

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“Many Federal departments and agencies rely on aging computer systems and networks running on outdated hardware and infrastructure that are expensive to operate and difficult to defend against modern cyber threats.”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 Scott¹

Summary

 Cost	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.” ²
 Accountability	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.
 Risk	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.
 Policy	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)³ and government-wide spending in this area continues to increase at a steady pace.⁴ 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.⁵ 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)⁶

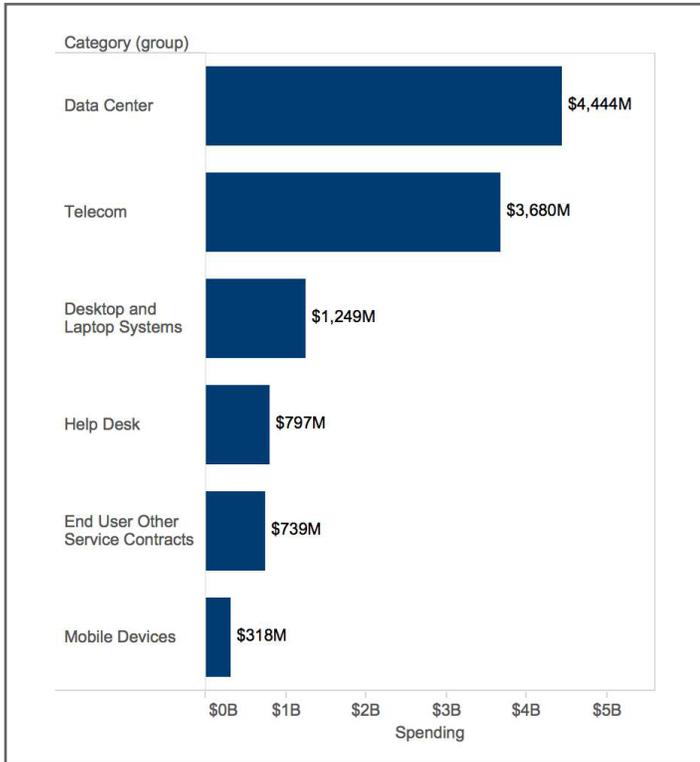
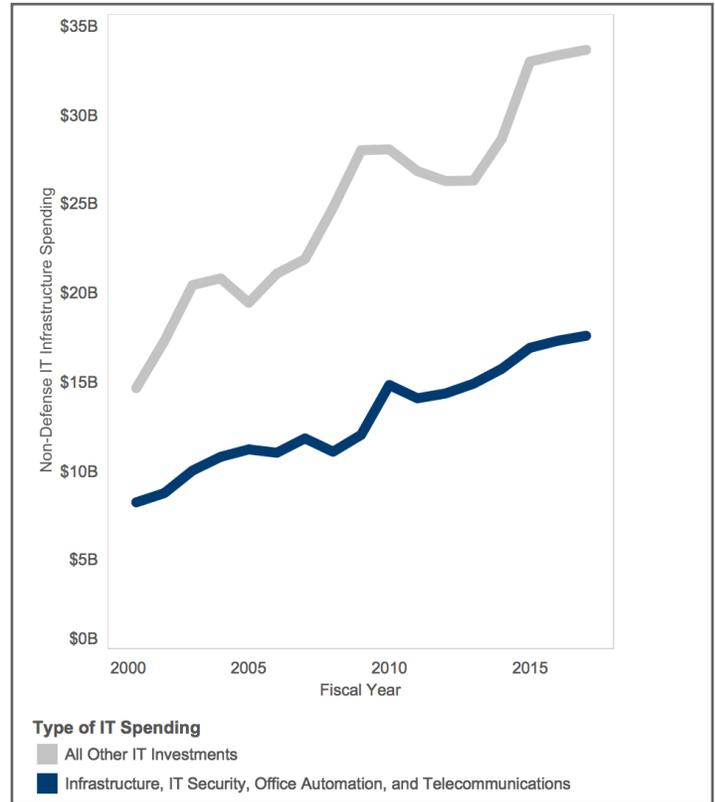


Figure B2: IT Infrastructure and all other IT Spending Over Time (Excluding DOD)⁷



Government spending on data centers represents a significant portion of the money spent on Federal IT infrastructure.⁸ 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.⁹ 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.¹⁰

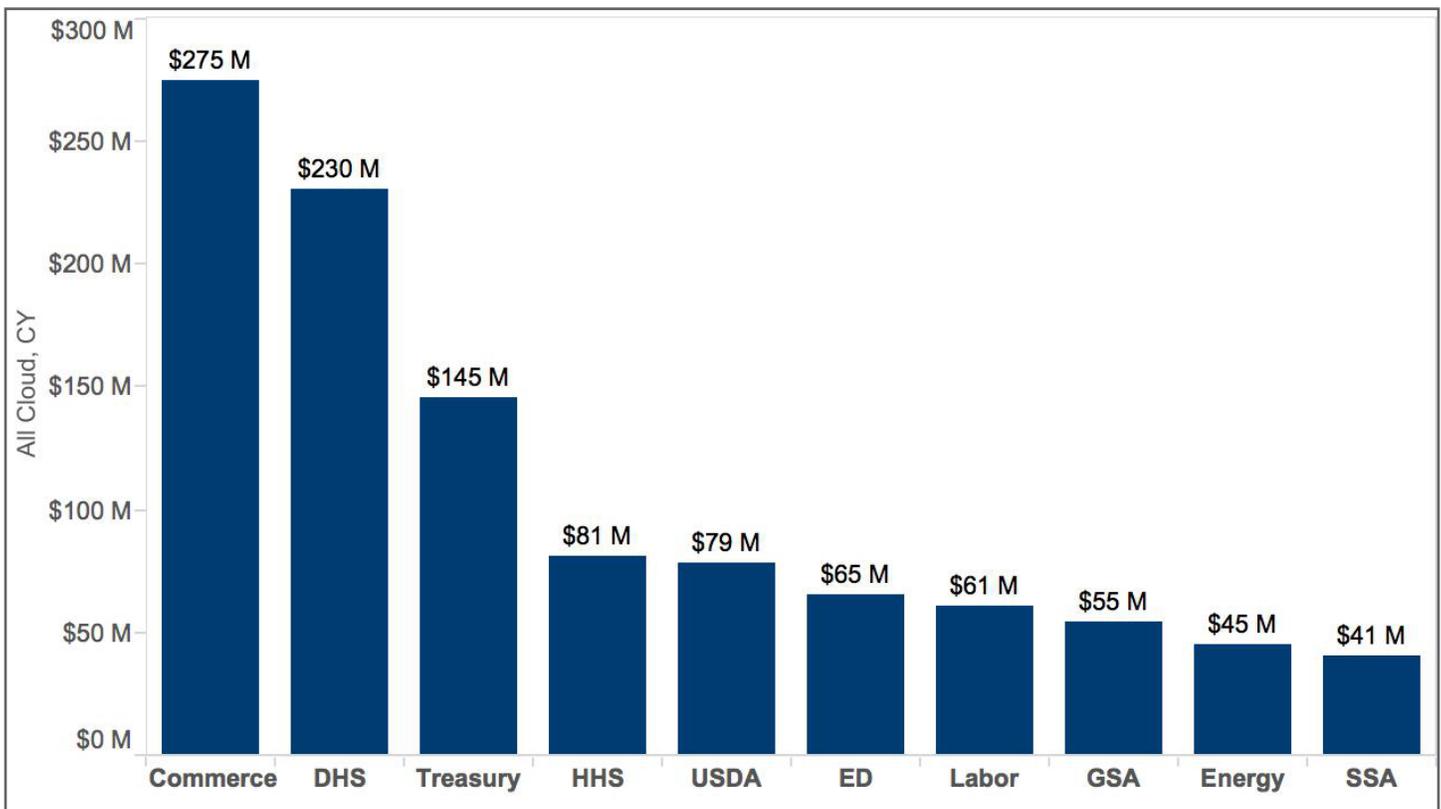
In recent years OMB pushed to move agencies to the cloud. With Federal agencies projected to spend over \$2 billion on cloud computing services out of a total of \$80 billion in IT spending in FY 2016, there are clearly more opportunities to adopt cloud-based solutions.¹¹ However, while agencies see 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)¹² 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 Spending¹³ (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.¹⁴ 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.¹⁵

IT Infrastructure Optimization Line of Business	
Key Strengths	<ul style="list-style-type: none"> Established government-wide assistance for agency migrations of IT infrastructure Defined common performance standards and metrics
Key Challenges	<ul style="list-style-type: none"> Participation was optional, so impact was limited to agencies already proactively investing in infrastructure improvements 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
Policy Impact	<ul style="list-style-type: none"> Established a baseline discussion of infrastructure services and performance models Early effort to capture consistent, standardized metrics relating to common infrastructure categories

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 Architecture¹⁶ 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 2011,¹⁷ other foundational policy documents are largely silent on the use of enterprise architecture.¹⁸

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

2010 – 2015

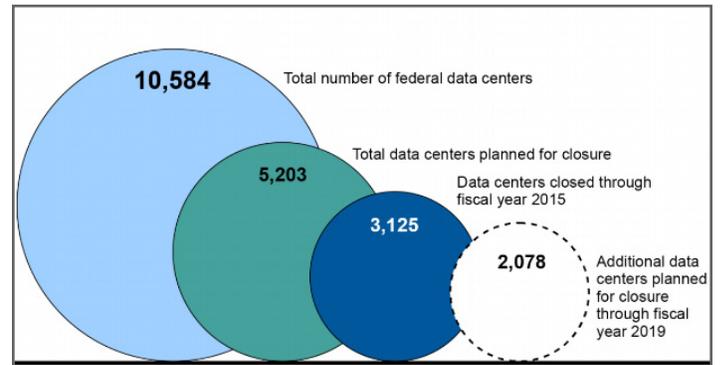
Federal Data Center Consolidation Initiative (FDCCI)

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.¹⁹ 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 2015.²⁰

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)²¹



Under the FDCCI, agencies were required to:

- Submit an inventory of each agency's data centers
- Develop a plan to consolidate data centers
- 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"> Consolidation targets provided agencies a clearly defined objective Provided executive level attention on core IT infrastructure issues
Key Challenges	<ul style="list-style-type: none"> Debates over what to “count” as a data center hampered efforts to establish a meaningful baseline to measure progress The focus on reducing the number of data centers distracted from the broader objectives of infrastructure modernization Agencies do not track their spending on individual data center facilities, hampering efforts to project cost savings based on consolidation activities 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 Shifting metrics from simply counting closures to evaluating various optimization metrics in PortfolioStat²² led to confusion amongst many agencies
Policy Impact	<ul style="list-style-type: none"> Successful in achieving agency cost savings due to consolidation or optimization of their data centers over the life of the effort Agency CIOs looking to move to alternative IT infrastructure providers used FDCCI to justify investment in migration to new providers (e.g., cloud alternatives) 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

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.²³ 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.²⁴ 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.”²⁵

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.²⁶ 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"> • Provided CIOs with the necessary “top cover” to push for more cloud adoption • Change in mindset began to shift CIOs’ thinking away from traditional servers and mainframes to cloud-based services in a more systematic way
Key Challenges	<ul style="list-style-type: none"> • Requirements were loosely defined - the requirement to shift three “must move” services did not provide sufficient guidance for how agencies might identify appropriate targets • 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 • OMB continued to accept budget requests for agency expansion of non-cloud systems with no explanation or negative consequences, despite the “Cloud First” principle
Policy Impact	<ul style="list-style-type: none"> • Agencies chose to prioritize cloud migrations for low impact services in order to meet OMB’s “three services” target • Agency CIOs faulted the policy for not providing sufficient follow-through to truly change their business practices

2011

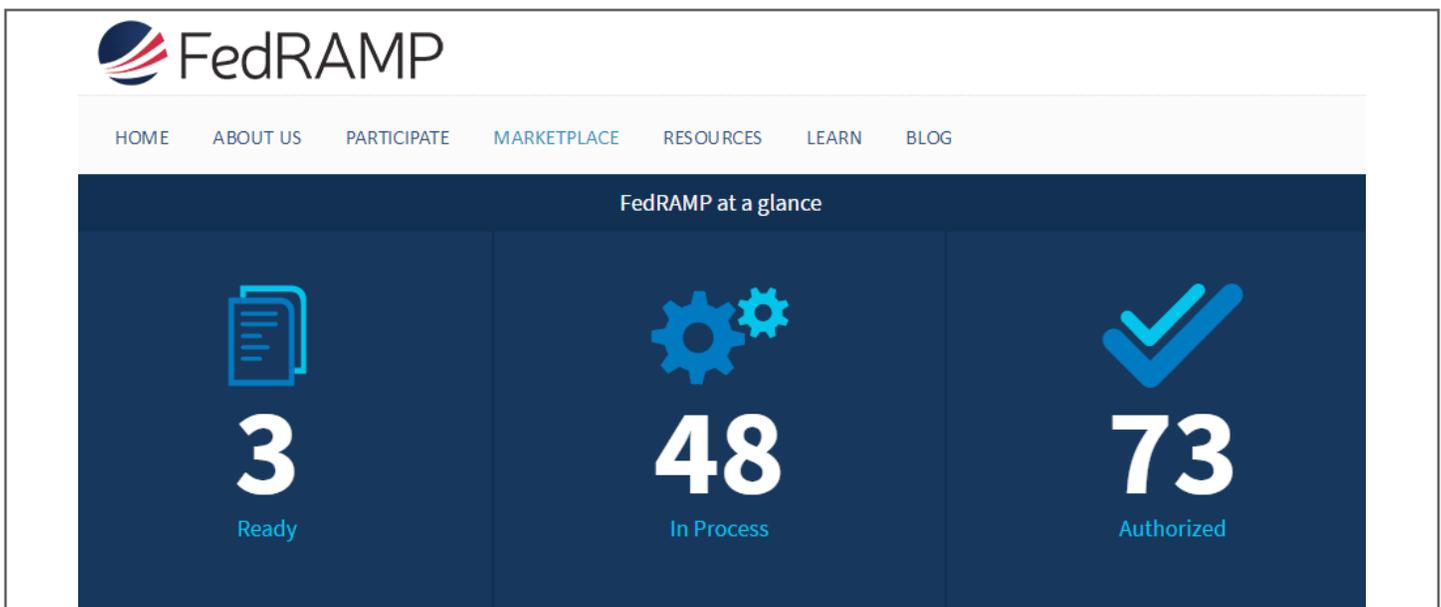
Federal Risk and Authorization Management Program (FedRAMP)

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.²⁷ FedRAMP was set up to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.²⁸ 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"> • Vision of providing a one-stop shop for identifying approved cloud providers gave agencies a framework for safely adopting cloud services • Unified risk management approach provides a common set of security standards and controls for cloud services
Key Challenges	<ul style="list-style-type: none"> • The average approval timeline is nearly 18 months, resulting in significant delays in adopting services • Agency CIOs must still conduct their own internal risk evaluations even on FedRAMP-approved services before adoption, negating some of the potential gains • Unclear path for maintaining approvals as technical and data management characteristics of approved providers change over time • Some agencies are unsure whether they may use cloud services which are not yet FedRAMP-approved
Policy Impact	<ul style="list-style-type: none"> • FedRAMP has successfully created a common security baseline for cloud-based services at the low, medium, and high levels • The program has currently [11/2/2016] authorized 77 cloud-based services, with another 49 "in process" • \$70 million per year in government-wide cost avoidance through the reuse of FedRAMP authorizations since the program's launch³⁰

IT Infrastructure Modernization

Figure B5: Example View of the FedRAMP Dashboard²⁹



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.³¹

In August 2016, in an attempt to further clarify the data center objectives of FITARA, OMB launched the Data Center Optimization Initiative (DCOI).³² 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.
- Continuing efforts to close data centers and report cost savings.

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

Agency Perspective

The Department of Energy’s (DOE) approach is to work with OMB to examine the six different types of data centers (e.g., 1st tier data centers, server closets) within the agency, and then focusing in on the types of data centers the agency can best optimize. For example, DOE runs a small number of headquarters-level data centers that could be consolidated with other data centers. However, specialized data centers such as those containing supercomputers are treated differently. DOE has data processing facilities that need to handle at least 400Gbps of data throughput – something that can’t be done over the Internet or over any great physical distance. This makes facilities housing those supercomputers less attractive candidates for consolidation.

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 have 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.³³ 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).³⁴

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.³⁵ 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 2012.³⁶

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

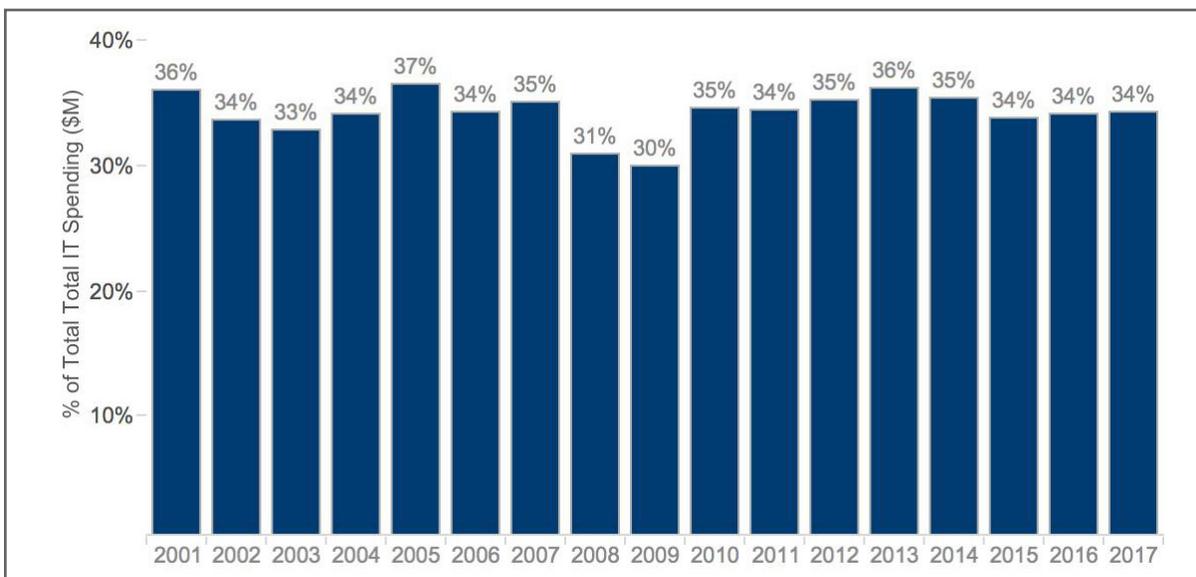
Notably, while savings of \$8.1 billion have been reported through data center consolidation, PortfolioStat, and other reform initiatives, efforts to measure cost savings have been challenged both by the lack of consistent baseline data as well as changes in definitions over time. As GAO summed it up, “Inconsistencies in OMB and agencies’ reporting make it difficult to reliably measure progress in achieving PortfolioStat savings.”³⁷ 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), 2001-2017³⁸



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 2005,³⁹ 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
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
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
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
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
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
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. 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
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
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