*“With over 3,300 contracting offices and often thousands of contracts for the same goods and services – many with the same vendor – the Federal Government buys like many small, separate entities.”*

- Anne Rung

Former Administrator, Office of Federal Procurement Policy, OMB in testimony June 10, 2015 before the Subcommittees on Information Technology and On Government Operations of the Committee on Oversight and Government Reform United States House of Representatives

## Buying as an Enterprise: Sharing Contract Agreements

The government has expanded the variety of IT services and products offered through shared multi-agency contract mechanisms, which help agencies leverage the government’s buying power. These agreements, vehicles, contracts, and other mechanisms allow various forms of “negotiate once, buy many” options for agencies to use.

A major focus of OMB’s IT acquisition efforts is to expand and publicize these options and address obstacles agencies encounter in using them. Below is a brief listing of some of the methods by which agencies can share contracts.<sup>9</sup>

- *Blanket Purchase Agreements (BPA)* are simplified acquisitions that Federal agencies use to fill anticipated repetitive needs for supplies or services. BPAs allow the government to negotiate a portion of potential contracts up front with vendors so that future purchases are streamlined. As GSA describes them, “blanket purchase agreements eliminate such contracting and open market costs as the search for sources, the need to prepare solicitations, and the requirement to synopsise the acquisition.”<sup>10</sup> Some BPAs may be multi-agency while others aggregate needs across multiple programs or over time for a particular type of need or area of products or services.
- *Indefinite-Delivery, Indefinite Quantity (IDIQ)* agreements allow an agency to negotiate terms with a vendor once and then make additional future purchases using that pre-existing agreement.
- *The Federal Supply Schedules* program consists of contracts for similar or

comparable goods or services from more than one supplier at varying prices (awarded usually by GSA), for example, GSA’s Schedule 70 for information technology. GSA’s SmartBuy program for enterprise software is an example of a topic-specific purchasing program which leverages Schedule 70 to offer enterprise software options for agencies.

- *Government-wide Acquisition Contracts (GWAC)* are types of multi-agency contracts with more flexibility and fewer limitations than other multi-agency contracts. GSA operates a variety of IT related GWACs through its Federal Acquisition Service.
- *Other multi-agency contracts* enabled by statutory flexibilities, such as the Economy Act, are subject to various other limitations, conditions, or requirements.<sup>11</sup>

These mechanisms have provided agencies access to shared contracts and agreements for products and services such as cloud platforms (GSA’s Salesforce Implementation, Integration and Support BPA),<sup>12</sup> IT consulting and development (IT Schedule 70), enterprise software (SmartBUY),<sup>13</sup> mobile services (FSSI-Wireless), and telecommunications (Networx, which will be succeeded by Enterprise Infrastructure Solutions). As OMB and GSA’s collaboration with agencies through efforts such as Category Management expands, new agreements offering more options to agencies are likely to make use of similar flexibilities. However, while the potential for savings is clear, in many situations, agencies may wish to switch to one of these consolidated contracts, but the timing of their current contracts does not allow them to, or it may be too costly to transition out of their current contract ahead of schedule.

Buying as an Enterprise: Sharing Contract Agreements	
Summary of Effort	<ul style="list-style-type: none"> <li>• Multi-agency contract mechanisms which help agencies buy within the scale of the Federal government</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>• GSA’s SmartBUY program - government-wide approach for enterprise licenses on common software</li> <li>• Category Management</li> <li>• Blanket Purchase Agreements (BPAs)</li> <li>• Indefinite-Delivery, Indefinite Quantity (IDIQ) agreements</li> <li>• Federal Supply Schedules</li> <li>• Government-wide Acquisition Contracts (GWAC)</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>• Increase an agency’s purchasing power while simultaneously decreasing costs</li> <li>• Encourage agencies to use larger, shared contract agreements</li> <li>• These agreements allow various forms of “negotiate once, buy many” options for agencies to use</li> </ul>

*“The Salesforce BPA is a significant step forward in supporting FITARA, our customers, and improving acquisition efficiency and effectiveness in the Federal Government. This unique, first-of-its-kind, cross-agency initiative will reduce the number of duplicative contracts for these services and lower overall costs by leveraging the buying power of the government into a consolidated services vehicle.”*

- Tom Sharpe, FAS Commissioner, from GSA news release on award of Salesforce BPA

## Buying as an Enterprise: Strategic Sourcing and Category Management

OMB and GSA have worked to provide agencies access to shared groups of experienced IT acquisition professionals to offer support and expertise regarding their IT needs. This approach to pooling expertise centrally and making it available to agencies can provide greater access to best practices in industry, acquisition, and familiarity with emerging technology.

Since 2005, the Federal Strategic Sourcing Initiative (FSSI) has offered a “structured and collaborative process of critically analyzing an organization’s spending patterns to better leverage its purchasing power, reduce costs, and improve overall performance” in selected acquisition areas, such as mobile service contracts.<sup>14</sup> OMB began to explore extending this strategic sourcing approach beyond its original areas of focus in 2012.<sup>15</sup>

OMB and GSA expanded the approach to six IT-related sub-categories through the Category Management and Acquisition Gateway programs launched in 2014.<sup>16</sup> The first government-wide “category manager” was appointed for IT in 2015, who now leads the six IT areas (“Hallways”) of IT Software, Hardware, Consulting, Security, Outsourcing, and Telecommunications. Additionally, TechFAR Hub, also hosted by GSA, provides a platform for a community of experts with a focus on agile methodology and modern IT digital services.<sup>17</sup> OMB has also encouraged agencies to pool their acquisition expertise at the agency level through agency “buyer’s clubs” or “acquisition innovation labs” led by acquisition innovation advocates.<sup>18</sup>

Buying as an Enterprise: Strategic Sourcing and Category Management	
Summary of Effort	<ul style="list-style-type: none"> <li>• Provide access to shared groups of experienced IT acquisition professionals to offer support and expertise around agencies’ IT needs</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>• FSSI</li> <li>• Category Management</li> <li>• Acquisition Gateway<sup>19</sup></li> <li>• TechFAR Hub</li> <li>• Acquisition Innovation Labs</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>• Reduce duplication within and between agencies</li> <li>• Increase focus on and use of agile methodologies</li> </ul>

## Buying as an Enterprise: Consolidating IT Procurement Authority Under the CIO

Federal dollars are often appropriated directly to a program or lower level bureau, rather than to the agency as a whole. As a result, IT purchases are often made within programs or bureaus directly without the supervision or knowledge of the agency CIO. This can lead to unnecessary duplication, missed opportunities for savings, and procurements that are not aligned with agency-wide strategies. Over the years, both OMB and Congress have taken steps to increase the responsibility of CIOs and extend their influence over IT acquisitions into agency programs and bureaus.

For example, in August 2011, as part of a broader effort to strengthen CIO authorities, OMB directed agencies to “pool their agency’s purchasing power across their entire organization to drive down costs, improve service for commodity IT” and use shared services.<sup>20</sup> To assess agency progress towards this goal, OMB launched the PortfolioStat initiative, a “face-to-face, evidence-based review...of an agency’s IT portfolio” that focused on the consolidation of commodity IT at an agency in March 2012.<sup>21</sup> As a result of the PortfolioStat process, agencies were required to develop commodity IT consolidation plans that were reviewed and approved by OMB. These plans resulted in commitments from agencies to achieve over \$2.5 billion in target cost implications by 2015.<sup>22</sup>

Over time, OMB followed up on these projects with 2013 PortfolioStat and tracked their actual savings in regular reports to Congress.<sup>23</sup> OMB incorporated the proposed savings from these IT commodity consolidation plans into the overall budget process for FY 2014, including offering ways for agencies to describe how they would turn their cuts to commodity IT into investment in innovative technology programs.<sup>24</sup>

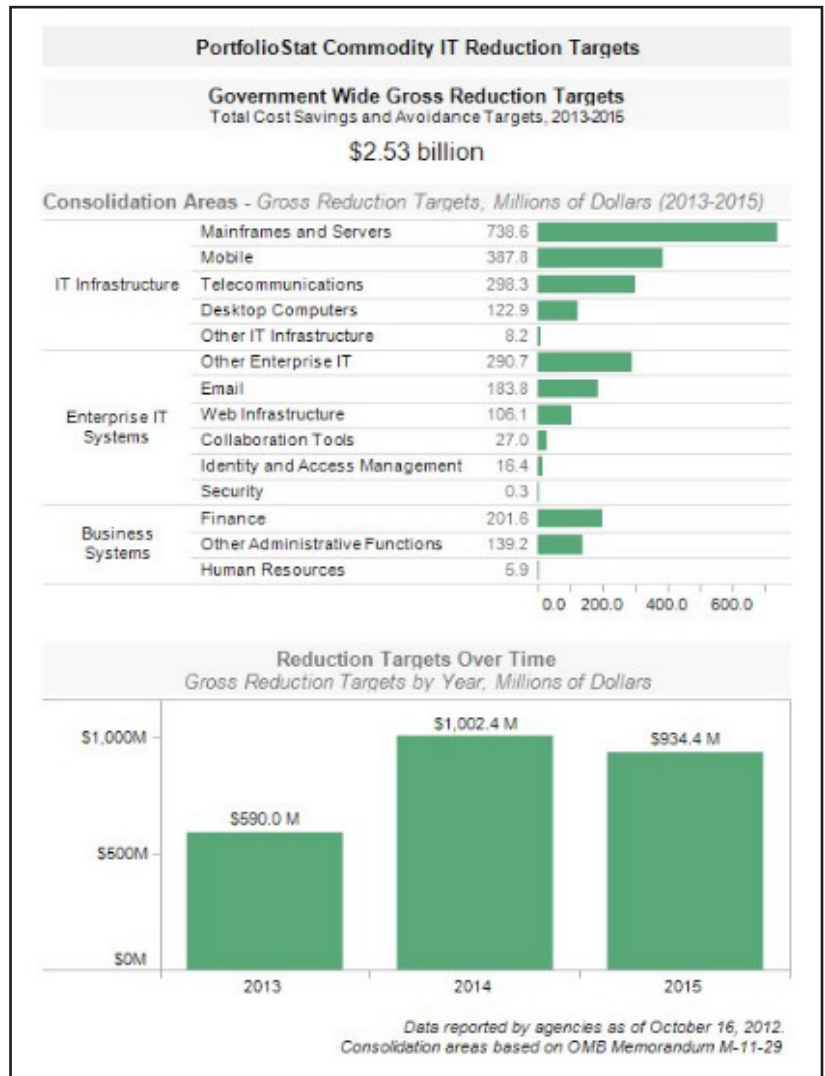


Figure F1: PortfolioStat Commodity IT Reduction Targets

Despite the new CIO Authorities policy and creation of the PortfolioStat initiative, agency CIOs did not necessarily see a significant shift in their procurement authorities for several reasons. There are a number of steps which could address this. First, although OMB declared that “the CIO shall pool their purchasing power across their entire organization to drive down costs and improve service for commodity IT,” there was no real mechanism to do so. Changing how agencies actually receive their funding or improving the CIOs’ visibility into funding at the program and bureaus could help CIOs take this action. Without these steps, agency CIOs were given responsibility for consolidating their agencies commodity IT, but they were not given the authority to actually accomplish it.

Second, while the supporting OMB memoranda<sup>25</sup> provided examples of what constituted “commodity IT,” actually defining the term could help strengthen the approach. Without a clear definition, bureaus and programs were able to avoid including systems that could be consolidated.

Finally, this attempt to further empower agency CIOs appears to have been hampered by a lack of consistent oversight. For example, although the first PortfolioStat (2012) focused on the consolidation of commodity IT, the next year’s version of PortfolioStat (2013) shifted the focus away from the consolidation of commodity IT.<sup>26</sup> While agencies established Commodity IT Consolidation Plans as a part of PortfolioStat 2012, there is no evidence OMB followed-up on these plans or asked agencies to send updated status of in-progress projects or results of completed projects.

Buying as an Enterprise: Consolidating IT Procurement Authority Under the CIO	
Summary of Effort	<ul style="list-style-type: none"> <li>Expand the responsibility and influence of agency CIOs over IT acquisitions into programs and bureaus</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>Commodity IT Consolidation Plans</li> <li>Developed PortfolioStat</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>Encompass true portfolio management for all IT</li> </ul>

## Buying as an Enterprise: Standardizing Requirements and Configurations

Reducing the need for variation across agencies in requirements, features, and configurations of software and hardware purchased can lead to significant savings, increased operational efficiencies, and even a stronger cybersecurity posture.<sup>27</sup> This idea is reflected in two 2016 memoranda laying out standard configurations for Federal laptops and desktops and agency-wide approaches to software license management.

- *Desktops and Laptops.* OMB’s first Category Management memorandum made standardized configurations mandatory, requiring that agency CIOs: “ensure that at least 80% of their agency’s new basic laptop and desktop requirements are satisfied with [a government-wide approved] standard configuration” unless an exception is granted.<sup>28</sup> Numerous contract vehicles were identified to assist agencies with procuring desktops and laptops, however, several agency CIOs indicated they believed they could get better pricing on their own procurements. Additional efforts to leverage purchasing of desktops and laptops as an enterprise are needed.
- *Software License Management.* In addition, reducing the complexity of agencies’ software license purchases was a major focus in OMB’s Category Management memorandum.<sup>29</sup> This required agencies to appoint an agency-wide enterprise software manager, establish agency-wide software license inventories, and implement a “Software Management Centralization Plan” while reporting all cost savings to OMB’s Integrated Data Collection.

Buying as an Enterprise: Standardizing Requirements and Configurations	
Summary of Effort	<ul style="list-style-type: none"> <li>• Created standard configurations for desktops, laptops, and agency-wide approaches to software license management</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>• M-16-02 Category Management Policy 15-1</li> <li>• M-16-12 Category Management Policy 16-1</li> <li>• Software Management Centralization Plan</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>• Mandated no less than 80% standardization across an agency for laptops and desktops</li> <li>• Alignment across these areas could achieve significant savings, increased operational efficiencies, and a stronger cybersecurity posture</li> </ul>

*Getting acquisition officers trained on how to acquire utility services that aren't defined as such in the FAR is a huge issue. Cloud First says SaaS, IaaS, etc. are utilities, but the FAR doesn't treat them that way.*

- Agency CIO



## Acquisition Training and Certification

Newer digital technologies and agile methodologies frequently present challenges to an agency acquisition workforce trained in an era of legacy systems and a waterfall development approach. Working through the Federal Acquisition Institute (FAI), Defense Acquisition University, private sector vendors, and other Federal agencies, OFPP has sought to equip the Federal acquisition workforce with the knowledge, skills, and expertise in using emerging tools and technologies in a more agile manner to solve agencies' needs. The U.S. Digital Service also created a new Digital IT Acquisition Professional Training Program (DITAP), which seeks to train contracting officers on agile acquisition principles and how to leverage the FAR to support these activities.<sup>30</sup>

*The biggest opportunity is streamlining how we do our acquisitions and hiring. — I have a project that might get approved this month that is 18 months behind schedule before any work is done, before any protest. We were not able to buy any network hardware for two years due to an acquisitions protest. It is unacceptable for a BPA to take 2.5 years. Very understaffed and fearful of risk. It has put my infrastructure at end of life with no patches. 70% of [my agency's] network is at risk now.*

- Agency CIO

For example, in 2011, OFPP issued guidance defining “Specialized IT Acquisition Cadres,” highlighting the training and skillsets of particular relevance for the IT acquisition workforce.<sup>31</sup> In 2013, under the Federal Acquisition Certification program, OFPP began a process to expand and strengthen the acquisition training and certification requirements (known as “FAC P/PM”) for project managers and program managers, with a particular focus on the IT workforce.<sup>32</sup> More recently, in 2015, as a part of the implementation of FITARA, OMB instructed agencies to include detailed analysis of these IT acquisition cadres in their Agency Human Capital Plans.<sup>33</sup> Enhanced acquisition training needs to extend beyond acquisition staff to encompass project managers who have significant acquisition responsibilities. This need is underscored by the fact that 82% of IT projects larger than \$2M do not have managers with a Federal Acquisition Certification for Program or Project Managers.<sup>34</sup>

Acquisition Training and Certification	
Summary of Effort	<ul style="list-style-type: none"> <li>Provide the training tools needed to equip the Federal acquisition workforce with the knowledge, skills, and expertise so they can use emerging tools and technologies in a more agile manner</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>Specialized Acquisition Cadres</li> <li>Strengthen the acquisition training and certification requirements</li> <li>Digital IT Acquisition Professional Training Program (DITAP)</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>Achieve better value for government acquisitions</li> <li>Develop a digital service core-plus specialization for contracting professionals</li> </ul>

## Awareness and Outreach

In addition to the training opportunities discussed above, OMB also initiated a series of education efforts to increase familiarity amongst IT project managers and the acquisition workforce of the flexibilities and options allowed by procurement regulations. This began with the 2011 release of OMB’s *25 Point Implementation Plan to Reform Federal IT*,<sup>35</sup> which included a series of “mythbuster” documents, guidebooks, and other explanatory documents designed to dispel common misconceptions of procurement procedures or illustrate examples of flexibility in the FAR. A few examples of these documents include:

- OMB’s “Mythbusters” documents addressed the misconception that meeting with a potential vendor before a planned award was generally forbidden by outlining situations where that kind of “market research” is not only permissible, but encouraged.<sup>36</sup>
- The TechFAR Handbook provides guidelines on how to support agile development and other modern project management approaches using existing procedures in Federal regulations.<sup>37</sup>
- OMB’s *2012 Contracting Guidance to Support Modular Development* similarly outlined how to use existing procedures to support innovative procurements.<sup>38</sup>

Each of these initiatives did not seek to change the procurement process, but rather to improve general understanding of how the existing procedures may be used to support innovative IT practices. Breaking through many of these myths requires a long-term, coordinated approach to changing people’s understanding of the rules. OMB has tried to improve awareness of these documents by including “number of contracting officers who have finished the Digital Service Certification Program” which draws on materials such as the TechFAR,<sup>39</sup> as part of the Smarter IT Delivery CAP Goal.

Awareness and Outreach	
Summary of Effort	<ul style="list-style-type: none"> <li>• Increase familiarity amongst IT project managers and acquisition workforce of the flexibilities and options allowed by procurement regulations</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>• “Mythbusters”</li> <li>• Additional guidelines in TechFAR Handbook on how to support agile development</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>• Improve the general understanding of how existing processes can support innovative IT practices</li> </ul>

## The Federal Information Technology Acquisition Reform Act (FITARA)

In December 2014, Congress attempted to further empower agency CIOs in the acquisition process by passing FITARA.<sup>40</sup> In addition, the subsequent development of OMB’s Common Baseline of CIO roles and responsibilities reinforced CIO approval of all IT acquisitions through partnership with the CAO around all acquisition strategies and acquisition plans. To improve how the Federal government acquires, implements, and manages its IT investments, FITARA gave the Agency CIO more authority over the budget, governance, and personnel processes for Agency IT investments. With regard to the acquisition process, FITARA stated that an agency “may not enter into a contract or other agreement for information technology or information technology services, unless the contract or other agreement has been reviewed and approved by the CIO of the agency.”<sup>41</sup> The goal is for CIOs to participate earlier in the conversation as an enabler for the mission staff.

Ensuring CIO visibility is a minimal first step, additional efforts are needed by CIOs to be proactively involved in acquisitions early in the process to leverage potential efficiencies and ensure strategic alignment.<sup>42</sup> For example, despite its strong statutory language, CIOs expressed concerns regarding this authority during interviews, indicating there remains room for improvement and clarification. As one CIO put it: “what does it mean when FITARA says ‘I need to approve all purchases?’ Am I just showing up at the 11th hour, approving requisitions? I want to have more say over the formulation of the spend.”

## The Federal Information Technology Acquisition Reform Act (FITARA)

Summary of Effort	<ul style="list-style-type: none"> <li>Provide CIO with more authority as it relates to IT investments</li> </ul>
Major Initiatives	<ul style="list-style-type: none"> <li>FITARA</li> <li>OMB Common Baseline for the Management of IT</li> </ul>
Goals of Effort	<ul style="list-style-type: none"> <li>Consolidate knowledge of agency IT acquisition efforts and strategy in CIO’s office</li> </ul>

## Metrics and Oversight

### Primary Objective Emphasized in Metrics and Oversight

Based on the metrics used in oversight, the primary focuses of OMB's efforts in IT acquisition have been to reduce the cost of IT goods and services and improve agency satisfaction with the acquisition staff. By better leveraging the scale of the Federal government and by not repeating acquisition processes unnecessarily, agencies can reduce the cost of IT acquisition. Repeatedly, the potential value of efforts like strategic sourcing, category management, and commodity IT consolidation has been described in terms of the potential reductions in spending due to elimination of duplicative processes or purchases.

### Examples

PortfolioStat and the Benchmarking initiative have gathered data to establish a baseline of Federal spending in common business areas, through commodity IT data calls and management function spending data calls, specifically:

- In PortfolioStat, agencies reported how many GWACs and BPAs they used for each commodity IT area; and
- In the Benchmarking initiative, cost-efficiency, customer satisfaction, and operational metrics (e.g., a comparison of cost per email box versus email satisfaction) were developed to provide further context into which agencies were more efficient at each area.

Strategic sourcing and category management have established their own more nuanced baseline by defining the total likely "addressable spend" within each business area or type of services they

examine, then measuring agency progress adopting or applying recommended approaches to that addressable spend. OMB assumes that 7.5% of any services using strategic sourcing are achieved as cost savings, according to the Category Management CAP Goal, though the details behind this estimate are not provided.<sup>43</sup> OMB has not released how each agency's spending on each commodity IT area examined in 2012 PortfolioStat has changed in the 4-5 years since launching consolidation projects.

Other behaviors that OMB has recommended, required, or examined include wider FAC P/PM training for acquisition officials involved in IT acquisitions, adoption of the Common Baseline's acquisition-related elements, and practices emphasized in USDS's acquisition training described in the Smarter IT Delivery CAP Goal.

Most years of PortfolioStat have included key performance indicators related to the acquisition approaches related to commodity IT. PortfolioStat included key performance indicators for some form of commodity IT related spending or savings in every year from 2012 - 2016.<sup>44</sup> Similar data was also used in GSA's Benchmarking Initiative, the Benchmark and Improve Mission-Support Operations CAP Goal, and FedStat.<sup>45</sup> Additionally, years 2013 - 2015 particularly focused on the mobile device and mobile service contracts category of commodity IT. Similarly, also see the IT Infrastructure Modernization policy paper for PortfolioStat KPIs related to spending on the data centers category of commodity IT.<sup>46</sup>

## Lessons Learned

It is unclear how widely adopted strategic sourcing, category management, commodity IT consolidation, and other strategies are by agencies. The Category Management CAP Goal reports that as of Q3 of FY 2016, zero percent of the “common spend” is “under government-wide management,” but it is difficult to determine how widely agencies are using other category management approaches.

For strategies which rely on agency adoption of recommended practices, OMB has not always been consistent on measuring and emphasizing such adoption. As metrics were not included that evaluate agency progress implementing the Common Baseline in 2015 or 2016 PortfolioStat, agencies may not be placing progress adopting its CIO and CXO<sup>47</sup> acquisition roles and responsibilities at the same level of priority as policies that are emphasized in PortfolioStat KPIs.

# Agency Observations and Findings

The Federal acquisition process has been a constant source of frustration for agency IT personnel. As OMB and GSA continue to work towards improving resources and available tools, agency CIOs continue to struggle with internal processes that do not align with modern technology management and have not used the available tools to a great extent. The acquisition process needs to evolve to serve agency IT needs rather than impede success specifically in today's constant threat environment.

## FINDING #1

### Despite Better Awareness, Existing Acquisition Flexibilities Are Underutilized by Agencies.

Although OMB and GSA have worked together on several informational campaigns to publicize the flexibilities and procedures available to support innovative approaches to IT acquisition, these are still underutilized by agencies. CIOs shared that their acquisition partners remain reluctant to explore these flexibilities. In addition to educating agencies, OMB has focused on initiatives dedicated to helping the government pool its common resources to achieve government-wide savings and efficiencies. Although these initiatives have led to new acquisition approaches, there has been reluctance on the part of agencies to widely adopt them. CIOs are often highly dependent on their partners in the acquisition community to understand what their options are, partly because of short tenures or lack of Federal procurement experience.

## FINDING #2

### Delays and Uncertainty Due to Procurement Process Length are Obstacles to Effective IT.

A number of CIOs stated that the procurement process takes too much time to keep up with rapidly changing cybersecurity needs and customer demands for technology. Moreover, CIOs must deal with uncertainty over how long the process will take, whether there will be protests, and what the results are likely to be. These types of delays can leave agencies without the ability to purchase network hardware until the protest is settled.

*I have a project that \*might\* get approved this month that is 18 months behind schedule before any work is done, before any protest. It is unacceptable for a BPA to take 2.5 years.*

- Agency CIO

The challenges of the Federal budgeting environment, such as the possibility of available funding expiring at the end of the year, can exacerbate such delays. This environment encourages agency Contracting Officers (COs) to be more risk-averse when selecting procurement strategies to limit the potential for an award protest. This effort to minimize the schedule and planning risks comes at the expense of other factors such as price and performance, and may diminish the effectiveness of the end product. These types of situations can lead to increased risk for agencies.

**FINDING #3****Acquisition Staff Face Challenges Evaluating Complex, Innovative Technology Without Greater Technology Expertise, However Efforts are Underway to Address Challenges.**

Multiple CIOs described challenges with relying on partners in the acquisition community who lack the background in modern IT necessary to evaluate vendors' ability to perform the services required by agencies. Recent efforts could help address this, such as: category managers for IT categories, continued growth of specialized IT acquisition cadres, and USDS and 18F's focus on hiring acquisition staff with more modern technology experience.

**FINDING #4****Restrictions to Accessing Vendors Create Unintentional Risks to Meeting IT Needs.**

According to CIOs, pressure to incorporate what they see as secondary factors into vendor selection criteria increases the risk that awardees may be unable to meet the government's requirements. These factors often arise from the agency's interest in demonstrating compliance with government-wide procurement rules and strategies, real or perceived. As such the

*Acquisitions are more about "fairness" than they are about best price [and that's an issue]*

- Agency CIO

*Acquisitions are about fairness and equality, but it should be about better buying power.*

- Agency CIO

may cause agencies to artificially exclude potential vendors with appropriate and cost effective solutions.

need to achieve small business and other set aside goals, demonstrate use of existing BPAs and Federal supply schedules, or use programs like FedRAMP<sup>48</sup>

One CIO described feeling required to use the agency's network operations support contract to help the agency achieve its small business set aside goals, but indicated the selected vendor proved unable to fully perform the work.

Other CIOs described pressure to first prove that vendors available through supply schedules, BPAs, or FedRAMP could not meet the government's requirements, rather than conducting a wide competition designed to reach the best solution. This built-in preference for existing vendors or other limited pool of potential vendors, while promoting certain goals, limits government access to the best vendor and introduces performance risk which can have other unintended schedule, security, and cost consequences.

**FINDING #5****Agency Funding Mechanisms Negatively Impact the Ability of the Federal Government to "Buy as an Enterprise."**

Finally, the appropriations process creates an additional burden on agencies attempting to leverage enterprise-wide buying as programs, offices or bureaus receive discrete appropriations, and appropriations law limits the ability to transfer funds to other organizations to facilitate consolidated enterprise purchases. As a result, agencies often have multiple contracts for the same products, such as Oracle database software, and paying different prices or with different configurations.

# Notes

1. M-16-20. Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops. 10/16/2015. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m\\_16\\_20.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_20.pdf) and M-16-12. Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing. 6/2/2016. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12\\_1.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf) and M-16-02. Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops. 10/6/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-02.pdf>
2. For more information about cybersecurity initiatives and technologies, see Policy Chapter E: Cybersecurity
3. FAC P/PM certification of entry-level, mid-level, or senior-level; Based on an analysis of the Projects data feed from IT Dashboard, Based on OMB's PortfolioStat 2016 methodology, includes all IT projects which completed after December 1, 2014 or are in progress, and a project lifecycle cost of greater than \$2 million. Original data source: <https://itdashboard.gov>
4. The small business set aside is mandated by statute. The FAR requires that agencies evaluate all potential requirements to determine if a small business is capable of performing the work. If two small businesses are capable of performing the work, then the acquisition generally must be set-aside for small businesses, in a process called the "Rule of Two." In some situations, this analysis can be taken care of quickly through market research, however, in many situations, an agency must conduct a Request For Information and evaluate potential small business sources. Agencies must set an annual goal and SBA monitors agencies' achievements against goals throughout the year. For more information on agency goals and contracts awards to various groups, see Small Business Administration. "Contracting". <https://www.sba.gov/contracting/contracting-officials/goaling>
5. Vendors have been filing more protests in recent years, though the underlying reasons for why are not fully known. Some of the potential factors include a depleted acquisition workforce that struggles with high turnover, low morale and difficulty in attracting new talented staff resulting in less than ideal acquisition, or increased pressure on companies to compete over fewer potential contracts as agencies face budget pressure brought on by sequestration and the use of continuing resolutions to fund the government. See Nextgov.com. "GSA Officials on Increased Bid Protests: 'This is how it is going to be'". 8/2/2016. <http://www.nextgov.com/technology-news/2016/08/gsa-officials-increased-bid-protests-how-its-going-be/130417/> and Congressional Research Service. "GAO Bid Protests: Trends and Analysis". 6/21/2015. <http://fas.org/sgp/crs/misc/R40227.pdf>
6. The U.S. Digital Service's new Digital IT Acquisition Professional Training Program (DITAP) seeks to train contracting officers on agile acquisition principles and how to leverage the FAR to support these activities. Challenge.gov. "Digital Service Contracting Professional Training and Development Program Challenge". <https://www.challenge.gov/challenge/digital-service-contracting-professional-training-and-development-program-challenge-2/>
7. M-01-15. Performance Goals and Management Initiatives for the FY 2002 Budget. 3/9/2001. <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/m01-15.pdf>
8. Federal Information Technology Acquisition Reform Act. 12/19/2014. Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Public Law No: 113-291: <https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148> For more information about FITARA, see Policy Chapter A: Management and Oversight of IT
9. General Services Administration. "Your Single Acquisition Source Reference Guide for GSA Technology". [http://www.gsa.gov/graphics/fas/ITS\\_COMPARISON\\_Matrix.pdf](http://www.gsa.gov/graphics/fas/ITS_COMPARISON_Matrix.pdf)
10. General Services Administration. "Blanket Purchase Agreements (BPAs)" <http://www.gsa.gov/portal/content/199353>
11. GAO-13-231. Acquisition Workforce: Federal Agencies Obtain Training to Meet Requirements, but Have Limited Insight into Costs and Benefits of Training Investment. 3/28/2013. <http://www.gao.gov/assets/660/653437.pdf>
12. Anne Rung, Former Administrator, Office of Federal Procurement Policy, OMB, has described the Salesforce BPA as representing the "best of the Administration's efforts to drive category management and increase innovation in the delivery of IT. By driving agencies to these BPAs, we will be able to leverage industry's agile talent while ensuring that we deliver the best value for the American taxpayer." General Services Administration. "GSA Awards BPA for Salesforce Integration and Support Services". <http://www.gsa.gov/portal/content/121238>
13. M-03-14. Reducing Cost and Improving Quality in Federal Purchases of Commercial Software. 2/25/2004. [https://www.whitehouse.gov/omb/memoranda\\_m03-14](https://www.whitehouse.gov/omb/memoranda_m03-14) and M-04-08. Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives. 2/25/2004. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-08.pdf> and M-05-25. SmartBUY Agreement with Oracle. 8/25/2005. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-25.pdf>
14. OMB Memorandum. Implementing Strategic Sourcing. 5/20/2005. [https://www.whitehouse.gov/sites/default/files/omb/procurement/comp\\_src/implementing\\_strategic\\_sourcing.pdf](https://www.whitehouse.gov/sites/default/files/omb/procurement/comp_src/implementing_strategic_sourcing.pdf)
15. M-13-02. Improving Acquisition through Strategic Sourcing. 12/5/2012. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-02\\_0.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-02_0.pdf)
16. OFPP Memorandum. Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings. 12/4/2014. <https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/simplifying-federal-procurement-to-improve-performance-drive-innovation-increase-savings.pdf>
17. U.S. Digital Service. "TechFAR Hub: Introduction". <https://techfarhub.cio.gov/>



18. OMB Memorandum. Acquisition Innovation Labs & Pilot for Digital Acquisition Innovation Lab. 3/9/2016. <https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/acquisition-innovation-labs-and-pilot-for-digital-acquisition-innovation-lab-memorandum.pdf>
19. General Services Administration. "Acquisition Gateway". <https://hallways.cap.gsa.gov/login-information>
20. OMB defined "commodity IT" as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (email, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions). M-11-29. Chief Information Officer Authorities. 8/8/2011. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf>
21. M-12-10. Implementing PortfolioStat. 3/30/2012. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10.pdf>
22. In the years since, however, GAO and others have questioned the validity of these savings, noting that only one agency addressed all the requirements issued by OMB and that GAO's review of agency materials concluded that the potential for savings may be even greater than reported. GAO-14-65. Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings. 11/6/2013. <http://www.gao.gov/assets/660/658883.pdf> and GAO-15-296. Information Technology: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked. 4/16/2015. <http://www.gao.gov/products/GAO-15-296>
23. M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. 3/27/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>
24. M-12-13. Fiscal Year 2014 Budget Guidance. 5/18/2012. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-13.pdf>
25. M-11-29. Chief Information Officer Authorities. 8/8/2011. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf>. and M-12-10. Implementing PortfolioStat. 3/30/2012. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10.pdf>
26. M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. 3/27/2013. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>
27. For example, by reducing the variety of desktop software installed government-wide, it would become easier to secure networks to ensure that software vulnerabilities were mitigated or removed. For more detailed information about efforts related to cybersecurity-specific acquisitions, see Policy Chapter E: Cybersecurity
28. M-16-02. Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops. 10/16/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-02.pdf>
29. M-16-12. Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing. 6/2/2016. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12\\_1.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf)
30. The Federal Acquisition Institute. "Digital IT Acquisition Professional Training (DITAP) with Joanie Newhart". [https://www.fai.gov/media\\_library/items/show/27](https://www.fai.gov/media_library/items/show/27)
31. OFPP Memorandum. Guidance for Specialized Information Technology Acquisition Cadres. 7/13/2011. <https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/guidance-for-specialized-acquisition-cadres.pdf>
32. OFPP Memorandum. Revisions to the Federal Acquisition Certification for Program and Project Managers. 12/16/2013. [http://www.fai.gov/drupal/sites/default/files/FAC%20PPM%20Policy\\_121613.pdf](http://www.fai.gov/drupal/sites/default/files/FAC%20PPM%20Policy_121613.pdf)
33. M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>
34. FAC-P/PM certification of entry-level, mid-level, or senior-level; Based on an analysis of the Projects data feed from IT Dashboard, September 21, 2016. Based on OMB's PortfolioStat 2016 methodology, includes all IT projects which completed after December 1, 2014 or are in progress, and a project lifecycle cost of greater than \$2 million. <https://itdashboard.gov/drupal/data/datafeeds?format=csv>
35. Vivek Kundra. 25-Point Implementation Plan to Reform Federal IT Management. 12/9/2010. <https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>
36. OFPP Memorandum. "Myth-Busting": Addressing Misconceptions to Improve Communication with Industry during the Acquisition Process. 2/2/2011. <https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/Myth-Busting.pdf> and OFPP Memorandum. "Myth-Busting 2": Addressing Misconceptions and Further Improving Communication During the Acquisition Process. 5/7/2012. <https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/myth-busting-2-addressing-misconceptions-and-further-improving-communication-during-the-acquisition-process.pdf>
37. U.S. Digital Service. "TechFAR Hub: Introduction". <https://techfarhub.cio.gov/>
38. Contracting Guidance to Support Modular Development. 6/14/2012. <https://www.whitehouse.gov/sites/default/files/omb/procurement/guidance/modular-approaches-for-information-technology.pdf>
39. Performance.gov. "Cross-Agency Priority Goal: Smarter IT Delivery". FY 2016 Q2 Update. <https://www.performance.gov/node/3403/view?view=public#progress-update>
40. Federal Information Technology Acquisition Reform Act. 12/19/2014. Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Public Law No: 113-29. <https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148>

41. OMB's FITARA implementation guidance also committed to revising the Federal Acquisition Regulation (FAR) to expand the definition of "information technology," broadening the CIO's purview to clearly include cloud computing services and significant IT operated by contractors related to the agency environment. M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>
42. Measurement: There are no PortfolioStat key performance indicators which evaluate the role of the CIO. However, the Smarter IT Delivery CAP Goal reports the "number of approved FITARA agency plans." OMB collects Common Baseline Self-Assessments and milestones updates from agencies in order to evaluate their progress implementing the responsibilities required by FITARA, but these have not been incorporated into PortfolioStat
43. Performance.gov "Cross-Agency Priority Goal: Category Management." FY 2016 Q3 Update. <https://www.performance.gov/node/3399/view?view=public#progress-update>
44. Although OFCIO removed its commodity IT areas data collection from the IDC, it restored data center related categories to its CPIC guidance and GSA's Benchmarking effort continued to collect spending data in help desks and other areas. It is unclear whether these varied data collection efforts used the same definitions and reporting instructions, so it may be difficult to accurately compare agency data from year to year
45. Performance.gov. "Cross-Agency Priority Goal: Benchmark and Improve Mission-Support Operations". Quarterly Progress Update. <https://www.performance.gov/node/3397/view?view=public>. For more information about government-wide Benchmarking initiative, see Policy Chapter A: Management and Oversight of IT
46. For more detailed information about efforts related to IT Infrastructure Modernization initiatives, see Policy Chapter B: IT Infrastructure Modernization
47. Senior Agency Officials such as Chief Acquisition Officer (CAO), Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO), Chief Information Officer (CIO), Chief Operating Officer (COO); defined in M-15-14. "Management and Oversight of Federal Information Technology " 6/10/2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>
48. For more information about FedRAMP, see Policy Chapter B: IT Infrastructure Modernization

# Executing on the Future of IT

The recommendations provided below are drawn primarily from the findings surfaced during interviews with Federal agency CIOs, conversations with the Office of the Federal Chief Information Officer (OFCIO), and research conducted using government data, reports, and testimony. These findings were analyzed to develop the following overall themes, which form the basis for the subsequent recommendations.

## Themes

### Adopt a Customer-focused Approach

Rather than a top-down model of pushing out new policies to agencies, OFCIO should embrace a model that incorporates agency viewpoints and feedback throughout the entire process, including implementation and oversight. This includes the creation of feedback loops, outreach mechanisms, and prioritizing workforce development.

### Focus on Execution

Many agencies reported significant challenges in meeting the shifting priorities and proliferation of new OMB policies and initiatives. By focusing on executing a more limited number of policies and initiatives, agencies and OMB can improve outcomes. For example, the FITARA Common Baseline is the first step in a much longer process to improve the management of government IT. Moving forward, OMB should work with agencies to not just fully implement the Common Baseline, but to set evolving standards for improving agencies' IT management, budgeting, acquisition, and workforce.

### Orient Around Outcomes

Government-wide policies and initiatives often set implementation targets that do not always align with agency operations and mission. This can lead to inconsistencies in data reported on key performance indicators. An outcome-oriented focus on measuring performance would drive higher quality reporting and could provide more insight into policy areas such as open government and open data.

### Act as an Enterprise

Agencies should leverage FITARA and other authorities to drive better cooperation between bureaus and the agency CIO, as well as between all senior agency officials. Similarly, OMB should coordinate between its management and budget offices, as well as other government-wide policy stakeholders, such as OSTP, to provide clear policy guidance and lines of communication to agencies. The end goal is to have an enterprise-wide view of IT policies and investments to drive better decisions and outcomes.

# Recommendations

## Recommendation #1

### Focusing on Customer Experience: Increasing CIO Engagement with Agency Programs

The role of the CIO has evolved well beyond that of merely providing basic IT services such as desktop computing and networking. Today's CIOs need to be true business partners focused on delivering impactful results to agency programs. As such, agencies and CIOs should apply best practices from the private sector and look to overall customer experience as the primary way to measure the success of IT, as opposed to more traditional operational measures such as cost savings or data center closures. This builds on work underway within the government at groups like USDS and 18F and will require CIOs to deepen their understanding of their customers and their needs.

Going forward, CIOs at all levels of an agency should work with program leaders and other senior agency officials to establish the appropriate customer-based metrics and measurement tools. Tools like customer stakeholder surveys, web analytics, and net promoter scores, can provide continuous insight into the customer experience. This parallels innovative private-sector management practices such as "lean startup" which

emphasize continuous testing of assumptions through customer value metrics and iterative delivery rather than assuming IT providers "know what is best."

To the extent possible, OMB should incorporate this shift in thinking into its policy formulation, oversight, and governance processes. For example, the IT Dashboard could gather data and feedback from customer stakeholders in addition to the CIO evaluation. Also, OMB should continue working with agencies to establish catalogs of customer-facing services and to evaluate effectiveness of agency technology in supporting those services.

#### Findings Addressed

- Agency Operations Do Not Always Align With OMB Reporting (A5)
- Changes in Messaging and Oversight Metrics Can Discourage Agencies From Taking Action (B2)
- Agencies Struggle to Apply Government-wide Policies to Their Environments (A6)

## Recommendation #2

### Standardize Data Collection: Establish Data Analysis and Research Team at OFCIO

By creating a new team dedicated to the coordination and oversight of all data collection efforts, OFCIO can substantially reduce inefficiencies and inaccuracies in its data collection processes. This group, the Data Analysis and Research Team (DART), would manage and standardize reporting processes, provide clear and consistent guidance to ensure data quality and consistency, and set strategic direction on improving data management.

Building upon the work started in OFCIO's Integrated Data Collection (IDC), the team should:

- Standardize around a set of tools and templates for the collection of agency data;
- Establish standard rules and regular data collection cycles, as well as common tools and terminology across OFCIO;
- Review potential data collections to ensure that new data is not duplicative of current efforts;
- Periodically review all OFCIO data collection elements to determine if they are still needed;
- Recommend the removal of a data element where there is no clear need for that data (e.g., not used for metrics or public reporting); and

- Establish regular communications with agencies to get feedback on data collection efforts from the agency perspective (e.g., alignment with internal agency reporting, burden of data collection).

Though DART, as proposed here, is focused solely on collection of IT-related data, their role could evolve to encompass data governance for other OMB Management Offices (e.g., OFPP, OFFM). The team could also coordinate efforts closely with OMB's Budget Review Division, leveraging both its analytical capabilities as well as its established information collection processes such as Budget Data Requests.

#### Findings Addressed

- Agency Operations Do Not Always Align With OMB Reporting (A5)
- Changes in Messaging and Oversight Metrics Can Discourage Agencies From Taking Action (B2)

## Recommendation #3

### Continue Shift Towards Agency (Customer) Driven Policy Development and Implementation

Numerous CIOs reported that many government-wide policy initiatives and reporting requirements did not always align with the mission objectives or business processes in each agency. Furthermore, the lack of a consistent approach to performance management coupled with the sheer number of policies taxes agency ability to keep pace and effectively meet OMB's objectives.

Recently, OMB has undertaken efforts to provide greater structure to how it formulates policies and initiatives, but the opportunity exists to expand upon this work in both implementation and oversight. Ultimately, the goal is to develop a customer-oriented approach that meets both agencies' needs and the priorities of the Administration. Potential activities include:

- ***Rationalization of Current Policies.*** Continue current review efforts of existing IT policies to reduce overlap and redundancy, retire outdated policies, and improve alignment with Administration priorities. Additionally, work should continue to establish a comprehensive policy library and to map policies to overarching Administration IT objectives.
- ***Development of Customer-Driven Process for Policy Formulation and Implementation.*** Policy objectives are often best achieved when there is buy-in from all stakeholders involved. OMB should work with agencies, industry, and Congress to surface new opportunities to address pressing needs across the broader IT community. Any new policies or initiatives should be rigorously reviewed to prevent conflicts and

duplication with existing policies, regulations, and laws. Additionally, OMB should expand upon its current efforts to solicit public comments and agency feedback on its draft policies.

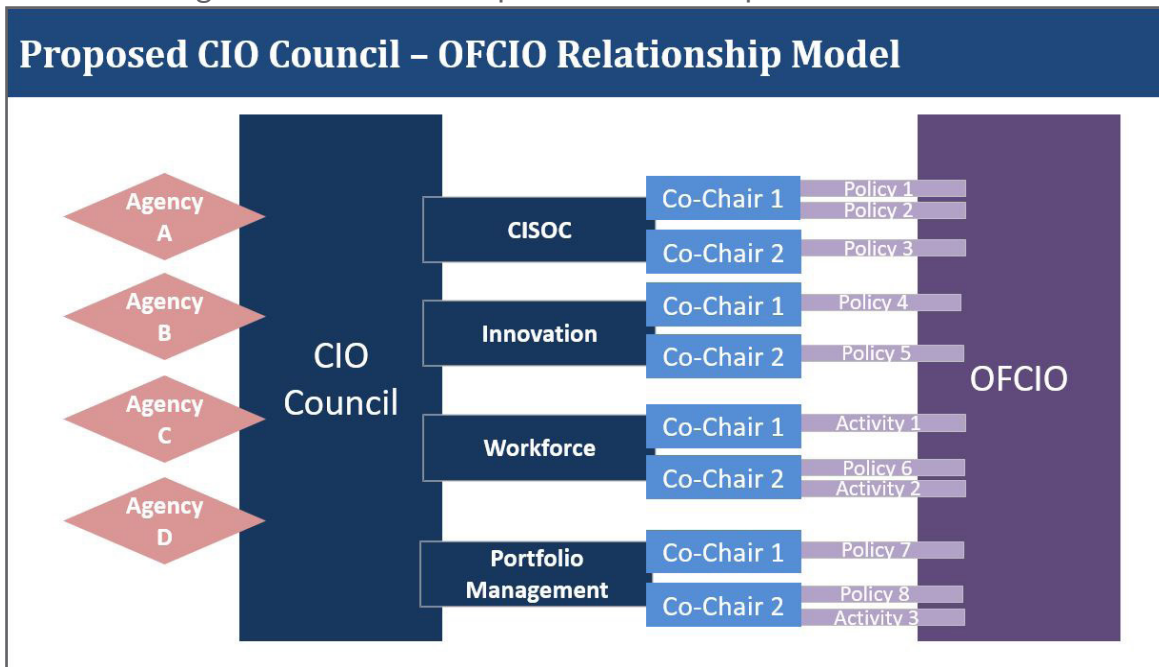
OFCIO can also build upon the reorientation of the CIO Council's committee structure, which is designed to better align agency CIOs and the Council's committees to OFCIO policy development process, to facilitate this change (see Figure). Using the CIO Council in such a manner can reduce confusion and increase impact and successful implementation of policies across the government. OFCIO should engage early and often with the CIO Council, leveraging their ability to solicit opinions from across the IT community to better inform actions.

- ***Establishment of Common Structure for Policies.*** The development (and usage) of a standard template can ensure policies always include common elements such as intended purpose, oversight mechanisms, linkages to existing policies, and reporting requirements. This can serve to help agencies reduce confusion and improve their ability to execute. Furthermore, both draft and finalized policies can be published in a structured format using a standard schema and open formats (e.g., JSON, XML) in addition to traditional PDF formats. This can improve the ability of agencies and oversight groups to monitor policy progress through web tools, data analytics, and other performance management tools.

**Recommendation #3**

**Continue Shift Towards Agency Driven Policy Development and Implementation (continued)**

Figure Rec-1: CIOC Proposed Relationship Model with OFCIO



This organizational chart provided by the Federal CIO Council (CIOC) represents the reorientation of the CIOC to better facilitate agency participation in the policymaking process.

- Linking management and budget decisions.** OMB’s internal management and budget functions should increase collaboration in the area of policy development and implementation. This increased collaboration could allow OMB to consider agency-specific budget concerns during policy development. In addition, OMB could consult with agencies directly. Drafting policies that address these concerns should drive better outcomes and result in fewer budget conflicts once the policies are implemented. Additionally, agency leadership will be able to make more effective business process and budget-related decisions if they have access to more information about policy discussions and implementation requirements.

**Findings Addressed**

- Agency Operations Do Not Always Align With OMB Reporting (A5)
- Agencies Struggle to Apply Government-wide Policies to Their Environments (A6)
- Current Approach to Modernizing IT Infrastructure Does not Necessarily Align with Agency Needs (B1)
- Changes in Messaging and Oversight Metrics Can Discourage Agencies from Taking Action (B2)
- Outcomes of Open Government and Open Data Efforts Can Be Hard to Gauge (C4)
- High Visibility in Cybersecurity Leads to Multiple Policy Messages, Metrics and Priorities (E4)

**Recommendation #4****Bolster OMB's Personnel to Focus on Customer Service Model**

As OMB takes a more customer-focused approach to working with agencies, it is essential to have staff (both employees and contractors) with the right blend of hands-on, agency-based and government-wide experience to support policy formulation, implementation, and oversight. This combination of experience can help facilitate better relationships between OMB and agencies while also ensuring that new policies and oversight practices are grounded in lessons learned and best practices from previous government-wide and agency efforts. OMB can increase its ability to find such staff by:

- Expanding upon current agency rotational programs (e.g., agency detailees, Presidential Innovation Fellows) to ensure the continuous exchange of talent between agencies and OMB;
- Revisiting its hiring and contractor selection processes to prioritize and more directly screen for agency experience and customer-focused mindset;
- Using the CIO Council committees as a proving ground for potential staff by offering the opportunity to work on committee policies or activities to interested government employees; and
- Recruiting and training more young policy professionals through expanding the use of the CIO Council's IT Job Shadow Days, internships, and other related efforts.

However, hiring and retaining a service-oriented workforce with the right mix of experience is only the first step. Going forward, OMB should also develop feedback loops to assess their current staff, the quality of support provided, and emerging needs. For example, agencies could be provided with regular customer satisfaction surveys to measure OFCIO desk officer performance against metrics such as timeliness of implementation support, clarity in communicating requirements, and effectiveness in working with agencies to achieve policy objectives.

**Findings Addressed**

- Agency Operations Do Not Always Align With OMB Reporting (A5)
- Agencies Struggle to Apply Government-wide Policies to Their Environments (A6)
- Current Approach to Modernizing IT Infrastructure Does not Necessarily Align with Agency Needs (B1)
- High Visibility in Cybersecurity Leads to Multiple Policy Messages, Metrics and Priorities (E4)
- Despite Better Awareness, Existing Acquisition Flexibilities Are Underutilized by Agencies (F1)
- Acquisition Staff Face Challenges Evaluating Complex, Innovative Technology Without Great Technology Expertise (F3)



## Recommendation #5

### FITARA 2.0: Facilitate Additional CXO Collaboration at Agencies and with OMB

CIOs are much more effective and capable of achieving Administration priorities and agency IT goals when they are fully engaged with their peers across the CXO suite. Yet despite recent FITARA implementation efforts, IT-related decisions at many agencies are still made without significant involvement from the CIO. Accordingly, OMB should work with agency leadership to increase CIO engagement with the acquisition community, the HR community, the financial community, and the programs themselves.

OMB took an important first step by instituting the FITARA Common Baseline. However, much more remains to be done to continue improving management of agency IT systems. First, OMB needs to ensure that agencies have met the requirements of the Common Baseline. Second, OMB should consider how to evaluate whether or not these changes in management structure and operations are improving outcomes. OMB should issue a follow up memorandum focused on evaluating oversight and execution. Specific recommended actions include:

- Making regular use of the President's Management Council (composed of Deputy Secretaries) to place proper attention on high priority government-wide initiatives, especially FITARA implementation;
- Rethink how PortfolioStat supports OMB's management agenda and key IT priorities. In particular, consider incorporating FITARA and customer service efforts more directly into the agenda. Additionally, consider including Deputy Secretaries and other CXO leaders at each agency to elevate the importance of IT issues (as was the case in the initial PortfolioStat sessions in FY 2012);
- Reviewing agency FITARA implementation plans to ensure that planned agency actions are sufficient to close lingering gaps between agency performance and full implementation of the Common Baseline;
- Aligning the FITARA Common Baseline with outcome-focused measures that are easily accessible, allowing Federal stakeholders to effectively evaluate the impact of FITARA across agencies;
- Exploring advocating for appropriations directly to CIO-managed offices or programs in select agency environments;

**Recommendation #5****FITARA 2.0: Facilitate Additional CXO Collaboration at Agencies and with OMB (continued)**

- Increase regular coordination at the principal level and the staff level to ensure consistent prioritization (and communication) across key OMB M-Team offices (e.g. OFCIO, OFPP, OPPM, OFFM) and other key stakeholders (e.g., OIRA, OSTP, GSA/OGP); and
- Continue to integrate the thinking behind the Technology Business Management (TBM) Council's Commission on IT Cost, Opportunity, Strategy, and Transparency (IT COST) frameworks and taxonomies and other related improvements into capital planning investment control data reporting to provide CIOs improved visibility into IT costs, benefits, and business value.

**Findings Addressed**

- Reaction to FITARA Implementation is Mixed (A2)
- The FITARA Common Baseline is Only the First Step in a Much Longer Process (A3)
- Successfully Improving Agency IT Management Functions Requires the Participation of All Members of the Executive Suite (A4)
- Infrastructure Only Gets Leadership Attention When IT Fails (B3)

## Recommendation #6

### Strengthening the Partnership Between IT and Procurement Communities

Building on recent joint efforts by OFPP and OFCIO (e.g., Category Management, Mythbusting), there are a number of opportunities to foster a productive working relationship between the procurement community, CIOs, and industry. Specific recommendations include:

- **Service-Level Agreements (SLAs).** Set clear expectations regarding procurement timelines and service levels to improve trust and reliability between procurement staff and IT. These SLAs could be measured via a scorecard-like approach for easy review and monitoring.
- **Feedback Systems.** Pilot ideas to gather feedback from the government and vendor community regarding the understandability, actionability, and results of past Requests for Information (RFIs) and Requests for Proposals (RFPs), to develop best practices.
- **Acquisition Centers of Excellence (COEs).** Designate (or have agencies nominate) acquisition offices which demonstrate leading performance in particular product/service areas, extending GSA's Category Management approach to build communities of experts throughout agencies. The COEs can also promote the sharing or reuse of contracts (e.g., GWACS) and the application of procurement practices that worked well in prior acquisitions.
- **Make Greater Use of Existing Certifications and Explore New Certifications.** Continue to standardize and streamline performance of procurement programs as well as project management activities and functions through the use of certifications such as the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM).
- **Increased Information Sharing.** Share RFI responses internally across government (as appropriate), increase visibility into the acquisition by making every RFI and RFP available (post-release) in a standardized, open format on a single website and allow all potential vendors easy access to any posted opportunity (regardless of set-aside status).

#### Findings Addressed

- Delays and Uncertainty Due to Procurement Process Length are Obstacles to Effective IT (F2)
- Restrictions to Accessing Vendors Create Unintentional Risks to Meeting IT Needs (F4)
- Government Procurement Processes Lack the Flexibility to Adapt to Evolving Cyber Threats (E1)

## Recommendation #7

### Clarify the Role of the CIO: Put the “Information” Back in CIO

The recent proliferation of IT-related “Chief” positions (e.g., Chief Digital Officers, Chief Innovation Officers, Chief Technology Officers) has made it difficult for many CIOs to understand their role and their place within the agency leadership team. Moreover, many CIOs reported spending the majority of their time focused on infrastructure management and operations rather than on mission-related efforts and the strategic use of information to drive decisions.

To address these issues, the role of the CIO and other IT-related positions should be further clarified both at the government-wide and agency levels. This can be accomplished as follows:

- Sharing best practices and proven models for OCIO organizational structures from across Federal agencies, other governments, and even the private sector. The Department of Transportation (DOT) provides one example, where the CTO works directly for the CIO with each having clearly defined roles.
- Development of a “model office” which can serve as a template for agencies to follow in structuring their own operations. The model office can lay out reporting relationships, responsibilities, and authorities of “Chief” positions involved in IT-related functions. Multiple models can be defined depending on the type of agency mission (i.e. definitions used in FedStat, such as Entitlement & Beneficiary Services or Economy & Infrastructure).

- Continuing to make greater use of commodity IT and shared services will enable CIOs to focus on more strategic, mission-oriented efforts. Ultimately this will allow CIOs to be the decision maker for the trade-offs between significant mission and operational priorities.

Finally, OMB should clearly outline the relationships between OFCIO and other IT-related offices and organizations within the Executive Office of the President and across the government (e.g., OSTP, USDS, OIRA, GSA) to provide a clear path for agencies to engage with the appropriate government-wide policy stakeholders.

#### Findings Addressed

- Authority and Role of CIOs Vary Between Agencies (A1)
- The Broad Range of Stakeholders Complicates Governance (C2)
- Agency CIOs Express Difficulty in Dedicating Resources to Open Government and Open Data Initiatives (C1)

**Recommendation #8****Establish a Standard Performance Management Framework**

The start of an Administration is an ideal time to establish an overarching strategy which identifies the key objectives and measurable goals across the government-wide management areas (e.g., human capital, financial management, procurement) that the incoming Administration would like to accomplish. As a part of a renewed President's Management Agenda, OMB should publish a multi-year vision that sets forth the strategic direction for Federal IT efforts. All new policies, performance indicators, and agency goals should then align to this broader framework. This strategy should be widely distributed across the government.

By starting with higher-level goals that remain relatively constant over time, OMB can keep agencies focused on its highest priorities even as individual actions and policy requirements may change to meet the current environment's needs. As OMB and agencies implement new policies, this performance framework can provide "line-of-sight" alignment between top objectives, lower-level goals, and the oversight or measurement process used to ensure continued progress towards those objectives. Whenever practicable, agencies should be encouraged to develop their IT business objectives around this framework.

As a part of maintaining consistent communication with agencies, OMB should maintain a list of performance gaps and measurement challenges, and plan short-term projects to address those gaps and challenges throughout the year. Finally, OMB should ensure there is an effective channel for agencies to provide feedback on their needs, policy challenges, and implementation concerns.

**Findings Addressed**

- Successfully Improving Agency IT Management Functions Requires the Participation of All Members of the Executive Suite (A4)
- Agency Operations Do Not Always Align with OMB Reporting (A5)
- Changes in Messaging and Oversight Metrics Can Discourage Agencies from Taking Action (B2)
- Infrastructure Only Gets Leadership Attention When It Fails (B3)
- Agency CIOs Expressed Difficulty in Dedicating Resources to Open Government and Open Data Initiatives (C1)
- Broad Range of Stakeholders Complicates Governance (C2)
- Cybersecurity Sprint Demonstrated a Highly-Effective Model of OMB-to-Agency Requirement Formulation and Implementation (E3)

**Recommendation #9****Focus on Knowledge Management: Collaborate, Coordinate, and Communicate**

CIOs emphasized that greater communication across the IT and management communities, including between agencies and OMB, could help spread successful solutions to common problems, lower confusion, and streamline agency oversight and policy compliance efforts. OMB should empower and designate the CIO Council as the official hub for government-wide IT knowledge management and communities of practice. These efforts could include:

- Increasing collaboration between OMB, the CIO Council, cross-agency governance organizations (e.g., USSM), other agencies, and other CXO councils to identify areas of interest for new communities of practice aligned with OMB and agency priorities. HUD's customer relationship coordinators provide a good example of how to hardwire program-and-IT collaboration at the agency level;
- Conduct "mythbusting" efforts on an ongoing basis to address misconceptions throughout IT management, particularly around hiring and acquisition flexibilities;
- Standardizing terms and definitions used in OMB reporting requirements, agency operations, and external communications to the extent practicable;

- Developing tools and processes to share best practices and lessons learned, and publicize communities of practice across IT disciplines;
- Increasing engagement with participants by using modern tools like mobile and social networking in addition to traditional listservs, web portals, and discussion forums; and
- Revamping a government-wide CIO Bootcamp effort to provide those new to IT leadership positions a common background of Federal IT management laws, regulations, policies, and practices.

**Findings Addressed**

- Existing Policies and Statutes Can Conflict with Open Data Efforts (C3)
- Despite Better Awareness, Existing Acquisition Flexibilities Are Underutilized by Agencies (F1)
- Acquisition Staff Face Challenges Evaluating Complex, Innovative Technology Without Great Technology Expertise (F3)
- New Tools Have the Potential to Accelerate Cost Savings and Infrastructure Rationalization (B5)
- The Federal IT Workforce is Not Adequately Equipped to Address Challenges in Cybersecurity (E2)

## Recommendation #10

### Establish Central Funding for Shared Services and Infrastructure Modernization

As heard throughout the interviews, requirements for upfront capital planning and investment, complex rules for transferring funding between agencies, and a lack of attention from agency leadership make it challenging for agencies to modernize IT infrastructure and move to shared services. To address these issues, OMB should continue its recent work with Congress to establish a centralized source of IT funding. This fund can:

- Provide multi-year funds, outside of traditional agency budgets, specifically prioritized for infrastructure modernization and shared services adoption;
- Establish a standard approach and sufficient authorities for transferring funds between and to agencies; and
- Provide centralized expertise and oversight for infrastructure modernization efforts to drive consistency across the government.

This fund can be centrally managed by OMB or a designated agency and should be tightly coordinated with current and emerging government-wide initiatives to modernize shared services and IT infrastructure, such as Unified Shared Services Management (USSM) and the Data Center Optimization Initiative (DCOI). A key precursor to this effort is providing an authoritative definition for the primary concepts of IT modernization and shared services. A central management office would be well-positioned to provide these definitions.

#### Findings Addressed

- Transfer of Funds Between Agencies Presents Challenges (D2)
- Agency Funding Mechanisms Negatively Impact the Ability of the Federal Government to “Buy as an Enterprise” (F5)

**Recommendation #11****Providing Common Cybersecurity Resources for Agencies**

OMB has made significant progress in addressing longstanding vulnerabilities in agency IT infrastructure to improve the government's overall cybersecurity posture. However, opportunities remain for additional improvement:

- **Awareness & Education.** Promoting cybersecurity-supportive behaviors and norms throughout the Federal workforce through increased training, awareness, education, and outreach;
- **Cybersecurity Workforce.** Experimenting with new, and scaling successful hiring and retention strategies, incentives, and process reforms for cybersecurity talent;
- **Sprint-Based Approach to Policy Implementation.** Scaling the lessons learned from the Cybersecurity Sprint and applying them to other key agency implementation gaps;
- **Centralized IT Infrastructure.** Extend efforts to establish a shared government-wide, modern, secure infrastructure which all agencies can adopt. By focusing cybersecurity expertise and technology on building this shared infrastructure, OMB can allow CIOs to focus on customer and mission-focused IT activities. This approach can be of particular benefit to organizations with limited infrastructure capabilities, such as small agencies (see Recommendation #12); and

- **Publicly-Available Dashboards Illustrating Potential Areas of Improvement.** Currently, agency performance on implementing safeguards is published in the annual FISMA Report and quarterly Cybersecurity CAP Goal in PDF formats. OMB started to release Excel workbooks to supplement this reporting, but it should take the next step to strengthen oversight by making an interactive, sortable dashboard modeled on Project Open Data Dashboard to make it as easy as possible to identify each agency's key areas for improvement in a quantitative, rigorous format.

**Findings Addressed**

- The Federal IT Workforce is Not Adequately Equipped to Address Challenges in Cybersecurity (E2)
- Cybersecurity Sprint Demonstrated a Highly-Effective Model of OMB-to-Agency Requirement Formulation and Implementation (E3)



**Recommendation #12****Establish Centralized IT Capability for Small Agencies**

Significant economies of scale can be achieved through use of shared services. This is particularly true for small agencies, which have limited internal resources and often lack specialized IT skills in critical areas such as cybersecurity and digital services. By establishing a centralized IT capability for small agencies, significant cost savings can be achieved. Additionally, centralizing IT can improve the speed of delivery, reliability, and security of IT services at small agencies.

This capability could either be housed in an existing agency office with shared services management expertise (e.g., USSM), or be managed by designating one or more shared service providers as managing partners. At a minimum, the focus should be on basic IT services (e.g., network, hosting, email) but could be expanded to include more complex services such as administrative and back office functions (e.g., HR, FM). Additionally, this approach could serve as a model for larger Federal agencies, providing an opportunity to first pilot service offerings and operating models on a small-scale before introducing them government-wide.

**Findings Addressed**

- Agencies Struggle to Apply Government-wide Policies to Their Environments (A6)
- Current Approach to Modernizing IT Infrastructure Does Not Necessarily Align with Agency Needs (B1)
- Transfer of Funds Between Agencies Presents Challenges (D1)
- The Federal IT Workforce is Not Adequately Equipped to Address Challenges in Cybersecurity (E2)

**Recommendation #13****Expand Engagement With Audit and Oversight Groups to Improve Data Availability**

While OMB, GAO, and the Inspectors General (IGs) can at times appear to be working towards different objectives, ultimately they share the same goal: an efficient and effective government that delivers for its citizens. As such, OMB should look to partner, where appropriate, with these groups to both improve data quality as well as to strengthen oversight of agency IT management. GAO and IGs bring specialized audit skills, methodologies and tools. Moreover, GAO and IGs can serve to focus agency attention on specific issues, in part because their findings are published publicly and can be accompanied by press coverage and Congressional scrutiny. OMB of course will need to preserve a level of independence, but can look to partner with GAO and IGs as follows:

**Targeted Audits & Oversight Efforts.** OMB should more directly engage with GAO and the IGs around specific policies and priorities and work with them to identify and remediate potential concerns raised in audits, as appropriate. Additionally, OMB should also work with these groups to identify opportunities to increase the transparency and availability of agency data through public-facing tools like the Federal IT Dashboard.

**Measurable Goals and Policy Requirements.** OMB should take steps to make it easier for other oversight groups to engage with agencies on IT management topics. For example, OMB should also write agency reporting requirements using consistent, structured data reporting to make it easier for GAO and the agency IG community to conduct audits by comparing reported data against agency records.

**Findings Addressed**

- Agency Operations Do Not Always Align with OMB Reporting (A5)
- Infrastructure Only Gets Leadership Attention When It Fails (B3)
- Outcomes of Open Government and Open Data Efforts Can Be Hard to Gauge (C4)

# SOFIT Findings Index

Policy Chapter	ID	Findings
Management and Oversight of IT	A1	Authority and role of CIOs vary between agencies
Management and Oversight of IT	A2	Reaction to implementation of FITARA is mixed
Management and Oversight of IT	A3	The FITARA Common Baseline is only the first step in a much longer process
Management and Oversight of IT	A4	Successfully improving agency IT Management functions requires the participation of all members of the Executive suite
Management and Oversight of IT	A5	Agency operations do not always align with OMB reporting
Management and Oversight of IT	A6	Agencies struggle to apply government-wide policies to their environments
IT Infrastructure Modernization	B1	Current Approach to Modernizing IT Infrastructure Does not Necessarily Align with Agency Needs
IT Infrastructure Modernization	B2	Changes in Messaging and Oversight Metrics Can Discourage Agencies from Taking Action
IT Infrastructure Modernization	B3	Infrastructure Only Gets Leadership Attention When It Fails
IT Infrastructure Modernization	B4	FedRAMP Has Not Accelerated Safe Adoption of New Cloud Services
IT Infrastructure Modernization	B5	New tools have the potential to accelerate cost savings and infrastructure rationalization
Open Government and Open Data	C1	Agency CIOs Expressed Difficulty in Dedicating Resources to Open Government and Open Data Initiatives
Open Government and Open Data	C2	Broad Range of Stakeholders Complicates Governance
Open Government and Open Data	C3	Existing Policies and Statutes Can Conflict with Open Data Efforts
Open Government and Open Data	C4	Outcomes of Open Government and Open Data Efforts Can Be Hard to Gauge
Federal Shared Services	D1	Transfer of Funds Between Agencies Present Challenges
Federal Shared Services	D2	Providing Shared Services Increases Agency Risk and Burden and Can Lead to Lower Quality of Service
Cybersecurity	E1	Government Procurement Processes Lack the Flexibility to Adapt to Evolving Cyber Threats
Cybersecurity	E2	The Federal IT Workforce is Not Adequately Equipped to Address Challenges in Cybersecurity
Cybersecurity	E3	Cybersecurity Sprint Demonstrated a Highly-Effective Model of OMB-to-Agency Requirement Formulation and Implementation
Cybersecurity	E4	High Visibility in Cybersecurity Leads to Multiple Policy Messages, Metrics, and Priorities
IT Acquisition and Contracts Management	F1	Despite Better Awareness, Existing Acquisition Flexibilities Are Underutilized by Agencies
IT Acquisition and Contracts Management	F2	Delays and Uncertainty Due to Procurement Process Length are Obstacles to Effective IT
IT Acquisition and Contracts Management	F3	Acquisition Staff Face Challenges Evaluating Complex, Innovative Technology Without Great Technology Expertise
IT Acquisition and Contracts Management	F4	Restrictions to Accessing Vendors Create Unintentional Risks to Meeting IT Needs
IT Acquisition and Contracts Management	F5	Agency Funding Mechanisms Negatively Impact the ability of the Federal government to "Buy as an Enterprise"