Congressional Research Service
Informing the legislative debate since 1914

Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Eric A. Fischer
Senior Specialist in Science and Technology

January 22, 2014

Congressional Research Service
7-5700
www.crs.gov
R42887

CRS REPORT
Prepared for Members and
Committees of Congress

c11173008

Summary

Cloud computing is a new name for an old concept: the delivery of computing services from a remote location, analogous to the way electricity, water, and other utilities are provided to most customers. Cloud computing services are delivered through a network, usually the Internet. Some cloud services are adaptations of familiar applications, such as e-mail and word processing. Others are new applications that never existed as a local application, such as online maps and social networks.

Since 2009, the federal government has been shifting its data storage needs to cloud-based services and away from agency-owned data centers. This shift is intended to reduce the total investment by the federal government in information technology (IT) (data centers), as well as realize other stated advantages of cloud adoption: efficiency, accessibility, collaboration, rapidity of innovation, reliability, and security.

In December 2010, the U.S. Chief Information Officer (CIO) released "A 25-Point Implementation Plan to Reform Federal IT Management" as part of a comprehensive effort to increase the operational efficiency of federal technology assets. One element of the 25-Point Plan is for agencies to shift to a "Cloud First" policy, which is being implemented through the Federal Cloud Computing Strategy. The Cloud First policy means that federal agencies must (1) implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists; and (2) begin reevaluating and modifying their individual IT budget strategies to include cloud computing.

However, there are challenges facing agencies as they make this shift. For example, some agency CIOs have stated that in spite of the stated security advantages of cloud computing, they are, in fact, concerned about moving their data from their data centers, which they manage and control, to outsourced cloud services. This and other concerns must be addressed to build an agency culture that trusts the cloud.

Congress has a number of means to monitor the status of the Federal Cloud Computing Initiative (FCCI). Individual committees may wish to monitor agencies under their jurisdiction by holding hearings; requesting review of an agency's status through the agency itself or a GAO study; and/or assessing an agency's progress and projected goals against the stated goals of the FCCI.

c11173008

Contents

Introduction 1
What Is Cloud Computing? 1
Characteristics of Cloud Computing 2
Deployment Models 2
Public 3
Private 3
Community 3
Hybrid 3
Deployment Model Comparison and Use by Federal Agencies 4
Service Models 4
Software as a Service (SaaS) 4
Platform as a Service (PaaS) 5
Infrastructure as a Service (IaaS) 5
Service Model Comparison 5
Service Model Use by Federal Agencies 5
Considerations in Cloud Computing Adoption 5
Cost 6
Energy Efficiency 8
Availability 9
Agility 9
Security 10
Reliability 11
Privacy 12
Trends in Total Federal Investment in Information Technology 13
Federal Planning and Activity 14
25-Point Implementation Plan to Reform Federal IT Management 15
Federal Cloud Computing Strategy 15
Federal Cloud Computing Strategy: Supporting and Complementary Initiatives, Programs, and Committees 17
Agency Cloud Adoption: Status 19
July 2012 Government Accountability Office Report 19
October 2012 InformationWeek Survey 20
Service Model Adoption 20
Deployment Model Adoption 21
Agency Cloud Adoption: Challenges 21
Security 21
Portability and Interoperability 22
Knowledge and Expertise 22
Certification and Accreditation 22
Implementation Guidance 22
Agency Cloud Adoption: Drivers 23
Budget Concerns 23
Data Center Consolidation 23
Activity in the 113th Congress 24

c11173008

Legislation 24
Hearings 26
Implementation of the Federal Cloud Computing Initiative: Options for Oversight by Congress 30
Hearings 30
Review of Agency Cloud Computing Plans and Implementation Assessments 31
Review of External Status Reports 31

Figures

Figure 1. Trends in Total Federal Investment in Information Technology 14

Tables

Table 1. Agency CIO Responsibilities Under the 25-Point Plan 16

Contacts

Author Contact Information 31

c11173008

Introduction

Since 2009, the federal government has been shifting its data storage needs to cloud-based services and away from agency-owned, in-house data centers. This shift is intended to reduce the total investment by the federal government in information technology (IT) (data centers), as well as realize other stated advantages of cloud adoption: efficiency, accessibility, collaboration, rapidity of innovation, reliability, and security. However, there are challenges facing agencies as they make this shift. For example, some agency chief information officers (CIOs) have stated that in spite of the stated security advantages of cloud computing, they are, in fact, concerned about moving their data from their data centers, which they manage and control, to outsourced cloud services. This and other concerns must be addressed to build an agency culture that trusts the cloud.

This report explains what cloud computing is, including cloud deployment models and service models, discusses issues that should be considered when adopting cloud services, and presents the federal government's planning for IT reform. It also provides information on assessments that have been conducted on agency cloud adoption and discusses both the challenges and drivers of cloud adoption. Finally, the report provides possible mechanisms for Congress to monitor agencies as they implement cloud computing.

What Is Cloud Computing?

Cloud computing is a new name for an old concept: the delivery of computing services from a remote location, analogous to the way electricity, water, and other utilities are provided to most customers.[1] Cloud computing services are delivered through a network, usually the Internet. Utilities are also delivered through networks, whether the electric grid, water delivery systems, or other distribution infrastructure. In some ways, cloud computing is reminiscent of computing before the advent of the personal computer, where users shared the power of a central mainframe computer through video terminals or other devices. Cloud computing, however, is much more powerful and flexible, and information technology advances may permit the approach to become ubiquitous.

Some cloud services are adaptations of familiar applications, such as e-mail and word processing. Others are new applications that never existed as a local application, such as online maps and social networks. It is clearly different from local computing in which local machines perform most tasks and store the relevant data.

As cloud computing has developed, specific descriptions of what it is and what it is not have been varied and sometimes nebulous. Such ambiguity can create uncertainties that may impede innovation and adoption. The National Institute of Standards and Technology (NIST) has tried to clear up that ambiguity by devising the following definition:

[1] For a discussion of utility and other models of providing computing services, see M. A Rappa, "The Utility Business Model and the Future of Computing Services," *IBM Systems Journal* 43, no. 1 (2004): 32–42, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5386779.

c11173008

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[2]

The first sentence of the definition basically states that cloud computing is a way of providing convenient, flexible access to a broad range of computing resources over a network. The characteristics and models referred to in the second sentence provide the specificity necessary to clarify what cloud computing is and is not.

Characteristics of Cloud Computing[3]

Cloud computing differs from local computing in many ways. NIST has identified five characteristics in particular:

- *On-demand self-service:* A user can directly access the needed computing capabilities from the source, no matter what specific resource is required. This can be considered somewhat analogous to a homeowner being able to change television channels or radio stations at will with a remote control.
- *Broad network access:* A user is not tied to one location but can access resources from anywhere the network (typically the Internet) is available.
- *Resource pooling:* Many users share the same overall set of resources from a provider, using what they need, without having to concern themselves with where those resources originate. An analogy with respect to the electric grid is that homeowners do not need to know what specific power plants generated the electricity they are using.
- *Rapid elasticity:* Users can quickly increase or decrease their use of a computing resource in response to their immediate needs. An analogy would be homeowners using as little or as much electricity at any one time as they need, within the capacity of their connections to the grid.
- *Measured service:* The amount of usage by a customer is monitored by the provider and can be used for billing or other purposes. An analogy is metering the use of electricity, water, and other utilities.

Deployment Models[4]

NIST has identified four standard models, or types, of cloud computing that can be implemented to satisfy varying needs of users or providers. Those models—public, private, community, and hybrid—vary in where the hardware is located, what entity is responsible for maintaining the system, and who can use system resources.

---

[2] The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf ("The NIST Definition of Cloud Computing").

[3] The NIST Definition of Cloud Computing.

[4] The NIST Definition of Cloud Computing.

c11173008

Public

In *public cloud* (sometimes called an *external cloud*) computing, a provider supplies one or more cloud-computing services to a large group of independent customers, such as the general public. Customers use the service over the Internet through web browsers or other software applications. Providers usually sell those services on a metered basis, an approach that is sometimes called "utility computing." Some common examples of services using a public cloud model include Internet backup and file synchronization[5] and web-based media services.[6] Public clouds may have price and flexibility advantages over other deployment models, but security and other concerns could restrict federal use.

Private

A *private cloud* (sometimes called an *internal cloud*) works like public cloud computing, but on a private network controlled and used by a single organization. Private clouds may provide services that are similar to those provided by public cloud providers, but with fewer purported risks. Potential disadvantages include cost and logistical challenges associated with purchasing and managing the required hardware and software. Private clouds can provide internal services such as data storage as well as external services to the public or other users.

Community

A *community cloud* allows a group of organizations with similar requirements to share infrastructure, thereby potentially realizing more of the benefits of public cloud computing than is possible with a purely private cloud. Because a community cloud has a much smaller user base than a public cloud, it may be more expensive to establish and operate, but it may also allow for more customization to meet the users' needs. It may also meet user-specific security and other requirements more effectively than a public cloud.

Hybrid

A hybrid cloud uses a combination of internal (private or community) and external (public) providers. For example, a user could employ a private or community cloud to provide applications and store current data but use a public cloud for archiving data. The flexibility of this deployment model may make it particularly attractive to many organizations.

[5] Examples include Dropbox (https://www.dropbox.com) and Microsoft's Skydrive (http://windows.microsoft.com/en-US/skydrive/home), which permit customers to share documents and other files across several devices; and Apple's iCloud (http://www.apple.com/icloud) and Google Drive (https://drive.google.com), which include file-sharing but also provide other services such as back-up or applications.

[6] Examples include Hulu (http://www.hulu.com), Netflix (http://www.netflix.com), and YouTube (http://www.youtube.com), which provide video streaming, and music-streaming service Spotify (http://www.spotify.com/us).

c11173008

Deployment Model Comparison and Use by Federal Agencies

In many ways, private-cloud computing may be easier to implement for federal agencies than public-cloud computing, especially where agencies already use data centers extensively.[7] It raises fewer concerns than other deployment models about the security and control of data, which can be significant obstacles to broad federal adoption. A challenge would be ensuring that benefits such as net cost savings are actually realized, given the potential expense of initial investment. The Department of Homeland Security (DHS), for example, provides a number of services to department components via a private cloud, while providing others through a public cloud.[8]

Service Models[9]

Cloud computing can provide various kinds of services, ranging from fundamental computing to provision of sophisticated applications. While they can be categorized in different ways, the NIST definition uses three basic *service models,* which are described below.[10]

Software as a Service (SaaS)

In the SaaS[11] model, customers use applications that the provider supplies and makes available remotely on demand, rather than using applications installed on a local workstation or server. SaaS is the most readily visible service model to the end user. In many cases, SaaS applications are accessible through hardware or software "thin clients."[12] They include web-based services such as Google Maps and Facebook, online storage, and services such as Paypal that websites can integrate into their applications.

---

[7] A data center is an information-technology facility that consolidates computing functions such as data storage and business applications that are made available for an organization across a network. Data centers are critical components of cloud computing, but may be used in other ways, depending on the architecture employed (see, for example, Cisco Systems, Cisco Cloud Computing: Data Center Strategy, Architecture, and Solutions, August 25, 2009, http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf). For discussion of issues related to data centers, see CRS Report R42604, *Department of Defense Implementation of the Federal Data Center Consolidation Initiative: Implications for Federal Information Technology Reform Management*, coordinated by Patricia Moloney Figliola.

[8] Richard Spires, "Celebrating Federal IT Reform with DHS Accomplishments," *CIOC Blog*, June 18, 2012, https://cio.gov/celebrating-federal-it-reform-with-dhs-accomplishments/.

[9] The NIST Definition of Cloud Computing. The generic term for cloud service models is *X*aaS. While the three described above are widely recognized as useful, they are not definitive. There may be other kinds of services, and the differences between models may not always be clear. Sometimes additional services are distinguished, such as data storage (DaaS) or communications (CaaS); or a particular service may have elements of two models, such as SaaS and IaaS.

[10] While other ways of characterizing cloud services have been discussed (see, for example, Sam Johnston, "Taxonomy: The 6 Layer Cloud Computing Stack," Sam Johnston, September 18, 2008, http://samj.net/2008/09/taxonomy-6-layer-cloud-computing-stack.html), the three models described by NIST are in widespread use.

[11] This is sometimes called *Applications as a Service.*

[12] A thin client is hardware or software that depends on the computer power of a server to which it is connected to perform computing tasks, rather than performing those tasks itself. It can therefore have less computing power—in other words, be "thinner"—than a client that performs those tasks itself. It is somewhat analogous to the "dumb terminal" once used to send instructions to a remote mainframe computer, where the computing hardware and software resided. An example of a modern hardware thin client is a mobile device such as a tablet computer or smartphone. An example of a software thin client is a web browser used as an interface for a cloud application. Examples of "fat" clients are desktop computers and local application programs such as word processors.

c11173008

Platform as a Service (PaaS)

With PaaS, customers create applications on the provider's infrastructure using tools, such as programming languages, supplied by the provider. One example of such an application is using PaaS to create a Web-based interface for customers. Such a platform could include hosting capability and development tools to facilitate building, testing, and launching a web application. The user controls the applications created via the platform, and the provider controls and maintains the underlying infrastructure, including networks, servers, and platform upgrades.

Infrastructure as a Service (IaaS)

IaaS providers supply fundamental computing resources that customers can use however they wish. Customers can install, use, and control whatever operating systems and applications they wish, as they might otherwise do on desktop computers or local servers. The provider maintains the underlying cloud infrastructure.

Service Model Comparison

A simple local-computing analogy for these three kinds of services would be the purchase of a desktop computer, which serves as *infrastructure* on which the user installs a chosen operating system such as Windows or Linux and uses it as a *platform* to create custom applications and run whatever commercial *software* is needed. By providing these services remotely, the cloud provider frees the customer from providing local infrastructure and support for them. In the case of IaaS, the user need not even have a local workstation, using instead a thin client with little embedded computing power.

Service Model Use by Federal Agencies

According to a survey of federal IT officials conducted in January 2012, the use of different deployment models within the government varies among the service models.[13] Reported use of public cloud computing decreased by half for IaaS and PaaS from 2011 to 2012, while use of public clouds for SaaS increased slightly. In both years, the majority of respondents reported using private clouds for each service model, with community or hybrid clouds[14] the next most common deployment model.

Considerations in Cloud Computing Adoption

Decisions in both the public and private sector regarding whether and how to use cloud computing involve consideration of several factors, notably cost, efficiency, accessibility, agility of improvements, security, reliability, and privacy.

[13] Federal Computer Week, "Research Report: Cloud Computing," March 20, 2012, http://fcw.com/microsites/2012/download-cloud-computing/index.aspx. The survey was based on 289 responses, and the described methodology did not permit a determination of how accurately the results represented overall patterns of use among agencies.

[14] The report presented combined results for these two deployment models.

c11173008

Cost

The potential financial benefits from cloud computing arise largely from the capability of this approach to provide far more efficient use of IT resources. Most commercial cloud services involve a different payment and cost model than local computing. Cloud providers make infrastructure investments that can lower cost barriers for IT end users, who can access services requiring expensive hardware or software without having to invest in it. Users pay only for the computing power that they consume. This approach to pricing is sometimes referred to as the "utility computing model" because of its similarity to how utilities such as electricity, water, and gas are provisioned. The model allows on-demand scalability that can meet a user's peak service requirements without the user having to invest in infrastructure to meet such requirements. Such peak demand may be periodic, as in the case of seasonal changes in use, or episodic, as in the case of a software developer needing temporary increases in computing capability for application development or testing.

With local IT, in contrast, users must acquire and maintain sufficient hardware, software, and other local resources, such as personnel, to provide for usage that varies over time, often in an unpredictable way. For example, even on most desktop computers, much of the memory and hard drive, and many applications, are usually idle. That is often also true for local servers and is one of the arguments made by the Obama Administration for its Federal Data Center Consolidation Initiative (FDCCI).[15] For example, for FY2012 the Treasury Department projected that in most of its data centers, servers would be idle more than one-third of the time on average.[16]

With cloud computing, in contrast, users need not invest in resources that will often remain idle, but can acquire and pay for services only as they use them. According to some economic analyses, cloud computing using a public cloud can produce savings over local computing when demand for a service varies significantly over time or cannot be predicted.[17] Also, as the cloud computing market continues to develop, it may result in a small number of large providers of cloud infrastructure most capable of taking advantage of the benefits of economies of scale.[18] Additional potential financial benefits of cloud computing include the savings cloud providers may realize from locating facilities in areas with lower-than-average energy and labor costs.[19]

In addition, cloud computing shifts some financial risks from the user to the provider. For example, if a new application that requires significant computing power proves unsuccessful, the implementing business or government agency would lose only the cost of the cloud services

---

[15] See CRS Report R42604, *Department of Defense Implementation of the Federal Data Center Consolidation Initiative: Implications for Federal Information Technology Reform Management*, coordinated by Patricia Moloney Figliola.

[16] Specifically, the department projected that in FY2012 only 10% of its servers would have average use rates greater than 65% (Department of the Treasury, *Treasury Strategic Sustainability Performance Plan*, June 2011, http://www.treasury.gov/about/organizational-structure/offices/Documents/Treasury%202011%20SSPP%20for%20posting%20v2.pdf).

[17] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report No. UCB/EECS-2009-28 (Electrical Engineering and Computer Sciences, University of California at Berkeley, February 10, 2009), http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[18] This appears to be what happened in the evolution of the microchip industry, where companies that once may have had to invest in facilities to manufacture their own chips, with attendant risks and costs, now contract with major providers who produce chips for many businesses at high volume in technologically advanced facilities. (Ibid.)

[19] Ibid.

c11173008

required, rather than the major investment in local IT that would have been required to provide the equivalent computing power.

In at least some cases, however, costs associated with cloud computing may outweigh potential financial benefits. One commonly cited cost is migration. If a user needs to move resources such as data from its own local facilities to those of the cloud provider, there will be a cost for such migration. That cost will depend on a number of factors, such as the size of the resources being moved, the method by which they are moved,[20] and whether the resources will need to be modified.[21] Such costs are also a consideration with respect to a potential move from one cloud provider to another. If a provider uses a nonstandard, proprietary platform, that would likely increase the cost of switching to another provider.

The potential economic benefits of cloud computing are also expected to vary depending on the deployment model. Use of a public cloud is thought to create greater savings in general than use of a private cloud. Presumably, that is because the former can take more advantage of economies of scale and other efficiencies, and is more subject to the effects of market competition. In addition, costs associated with inefficient use of local IT may be transferred to the cloud environment in some cases. For example, some organizations that maintained unused software in their local environments have retained similar software in switching to SaaS, incurring the costs associated with that inefficiency.[22]

Although most observers appear to believe that cloud computing can offer substantial economic benefits, attempts to project the cost advantages vary widely, with cloud services estimated to cost anywhere from 10% to 250% as much as local IT, but with most estimates projecting savings of at least 50%.[23] The large variation appears to reflect uncertainties arising not only from imperfect understanding of the economics of cloud computing in general, but also from variations in need and circumstance among potential users and uses. For example, a large organization that has a highly efficient data center may not benefit economically by moving it to a public cloud, whereas a small one might benefit.[24] Also, migration costs are likely to vary among different local computing environments. Some observers also have expressed skepticism about the accuracy of analyses purporting to show significant cost advantages, cautioning that they may be outdated or incomplete.[25]

[20] For example, the cost of moving data via the Internet may be substantially different from the cost via physical media such as compact disks.

[21] For example, if the cloud provider uses a different data standard or format than the user's local facilities, then the data will need to be converted as part of the move.

[22] Nicholas Kolakowski, "Companies Taking Bad IT Habits into Cloud, Says Gartner—Cloud Computing from eWeek," *eWeek*, June 14, 2010, http://www.eweek.com/c/a/Cloud-Computing/Companies-Taking-Bad-IT-Habits-Into-Cloud-Says-Gartner-467151/?kc=EWKNLCSM06152010STR5.

[23] Nelson, *Briefing Paper on Cloud Computing and Public Policy*; Darrell West, *Saving Money Through Cloud Computing* (Brookings Institution, April 2010), http://www.brookings.edu/~/media/Files/rc/papers/2010/0407_cloud_computing_west/0407_cloud_computing_west.pdf.

[24] See, for example, Steve Lohr, "When Cloud Computing Doesn't Make Sense," *Bits Blog—New York Times*, April 15, 2009, http://bits.blogs.nytimes.com/2009/04/15/when-cloud-computing-doesnt-make-sense/#more-6501.

[25] See, for example, John Foley, "Claims Of Government Cloud Savings Don't Add Up," *Information Week*, April 9, 2010, http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=224202488.

c11173008

Energy Efficiency

Computers, servers, and related devices require large amounts of energy to manufacture,[26] and they account for a growing share of world energy consumption.[27] "Green computing" is often cited as a potential benefit of cloud computing. It makes heavy use of data centers, which can be specifically designed for efficient power usage and cooling. Taking advantage of economies of scale, cloud computing can potentially deliver computing power to many users much more efficiently than would be possible with local computing.[28] Google has projected that a small office of 50 workers would use only 1% as much energy per user if it used Gmail cloud-based e-mail service rather than relying on local servers, although this level of savings is diminished for larger businesses.[29]

By using a utility business model, cloud computing can provide incentives for efficient use of computing resources. Users pay only for the power they consume, and thus have an incentive to consume only what they need.[30]

Despite such potential, cloud computing is not necessarily inherently efficient. According to some analyses, typical measures taken by providers to ensure reliability can be energy inefficient or have other negative environmental effects.[31] More generally, to the extent that innovations arising from cloud computing result in increased demand for computing resources, cloud computing could drive an increase in overall use of information technology, just as the advent of the personal computing led to such an increase.

Also, potential benefits and costs may vary among users, depending on their particular needs. A Department of Energy (DOE) report on its Magellan project, which was designed to investigate the potential of cloud computing to meet the department's scientific computing needs, concluded that switching from the current non-cloud approach to public- or private-cloud computing would

[26] Eric Williams, "Energy Intensity of Computer Manufacturing: Hybrid Assessment of Combining Process and Economic Input-Output Methods," *Environmental Science & Technology* 38 (2004): 6166–6174, http://www.scribd.com/doc/4183/Energy-Intensity-of-Computer-Manufacturing; GHGm, *Social and Environmental Responsibility in Metals Supply to the Electronic Industry*, 2008, http://www.gesi.org/LinkClick.aspx?fileticket=anlAuBauWU8%3d&tabid=60.

[27] Environmental Protection Agency, *Report to Congress on Server and Data Center Energy Efficiency: P.L. 109-431*, April 2, 2007, http://hightech.lbl.gov/documents/DATA_CENTERS/epa-datacenters.pdf.

[28] The potential gains are particularly large for small institutional users. One study found that a business of 100 users could cut energy use by more than 90% by switching from an on-site version of certain software applications to a cloud-based equivalent. Accenture, *Cloud Computing and Sustainability: The Environmental Benefits of Moving to the Cloud*, 2010, http://www.gesi.org/LinkClick.aspx?fileticket=3VjQDU8OEAI%3d&tabid=216; eWEEK Europe, "Forrester: The Cloud Is Inherently Green," July 5, 2011, http://www.eweekeurope.co.uk/news/forrester-the-cloud-is-inherently-green-33331.

[29] Google's Green Computing: Efficiency at Scale, Google, September 7, 2011, http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/green/pdfs/google-green-computing.pdf

[30] Doug Washburn and Lauren E. Nelson, "Cloud Computing Helps Accelerate Green IT" (Forrester Research, June 30, 2011), http://www.forrester.com/rb/Research/cloud_computing_helps_accelerate_green_it/q/id/58938/t/2?src=RSS_2&cm_mmc=Forrester-_-RSS-_-Document-_-11.

[31] James Glanz, "Data Centers Waste Vast Amounts of Energy, Belying Industry Image," *The New York Times*, September 22, 2012, sec. Technology, http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html.

c11173008

be more expensive and no more efficient, in part because of the special needs associated with scientific computing.[32]

Availability

Cloud computing may provide both advantages and disadvantages with respect to availability. It can improve availability by using Internet connectivity to provide mobile computing services, so that users can access data and applications wherever they can get an Internet connection. Its flexible capacity and scalability can also reduce the risk of downtime for a website or other service. Scalable cloud hosting sources may also make web-based services more resilient to denial of service and similar cyberattacks.

However, reliance on the Internet for cloud computing means that, in contrast to local computing, an Internet connection failure would prevent a user from accessing computing services. In contrast, a local network could still function. Loss of Internet access could be especially significant if users rely on thin clients, which may not have sufficient computing power to run applications locally in the event of a connection failure. Nevertheless, Internet outages are commonly thought to be far less common than outages of local networks, and even that risk can be reduced, for example by use of more than one provider.

Effective use of cloud computing depends on access to high-speed Internet or mobile telecommunications. Such broadband access is not evenly distributed within the United States. Rural access is significantly lower than that in urban areas, resulting in much greater access to cloud services in cities.[33] If the use of cloud computing accessed through thin clients continues to grow in market share, that "digital divide" between areas with and without high-speed network access could become more pronounced. The American Recovery and Reinvestment Act of 2009 (P.L. 111-5) included $7.2 billion for expansions to rural broadband infrastructure,[34] and some other countries have devoted resources to facilitate ubiquitous access to high speed Internet.[35]

Agility

Cloud computing can be more agile than local computing in at least two ways. It can permit faster and more efficient implementation of upgrades and other technological advances. It can also provide innovators with a broader range of scalable tools for research, development, and testing than they would be able to acquire cost-effectively for a local computing environment. In some ways, agility can be more limited under cloud computing than local computing. Differences among providers may limit *portability* and *interoperability*.[36] If a user wishes to switch to a new

[32] Department of Energy, The Magellan Report on Cloud Computing for Science, December 2011, http://science.energy.gov/~/media/ascr/pdf/program-documents/docs/Magellan_Final_Report.pdf.

[33] See CRS Report RL30719, *Broadband Internet Access and the Digital Divide: Federal Assistance Programs*, by Lennard G. Kruger and Angele A. Gilroy.

[34] http://www.broadbandusa.gov/

[35] South Korea, for example, plans to spread extremely high speed Internet access across the country by the end of 2012, http://www.nytimes.com/2011/02/22/technology/22iht-broadband22.html.

[36] In general, *portability* refers to the ability to move a resource from one computer environment to another, and *interoperability* refers to the ability of different systems to communicate effectively (Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases," July 2, 2010, http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf.).

c11173008

provider, because of dissatisfaction or some other factor such as the original provider going out of business, portability may be a problem. The platform used by the new provider may require substantial modifications to data or other resources being moved or may even be incompatible. Provider variation may also hinder interoperability, which would be needed, for example, if users wish different providers to supply different services involving a common set of data or applications. This may be less of a problem with local computing, which usually employs standard hardware and software platforms so that data and applications can be used by different persons or moved to new hardware without a need for significant modification. These limitations might be addressed in the future by the creation and adoption of appropriate portability and interoperability standards for cloud computing.

Cloud computing may also be less capable than local computing in creating and implementing some specialized applications, such as in scientific research. For example, DOE's report on its Magellan project found that cloud computing did not meet several requirements for the kinds of scientific data and applications used in research and development (R&D) at the department.[37]

Security

Some aspects of security in cloud computing are similar to those with local computing involving local networks. Both are potentially subject to attacks aimed at service disruption or theft of information, including espionage. Both are subject to threats from the Internet and from insiders. Vulnerabilities specific to particular operating systems and other applications need to be addressed whether those applications are provided through cloud or local computing.

However, some aspects of cloud computing have security implications that differ substantially from those for local computing.[38] Differences in security of cloud and local computing mirror the differences between concentrated versus distributed resources in general. Thus, the economies of scale associated with cloud computing can permit providers to invest much more effectively in security than most users could with local computing.[39] But such concentration of computing resources also makes cloud providers more inviting targets for potential attackers and increases the potential impact of an attack. With local computing, each user constitutes a point of attack that must be defended separately, but the impact of an attack is generally limited to that user.[40] With

[37] The Magellan Report on Cloud Computing for Science, Department of Energy, December 2011, http://science.energy.gov/~/media/ascr/pdf/program-documents/docs/Magellan_final_report.pdf.

[38] See, for example, Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, September 1, 2011, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[39] Those economies of scale permit a cloud provider to invest more in security than a typical IT department in an organization using local computing, and can provide other advantages. For example, the scalability of cloud computing can provide much better defense against a denial-of-service attack than is possible with local computing.

[40] That is not always true. For example, an attack on a business that maintains billing or other records with personal information of customers may have impacts well beyond the target. For example, in 2011, hackers breached the customer network of electronics manufacturer Sony, compromising more than 70 million records. The company estimated the cost of the breach at $171 million (Larry Dignan, "Sony's Data Breach Costs Likely to Scream Higher," Between the Lines, April 24, 2011, http://www.zdnet.com/blog/btl/sonys-data-breach-costs-likely-to-scream-higher/49161). In March 2011, the security company RSA reported in an open letter to its customers that it had experienced a breach from "an extremely sophisticated cyber attack," resulting in exfiltration of information relating to one of its security products (Art Coviello, "Open Letter to RSA Customers," March 17, 2011, http://www.rsa.com/node.aspx?id=3872). Some observers have suggested that the attack was one part of a larger effort to target critical infrastructure entities, especially defense contractors and financial institutions (Mathew J. Schwartz, "Lockheed Martin Suffers Massive Cyberattack," Information Week, May 31, 2011, http://www.informationweek.com/news/government/
(continued...)

c11173008

cloud computing, both the points of attack and the defenses are concentrated, as is the value of the target.

Some other security issues are more specific to cloud computing. For example, the sharing of computing resources by different customers that permits the economies of scale in cloud computing creates unique security requirements associated with that multi-tenancy. Also, use of a public cloud provider creates a potential for ambiguity in how to assign security responsibilities to the provider and to the user. The user's data and other resources are housed off-site and are therefore under the control of the cloud provider—the owner of the data effectively cedes control of it to the provider, and possibly even a third party that the cloud provider might use.[41]

In addition to direct concerns, other security-related factors may need to be considered. For example, the degree of legal protection afforded to information in the cloud may be significantly lower if it is stored in a public cloud rather than on a local computer.[42] In addition, information could potentially be stored on servers in countries other than that in which the customer resides, thereby potentially subjecting the information to different or even conflicting legal requirements for privacy and auditability.[43] Within the United States, different federal laws apply to different kinds of data, for example health and financial information. State requirements also vary.[44]

Reliability

Services hosted in the cloud may be distributed among several different data centers. That distribution can potentially improve reliability over use of only a local data center, especially if combined with redundancy. However, there have been cases in recent years of downtime at the IaaS level that caused widespread service interruptions.[45] Despite the publicity such disruptions received, service downtimes in cloud computing have been rare, and many observers consider cloud hosting to be more reliable than local hosting.

NIST has also raised the issue of the service-level agreements (SLAs) that customers sign when procuring cloud services. While reliability is a key element addressed by practically every SLA, how it is defined, what is being measured, and the associated guarantees vary. These leave

(...continued)

security/229700151).

[41] This might happen, for example, if the cloud service is an application such as e-mail and the service provider uses another provider for data storage.

[42] See, for example, David Navetta, "Legal Implications of Cloud Computing—Part One (the Basics and Framing the Issues)," *LLRX.com*, September 12, 2009, http://www.llrx.com/features/cloudcomputing.htm; Digital Due Process Coalition, "About the Issue," 2010, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

[43] See, for example, European Network and Information Security Agency, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[44] For further discussion, see, for example, Tanya Forsheit, "Legal Implications of Cloud Computing—Part Two (Privacy and the Cloud)," Information Law Group, September 30, 2009, http://www.infolawgroup.com/2009/09/articles/breach-notice/legal-implications-of-cloud-computing-part-two-privacy-and-the-cloud/.

[45] In 2011 and 2012, Amazon, a large cloud provider, experienced outages in mid-Atlantic data centers that caused widespread downtime for many websites (Quentin Hardy, "Amazon's Cloud Is Disrupted by a Summer Storm," *The New York Times*, July 1, 2012, sec. Technology, http://www.nytimes.com/2012/07/02/technology/amazons-cloud-service-is-disrupted-by-a-summer-storm.html).

c11173008

customers to evaluate different SLAs with cloud providers that may define reliability using different—

- terms (uptime, resilience, or availability);
- resources (servers, HVAC systems, customer support);
- time periods (hours, days, years); and
- risk guarantees (response time versus resolution time).[46]

Privacy

Privacy is a concern, especially for public and hybrid cloud services. The greater direct control that private clouds give to users over hardware and software may provide them more control over management of privacy.

Establishing an effective and appropriate legal structure for regulating cloud computing services is imperative, as cloud usage is expected to represent more than half of all Internet use by the end of this decade.[47] Globally, advances in technology services such as cloud computing paired with how those services are used by consumers have increased the difficulty of maintaining the appropriate legal balance between individual rights and the needs of law enforcement. As the depth and breadth with which consumers incorporate cloud services into their daily lives increases, the need for balance becomes even more important, but also more difficult to attain.

In the United States, the Electronic Communications Privacy Act of 1986 (ECPA)[48] governs the privacy of electronic communications.[49] However, ECPA leaves gaps in how to treat certain now commonly used services, such as web-based e-mail and documents created and stored in the cloud (e.g., Google Docs); such services had not been created, nor even conceived, when the law was enacted. Many contend that ECPA is a difficult law to understand and apply, in part because the law is old and relies on a model of electronic mail and Internet activity that is generations behind current practice and technology. It is extremely difficult to interpret or predict the privacy

[46] NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume I , November 2011, http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf.

[47] Michael R. Nelson, *Briefing Paper on Cloud Computing and Public Policy*, September 29, 2009, http://www.oecd.org/dataoecd/39/47/43933771.pdf.

[48] Title II of the Electronic Communications Privacy Act (ECPA), also called the Stored Communications Act (SCA). Electronic Communications Privacy Act of 1986 (ECPA), P.L. 99-508. 18 U.S.C. §§2701–2711 (2000). The statute is called by a variety of names, including (1) the "Electronic Communications Privacy Act" or "ECPA" because it was first enacted as part of that statute; (2) "Chapter 121" because it has been codified in Chapter 121 of Title 18 of the United States Code; (3) the "Stored Wired and Electronic Communications and Transactional Records Access" statute or "SWECTRA" because that is the formal title given to Chapter 121 in Title 18; and (4) "Title II" because it was enacted as the second title of ECPA. See "A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It," Orin S. Kerr, 2004. An abstract, through which the full article can be accessed, is available online at http://ssrn.com/abstract=421860. With respect to consumer privacy rights, when most people talk about ECPA, they are referring to the SCA (18 U.S.C. §§2701-2711), which was ultimately enacted as Title II of ECPA. An in-depth review of the ECPA, in its entirety, can be found in CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[49] See also CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle; CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle, *Cloud and Mobile Privacy: The Electronic Communications Privacy Act* (Harvard Kennedy School, February 2012), http://belfercenter.ksg.harvard.edu/files/mohan-dp-mar-1-2012-02.pdf.

c11173008

protections available under ECPA for the wide range of cloud computing activities.[50] Companies offering communications and remote storage services (which were in their infancy in 1986), consumers, and law enforcement all seek uniformity in the law, but do not agree on how those changes should be made.

Trends in Total Federal Investment in Information Technology

Annual federal investment in information technology increased at an average annual rate of more than 6% in the last decade, from $46 billion in FY2001 to $81 billion in FY2010 (**Figure 1**). It has declined each year subsequently, with funding in FY2013 projected to be $5.7 billion, or 7%, less than in FY2010. In recent years, about 30% of the annual investment has been for new projects or significant modifications, with the remainder being for operations and maintenance.[51]

The Administration's budget requests since FY2011 have not included overall funding amounts for or projected savings from the cloud computing initiative. Independent projections have produced disparate estimates of future annual expenditures. INPUT, a market research firm, estimated that "cloud-related expenditures by federal agencies will grow from $440 million in 2010 to $1.44 billion in 2015."[52] However, Market Research Media, Ltd., another market research firm, estimated that figure to be closer to $7 billion by 2015.[53]

[50] Distinctions recognized by ECPA include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service. The precise characterization of an activity can make a significant difference to the protections afforded under ECPA. For example, if an "electronic communications service" holds a text message in "electronic storage," then law enforcement requires a probable cause warrant to obtain access. If a "remote computing service" stores the same text message on behalf of the subscriber, then law enforcement does not need a warrant, and a subpoena is sufficient.

[51] Office of Management and Budget, "Guidance on Exhibit 53—Information Technology and E-Government," August 5, 2011, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy13_guidance_for_exhibit_53-a-b_20110805.pdf. "Development/Modernization/Enhancement" (DME) refers to "costs for projects leading to new IT assets and projects that change or modify existing IT assets" (p. 9). Steady State (SS) refers to "the expenses associated with an IT asset that is in the operations and maintenance life-cycle phase" (p. 11).

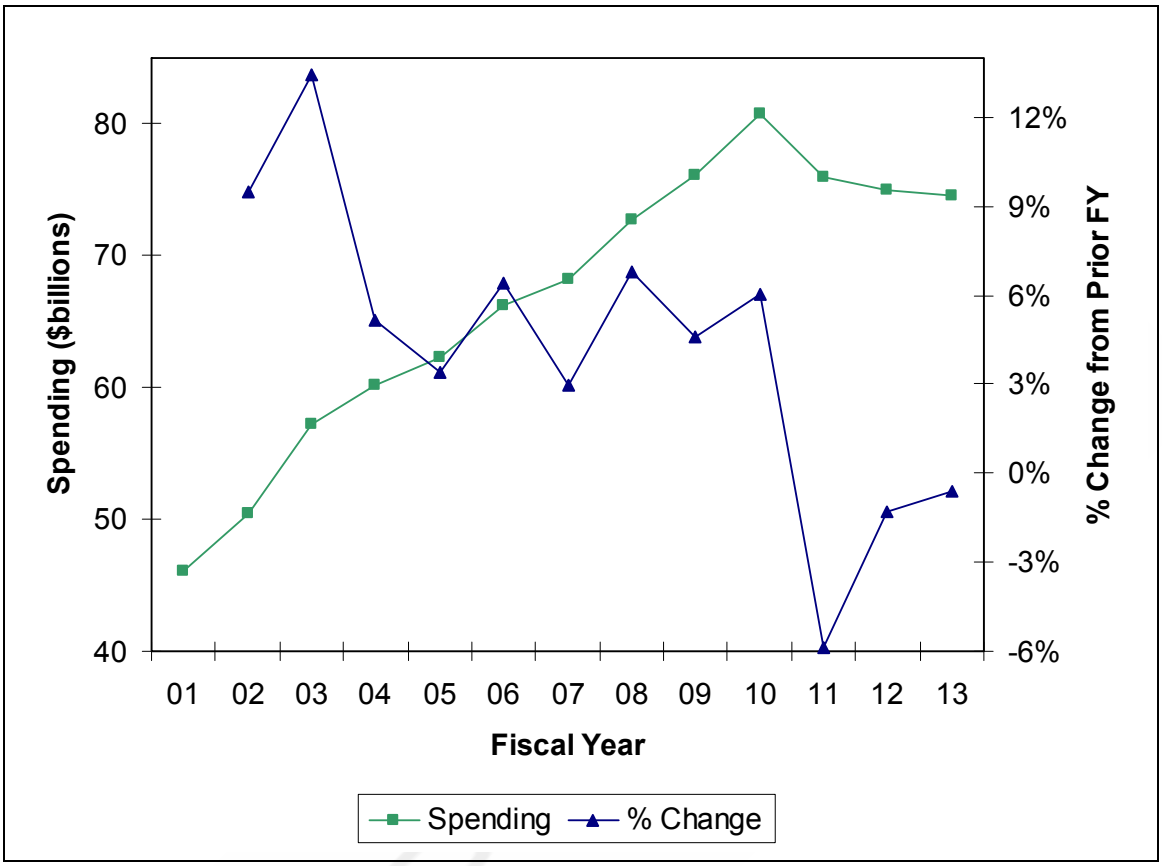
[52] John K. Higgins, "Getting Feds Comfortable With Cloud Culture," *E-Commerce Times*, February 23, 2011, http://www.ecommercetimes.com/story/71923.html.

[53] See High Performance Cloud Computing Symposium, March 23, 2011, http://www.technologyconference.com/?p=262.

c11173008

Figure 1. Trends in Total Federal Investment in Information Technology

Fiscal Years 2001-2013



Source: Spreadsheets on federal IT spending for Fiscal Years (FY) 2003-2013, available at OMB, "Office of E-Government & Information Technology," 2012, http://www.whitehouse.gov/omb/e-gov/docs/.

Note: Data are for actual expenditures, except FY2012 (enacted) and FY2013 (proposed) and include the costs of products, services, and personnel. The amounts in the spreadsheets may be somewhat lower than the corresponding amounts in presidential budget request documents, presumably because the spreadsheets omit IT investments for some federal entities and programs. For example, the request for FY2013 in the OMB spreadsheet is $74.5 billion, whereas that in the FY2013 budget request was $78.9 billion. These are the most up-to-date figures available at this time.

Federal Planning and Activity

The Federal Cloud Computing Initiative (FCCI) was announced in September 2009[54] to implement cloud computing within the federal government and improve operational efficiencies, optimize common services across organizations, and enable more government transparency.[55] Since then, the Administration has created a larger plan for implementing overall IT reform and developed a strategy specifically to achieve the goals of the FCCI.

[54] Vivek Kundra, "Streaming at 1:00: In the Cloud," The White House, September 15, 2009, http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/.

[55] http://www.info.apps.gov/node/2.

c11173008

25-Point Implementation Plan to Reform Federal IT Management

In December 2010, the U.S. Chief Information Officer (CIO) released "A 25-Point Implementation Plan to Reform Federal IT Management"[56] as part of a comprehensive effort to increase the operational efficiency of federal technology assets. The reforms put forth in the plan are focused on eliminating barriers that impede effective management of IT programs throughout the federal government. The CIO recognized that too many federal IT projects run over budget, fall behind schedule, or fail to deliver promised functionality, which hampers agency missions and wastes taxpayer dollars.

As the federal government implements the plan, the role of agency CIOs will move away from only policymaking and infrastructure maintenance to encompass complete IT portfolio management. There are four main areas in which agency CIOs now have a lead role: governance, commodity IT, program management, and information security (**Table 1**).

Within those four areas, CIOs will be held accountable for lowering operational costs, terminating and turning around troubled projects, and delivering meaningful functionality at a faster rate while enhancing the security of information systems.

Federal Cloud Computing Strategy

One element of the 25-Point Plan is for agencies to shift to a "Cloud First" policy ("Cloud First").[57] To implement that policy, the Administration developed the Federal Cloud Computing Strategy (FCCS).[58] The strategy describes the—

- mandate to agencies;
- impetus for developing the strategy;
- planned goals of the strategy; and
- expected savings from the strategy.

The day-to-day management of the FCCS is conducted by the General Services Administration (GSA) under the Federal Cloud Computing Program Management Office (PMO).

In accordance with the 25-Point Plan, the strategy mandates a shift to Cloud First, which means that federal agencies must (1) implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists; and (2) begin reevaluating and modifying their individual IT budget strategies to include cloud computing.

[56] A 25-Point Implementation Plan to Reform Federal IT Management, Office of the U.S. Chief Information Officer, December 9, 2010, https://cio.gov/wp-content/uploads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf. ("25-Point Plan")

[57] 25-Point Plan, pp. 6-8.

[58] Federal Cloud Computing Strategy, Office of the U.S. Chief Information Officer, February 8, 2011, http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf. ("Federal Cloud Computing Strategy")

c11173008

Table 1. Agency CIO Responsibilities Under the 25-Point Plan

Governance. CIOs must drive the investment review process for IT investments and have responsibility over the entire IT portfolio for an agency. CIOs must work with Chief Financial Officers and Chief Acquisition Officers to ensure IT portfolio analysis is an integral part of the yearly budget process for an agency. The IT Reform plan restructured the investment review boards (IRBs) by requiring agency CIOs to lead "TechStat" sessions—actionable meetings designed to improve line-of-sight between project teams and senior executives. Outcomes from these sessions must be formalized and followed-up through completion, with the goal of terminating or turning around one-third of all underperforming IT investments by June 2012.
Commodity IT. Agency CIOs must focus on eliminating duplication and rationalize their agencies' IT investments. Agency commodity services are often duplicative and sub-scale and include services such as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions). The CIO shall pool his or her agency's purchasing power across the entire organization to drive down costs and improve service for commodity IT. In addition, enterprise architects will support the CIO in the alignment of IT resources, to consolidate duplicative investments and applications. CIOs must show a preference for using shared services as a provider or consumer instead of standing up separate independent services.
Program Management. Agency CIOs shall improve the overall management of large federal IT projects by identifying, recruiting, and hiring top IT program management talent. CIOs will also train and provide annual performance reviews for those leading major IT programs. CIOs will also conduct formal performance evaluations of component CIOs (e.g., bureaus, sub-agencies, etc.). CIOs will be held accountable for the performance of IT program managers based on their governance process and the IT Dashboard.
Information Security. CIOs, or senior agency officials reporting to the CIO, shall have the authority and primary responsibility to implement an agency-wide information security program and to provide information security for both the information collected and maintained by the agency, or on behalf of the agency, and for the information systems that support the operations, assets, and mission of the agency. Part of this program will include well-designed, well-managed continuous monitoring and standardized risk assessment processes, to be supported by "CyberStat" sessions run by the Department of Homeland Security to examine implementation. Taken together, continuous monitoring and CyberStats will provide essential, near real-time security status information to organizational officials and allow for the development of immediate remediation plans to address any vulnerabilities.

Source: Memorandum for Heads of Executive Departments and Agencies, Office of Management and Budget, August 8, 2011.

In promulgating the strategy, the CIO cited low asset utilization in the current federal IT environment; a fragmented demand for resources; duplicative systems; environments which are difficult to manage; and long procurement lead times as the impetus for adopting the policy. The goals of the strategy are to accelerate the pace at which the government may realize the value of cloud computing by—

- articulating the benefits, considerations, and trade-offs of cloud computing;
- providing a decision framework and case examples to support agencies in migrating towards cloud computing;
- highlighting cloud computing implementation resources; and
- identifying federal government activities and roles and responsibilities for catalyzing cloud adoption.

An estimated $20 billion of the federal government's $80 billion in IT spending is a potential target for migration to cloud computing solutions.[59]

[59] "Progress Made but Future Cloud Computing Efforts Should Be Better Planned," Government Accountability Office, July 2012, http://www.gao.gov/assets/600/592249.pdf. ("GAO Report")

c11173008

Federal Cloud Computing Strategy: Supporting and Complementary Initiatives, Programs, and Committees

Implementation of the FCCS is not conducted in a vacuum. There are a number of other supporting and complementary government initiatives, programs, and committees that are intended to facilitate the adoption of cloud computing by federal agencies.[60]

Federal Data Center Consolidation Initiative[61]

Launched in February 2010, the FDCCI is aimed at reducing the number of data centers that the federal government operates to save money and energy and encouraging agencies to focus on efficient modes of computing instead of simply constructing more data centers. The goal of the FDCCI is to close 1,000 of the 2,015 total federal data centers by 2015.[62] As more centers are closed, agencies will have to shift to cloud computing. The day-to-day management of the FDCCI is conducted by the OMB. Additionally, the General Services Administration (GSA) has established an FDCCI PMO to support OMB in the planning, execution, management, and communication for the FDCCI.

Federal Risk and Authorization Management Program[63]

The Federal Risk and Authorization Management Program (FedRAMP) was established in December 2011 to provide a standard, centralized approach to assessing and authorizing cloud computing services and products. It reached initial operational capabilities in June 2012 and is to be fully operational during FY2014. FedRAMP provides security monitoring and authorization services for government and commercial cloud computing systems intended for multi-agency use. It will enable the government to buy a cloud solution once, with the ability to deploy that solution across multiple agencies. The specific stated goals of FedRAMP are to—

- ensure that cloud-based services have adequate information security;
- eliminate the duplication of effort and reduce risk management costs; and
- enable rapid and cost-effective procurement of information systems/service for federal agencies.

Under the primary leadership of the FedRAMP PMO at GSA, FedRAMP is managed jointly by the—

- FedRAMP PMO, which provides operational management of the program.
- Joint Authorization Board (JAB), which is the primary governance and decision-making body for the FedRAMP program. The JAB reviews and provides joint

[60] Less-closely related initiatives include the IT Shared Services Strategy (https://cio.gov/it-shared-services/); IT Dashboard (https://cio.gov/maximizing-value/it-dashboard/); and PortfolioStat (https://cio.gov/maximizing-value/portfoliostat/).

[61] http://www.cio.gov/fdcci

[62] Progress of the FDCCI can be tracked here: https://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37.

[63] http://www.fedramp.gov/

c11173008

provisional security authorizations of cloud solutions that will be adopted by the program. Members of the JAB are the CIOs from GSA, the Department of Homeland Security (DHS), and the Department of Defense.

- National Institutes for Standards and Technology (NIST), which provides technical assistance, maintains FISMA standards, and establishes technical standards.
- Federal CIO Council, which coordinates cross agency communications.
- DHS, which monitors and reports on security incidents and provides data for continuous monitoring.

TechStat[64]

The TechStat initiative, managed by OMB, provides evidence-based reviews of agency IT investments conducted between OMB and agency leadership, including plans to migrate to cloud services. This approach has reportedly reduced costs across all agencies by over $900 million dollars. Paired with the management improvements stemming from these reviews, the total cost savings is said to be nearly $4 billion.

Apps.gov[65]

Apps.gov is a program of the GSA that provides agencies with a single, consolidated source of SaaS applications, including business, productivity, and social media. Other services, including storage, processing, and hosting of applications, are being developed.[66] Apps.gov is intended to reduce the burden on agencies to conduct their own procurement processes and to concentrate investments in the highest-performing cloud providers.

Standards Acceleration to Jumpstart Adoption of Cloud Computing[67]

The Standards Acceleration Jumpstarting Adoption of Cloud Computing (SAJACC) initiative is designed to provide access to standards for cloud computing, as they are developed, and also to provide specifications and other guidance for cloud computing those areas where gaps exist.[68] The major focus is on portability, interoperability, and security of cloud services. To date, SAJACC has defined 24 generic technical use cases that can be used to validate key interoperability, security, and portability requirements. The SAJACC initiative is managed by NIST.

[64] https://cio.gov/maximizing-value/portfoliostat

[65] http://info.apps.gov/

[66] General Services Administration, "Apps.Gov."

[67] http://www.nist.gov/itl/cloud/sajacc.cfm

[68] Lee Badger and Tim Grance, "Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)" (presented at the NIST Cloud Computing Forum and Workshop I, Washington, DC, May 20, 2010), http://csrc.nist.gov/groups/SNS/cloud-computing/documents/forumworkshop-may2010/nist_cloud_computing_forum-badger_grance.pdf.

c11173008

CIO Council Executive Cloud Computing Executive Steering Committee

The CIO Council Executive Cloud Computing Executive Steering Committee (CCESC) was established to provide strategic direction and oversight for the Federal Cloud Computing Initiative. There are currently four subordinate groups[69] to the committee that are working to facilitate information sharing among agencies, support the migration of e-mail services to the cloud, develop a centralized security assessment and authorization process, and define cloud computing security, portability, and interoperability standards.

PortfolioStat[70]

PortfolioStat requires agencies to review IT spending in six areas: collaboration, unified communications, enterprise content management, search, reporting and analysis, and content creation. Agencies were required to submit in June 2012 a draft action plan on how they planned to consolidate commodity IT, including financial goals, and final plans for the next three years were due in August. Agencies have until the end of 2012 to migrate at least two "duplicative" commodity IT areas to shared services or cross-agency contracts. PortfolioStat is managed by OMB.

Agency Cloud Adoption: Status

The federal government is often described as being slower to adapt to new technologies such as cloud computing because of lengthy review processes and more stringent requirements for security, privacy, and reliability than most organizations in the private sector.[71]

July 2012 Government Accountability Office Report

In July 2012, the Government Accountability Office (GAO)[72] reported to the Senate on its findings concerning the Office of Management and Budget's (OMB's) "Cloud First" policy.[73] GAO had been asked by the Senate[74] to (1) assess the progress selected agencies have made in implementing this policy and (2) identify challenges they are facing in implementing the policy. To do so, GAO (1) selected seven agencies,[75] analyzed agency documentation, and interviewed agency and OMB officials; and (2) identified, assessed, and categorized common challenges.

---

[69] Those groups are the (1) Cloud Computing Advisory Council, which serves as a collaborative environment for senior IT experts from across the Federal Government; (2) Cloud Computing E-mail Working Group, which is a source of SaaS email information, solutions, and processes that foster adoption; (3) Cloud Computing Security Working Group, which provides a centralized cloud computing assessment and authorization body; and (4) Cloud Computing Standards Working Group which leads government-wide efforts to define cloud computing security, portability, and interoperability standards.

[70] https://cio.gov/maximizing-value/portfoliostat/

[71] http://www.marketconnectionsinc.com/images/stories/downloads/GITEC_Survey.pdf

[72] GAO Report, p. 7.

[73] The performance audit was conducted from October 2011 through July 2012.

[74] The Senate Committee on Homeland Security and Governmental Affairs and the Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security.

[75] The selected agencies are the Departments of Agriculture, Health and Human Services, Homeland Security, State, (continued...)

c11173008

GAO found that the selected agencies had made progress implementing the Cloud First policy. Consistent with the policy, each of the seven agencies had incorporated cloud computing requirements into its policies and processes. Further, the seven agencies had met the OMB deadlines to identify three cloud implementations by February 2011 and to implement at least one service by December 2011. GAO also noted that two agencies had reported that they did not plan to meet OMB's deadline to implement three services by June 2012, but did plan to do so by the end of 2012.

GAO also reported that each of the seven agencies had identified opportunities for future cloud implementations, such as moving storage and help desk services to a cloud environment. While all of the agencies submitted plans to OMB for implementing the cloud solutions, only one plan contained all of the key required elements. For example, 7 of the 20 plans did not include estimated costs and none of the plans for services that were to migrate existing functionality to a cloud-based service included plans for retiring or repurposing the associated legacy systems. According to agency officials, this was largely because the information was not available at the time the plans were developed. GAO concluded that until agencies' cloud implementations are sufficiently planned and relevant systems are retired, the benefits of federal efforts to implement cloud solutions—improved operational efficiencies and reduced costs—may be delayed or not fully realized.

October 2012 InformationWeek Survey

In addition to the July 2012 GAO report,[76] in October 2012, InformationWeek surveyed federal government IT professionals regarding the status of government cloud computing migration.[77] The survey results showed that half of federal agencies have adopted cloud computing in some way—21% are already moving forward with cloud adoption and 29% are in the early stages; last year the percentage that had begun to adopt cloud computing was 40%.[78] Further, more than half of agencies have identified use cases for cloud services and 46% have evaluated cloud products and services.[79]

Service Model Adoption

Public commercial cloud services are the most widely used in the federal government, cited by 18% of respondents using or assessing cloud services. Private clouds operating inside government data centers are next, used by 14%. In both cases, those results are a few percentage points higher than in 2011. Demand is building for private clouds, with 39% of respondents indicating they are highly likely to adopt them.

(...continued)

and Treasury; the General Services Administration; and the Small Business Administration.

[76] GAO Report.

[77] 2013 Federal Government Cloud Computing Survey, InformationWeek, October 05, 2012, http://reports.informationweek.com/abstract/104/9047/Government/research-federal-cloud-computing-survey.html?cid=pub_analyt__iwk_20121008. ("2013 InformationWeek Survey")

[78] 2013 InformationWeek Survey.

[79] No federal survey was conducted in 2013.

c11173008

Deployment Model Adoption

IaaS is the most-used type of cloud service among survey respondents, at 49%. That is followed by storage-as-a-service (32%),[80] SaaS (25%), and PaaS (19%).

Agency Cloud Adoption: Challenges

There are a number of reasons that adoption is not occurring more rapidly. Both the GAO[81] and the InformationWeek survey[82] identified some of the same (or similar) challenges to moving services to the cloud: security risks, ensuring portability and interoperability, perceived lack of knowledge and expertise in the workforce, lengthy certification and accreditation processes, and perceived lack of implementation guidance.

Security

The GAO and InformationWeek both found that security is the top concern of those responsible for implementing cloud computing at the agency level.

The GAO investigation found concerns that some cloud vendors may not be familiar with security requirements that are unique to government agencies, such as continuous monitoring and maintaining an inventory of systems. For example, Department of State officials described their ability to monitor their systems in real time, which they said cloud service providers were unable to match. Treasury officials also explained that the Federal Information Security Management Act's requirement of maintaining a physical inventory is challenging in a cloud environment because the agency does not have insight into the provider's infrastructure and assets.

In the InformationWeek survey, security was named by 68% of respondents as their primary concern regarding cloud adoption. FedRAMP, discussed previously, is intended to increase confidence in the cloud by standardizing the security assessment of vendor facilities and services.[83] The goal of the program is to eliminate duplication of effort and incompatible or inconsistent requirements for cloud security across agencies, and to streamline acquisition. At this time, according to the survey, only about 1 in 10 have begun using FedRAMP, so it is difficult to say what, if any, impact the program has had thus far. Given the time for FedRAMP to become more embedded in the acquisition process, it is expected to have considerable positive impact.

[80] Storage-as-a-service is not recognized by NIST as a service model. It involves a large service provider renting space in their storage infrastructure on a subscription basis and is often used to solve offsite back-up challenges.

[81] GAO Report.

[82] 2013 InformationWeek Survey. The top challenges identified by respondents to the InformationWeek survey who were using or assessing cloud services were security (68%), compatibility with legacy systems and processes (51%), lack of expertise and experience (31%), and inadequate guidance (25%).

[83] General Services Administration, "FedRAMP," 2011, http://www.gsa.gov/portal/category/102371; Pete Tseronis et al., "Federal Risk and Authorization Management Program," http://csrc.nist.gov/groups/SNS/cloud-computing/documents/forumworkshop-may2010/nist_cloud_computing_forum-mell.pdf.

c11173008

Portability and Interoperability

Agencies expressed concern to GAO that their ability to change cloud vendors could be limited through platforms or technologies that "lock" customers into a particular product. A Treasury official explained that it is challenging to separate from a vendor, in part due to a lack of visibility into the vendor's infrastructure and data.

Knowledge and Expertise

Agencies may not have the necessary tools or resources, such as expertise among staff, to implement cloud solutions. DHS officials explained that delivering cloud services without direct knowledge of the technologies has been difficult. Similarly, an HHS official stated that teaching their staff an entirely new set of processes and tools—such as monitoring performance in a cloud environment—has been a challenge.

Certification and Accreditation

Agencies may not have a mechanism for certifying that vendors meet standards for security, in part because the Federal Risk and Authorization Management Program (FedRAMP) had not yet reached initial operational capabilities.[84] For example, GSA officials stated that the process to certify Google to meet government standards for their migration to cloud-based e-mail was a challenge. They explained that, contrary to traditional computing solutions, agencies must certify an entire cloud vendor's infrastructure. In Google's case, it took GSA more than a year to certify more than 200 Google employees and the entire organization's infrastructure (including hundreds of thousands of servers) before GSA could use Google's service.

Implementation Guidance

Existing federal guidance for using cloud services may be insufficient or incomplete. Agencies cited a number of areas where additional guidance is needed such as purchasing commodity IT and assessing Federal Information Security Management Act security levels.[85] For example, an HHS official noted that the 25-Point Plan required agencies to move to cloud-based solutions before guidance on how to implement it was available. As a result, some HHS operating divisions were reluctant to move to a cloud environment. In addition, Treasury officials noted confusion over NIST definitions of the cloud deployment models, but noted that recent NIST guidance has been more stable.

[84] FedRAMP reached initial operational capabilities in June 2012. According to OMB, FedRAMP will reduce duplicative efforts, inconsistencies, and cost inefficiencies associated with the current security authorization process.

[85] As required under the Federal Information Security Management Act of 2002, NIST guidance defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The three potential impact levels of a breach are: low (limited adverse effect), moderate (serious adverse effect), and high (catastrophic adverse effect).

c11173008

Agency Cloud Adoption: Drivers

There are two main drivers of cloud adoption by federal agencies, budget concerns and data center consolidation.

Budget Concerns

In spite of the challenges to cloud adoption, the survey identified two strong drivers of cloud adoption: lowering the cost of IT operations and reducing investment in servers and data center equipment.[86] More than half of respondents using or assessing cloud services have compared the costs of cloud services to existing systems and found some level of savings.[87] It appears that in spite of existing challenges budget pressures may play a significant role in driving cloud adoption.

Data Center Consolidation

Data center consolidation, discussed previously, is another driver of cloud adoption. The Federal Data Center Consolidation Initiative (FDCCI)[88] is aimed at reducing the number of data centers that the federal government operates to save money and energy and encouraging the federal government to focus on efficient modes of computing instead of simply constructing more data centers. The FDCCI is directly tied to the FCCS. The goal of the FDCCI is to close 1,100 of the 2,015 total federal data centers by 2015.[89] As more centers are closed, agencies will have to shift to cloud computing. Consolidations are expected to result in nearly $3 billion in savings by 2015, as well as produce future savings.

[86] Lowering the cost of ongoing IT operations was the most-cited business driver, mentioned by 54% of the InformationWeek survey respondents. That was followed by reducing capital investment in servers and data center equipment (51%).

[87] "Federal Agencies Build a Business Case for the Cloud," *Information Week*, October 08, 2012, http://reports.informationweek.com/abstract/104/9047/Government/research-federal-cloud-computing-survey.html?cid=pub_analyt__iwk_20121008.

[88] http://www.cio.gov/fdcci. The FDCCI was also mentioned in the President's FY2013 Budget Request, p. 347. ("The Data Center Consolidation effort resulted in agencies committing to close nearly 1,100 data centers by 2015 (exceeding the original goal of 800), with 525 of those closures expected to be completed by the end of 2012 (over 25% of these closed in 2011). Consolidations are expected to save the Government $3 billion by 2015, and result in more savings in the years beyond 2015.")

[89] Progress of the FDCCI can be tracked here: https://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37.

c11173008

Activity in the 113th Congress

Legislation

H.R. 756—Cybersecurity Enhancement Act of 2013

H.R. 756 was introduced by Representative Michael McCaul on February 15, 2013. The bill was reported (amended) on April 11, 2013 (H.Rept. 113-33). It was passed by the House and referred to the Senate Committee on Commerce, Science, and Transportation on April 17, 2013. This bill would, among other things—

- Require the NIST Director, in collaboration with the federal Chief Information Officers Council, to continue to develop and encourage implementation of a comprehensive strategy for the use and adoption of cloud computing services by the federal government.
- Require consideration to be given to activities that:

  (1) accelerate the development, in collaboration with the private sector, of standards that address the interoperability and portability of cloud computing services;

  (2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

  (3) support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for federal agencies to use in addressing security and privacy requirements.

H.R. 967—Advancing America's Networking and Information Technology Research and Development Act of 2013[90]

H.R. 967 was introduced by Representative Cynthia Lummis on March 5, 2013. The bill was reported (H.Rept. 113-34) by the House Committee on Science, Space, and Technology on April 11, 2013, and referred to the Senate Committee on Commerce, Science, and Transportation on April 17, 2013. This bill would, among other things—

- Require the Director of the National Coordination Office, through the National Science and Technology Council, to convene an interagency working group to:

  (1) explore the R&D needed to enhance the effectiveness of cloud computing environments, increase the trustworthiness of cloud applications and infrastructure, and enhance the foundations of cloud architectures, programming models, and interoperability;

[90] H.R. 1468, the SECURE IT Act of 2013, is a related bill to H.R. 3834. Section 407 of the bill contains conforming and technical amendments to the High-Performance Computing Act of 1991. However, it does not change the functions of the program or its management structure.

c11173008

(2) examine how federal science agencies can facilitate the use of cloud computing for federally funded science and engineering research; and

(3) report to Congress on the findings and recommendations of the working group.

H.R. 1232—Federal Information Technology Acquisition Reform Act of 2013

H.R. 1232 was introduced by Representative Darrell Issa on March 18, 2013. The bill was referred to the Committee on Oversight and Government Reform and ordered reported on March 20, 2013. This bill would, among other things—

- Express the sense of Congress that transition to cloud computing offers significant potential benefits for the implementation of federal information technology projects in terms of flexibility, cost, and operational benefits.
- Require, in assessing cloud computing opportunities, that the Chief Information Officers Council shall define policies and guidelines for the adoption of government-wide programs providing for a standardized approach to security assessment and operational authorization for cloud products and services.
- In transitioning to the cloud, allow a Chief Information Officer of an agency to establish cloud service Working Capital Funds as may be necessary to transition to cloud-based solutions. These cloud service Working Capital Funds may preserve funding for cloud service transitions for a period not to exceed five years per appropriation.

S. 1197—National Defense Authorization Act for Fiscal Year 2014

S. 1197 was introduced by Senator Carl Levin on June 20, 2013. The bill was referred to the Committee on Armed Services and reported the same day (S.Rept. 113-44). This bill would, among other things—

- Require the Secretary of Defense, acting through the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, the Chief Information Officer of the Department of Defense, and the Chairman of the Joint Requirements Oversight Council, supervise:

  (a) Review, development, modification, and approval of requirements for cloud computing solutions for intelligence data analysis and storage by the Armed Forces and the Defense Agencies, including requirements for cross-domain, enterprise-wide discovery and correlation of data stored in cloud and non-cloud computing databases, relational and non-relational databases, and hybrid databases.

  (b) Review, development, modification, approval, and implementation of plans for the competitive acquisition of cloud computing systems or services to meet requirements described in subparagraph (A), including plans for the transition from current computing systems to systems or services acquired.

  (c) Development and implementation of plans to ensure that the cloud systems or services acquired pursuant to subparagraph (B) are interoperable and universally accessible and usable through attribute-based access controls.

c11173008

(d) Integration of plans under subparagraphs (B) and (C) with enterprise-wide plans of the Armed Forces and the Department of Defense for the Joint Information Environment and the Defense Intelligence Information Environment.

S. 1353—Cybersecurity Act of 2013

S. 1353 was introduced by Senator John Rockefeller on July 24, 2013. The bill was referred to the Committee on Commerce, Science, and Transportation and ordered to be reported with an amendment in the nature of a substitute favorably, on July 30, 2013. In addition to other purposes, this bill would direct the Office of Science and Technology Policy (OSTP) to develop, and update triennially, a federal cybersecurity research and development plan to meet cybersecurity objectives, including how to guarantee individual privacy, verify third-party software and hardware, address insider threats, determine the origin of messages transmitted over the Internet, and protect information stored using cloud computing or transmitted through wireless services.

S. 1843—Federal Information Technology Savings, Accountability, and Transparency Act of 2013

S. 1843 was introduced by Senators Tom Udall and Jerry Moran on December 17, 2013, and referred to the Committee on Homeland Security and Governmental Affairs the same day. S. 1843 is a scaled-back version of a House bill that was stripped from a compromise on the FY2014 National Defense Authorization Act (H.Res. 441). Although not as extensive as the House bill, H.R. 1232 (see above), S. 1843 would go "further to increase CIOs' authority over agency IT procurements through their inclusion in the budget planning process. Under the Senate bill, this authority would cover not only information technology or programs with significant IT components, but also would extend to 'the acquisition of an information technology product or service that is a commercial item.'"[91] Among other provisions, the bill would—

- increase the authority of federal CIOs to optimize how federal civilian agencies use IT;
- increase the responsibilities of the CIO Council to include developing cross-agency portfolio management practices to allow and encourage the development of cross-agency shared services and shared platforms and issue guidelines and practices for expansion of the federal enterprise architecture process, if appropriate; and
- require improvements to increase the transparency of the IT Dashboard, the OMB website that tracks federal IT spending.

Hearings

The House of Representatives has held four hearings on issues related to cloud computing.

[91] "Bill to Improve IT Acquisitions Introduced In Senate as Obama Calls for Action," BNA Daily Report for Executives, December 18, 2013, http://dailyreport.bna.com/drpt/7010/split_display.adp?fedfid=39115494&vname=dernotallissues&wsn=506578000&searchid=21916298&doctypeid=1&type=date&mode=doc&split=0&scm=7010&pg=0.1843.

c11173008

"Data Centers and the Cloud, Part II: The Federal Government's Take on Optimizing New Information Technologies Opportunities to Save Taxpayers' Money," July 25, 2013[92]

Highlights

The hearing was held by the Committee on Oversight and Government Reform's Subcommittee on Government Operations to discuss the status of federal IT initiatives led by GSA and OMB. Members criticized GSA for "setting a bad example" as the leader of the FDCCI because the agency had only closed one data center during FY2013. Although Mr. McClure assured the members that GSA intended to close 38 centers before the end of the fiscal year, members remained skeptical.[93] Other issues discussed during the hearing included the status of FedRAMP,[94] anticipated cost savings expected through the FedRAMP process, management of software user licenses, the status of the major cloud migration initiatives within the federal government, the PortfolioStat[95] and TechStat[96] processes, and contract duplication.

Witnesses

- David L. McClure, Ph.D., Associate Administrator, Office of Citizen Services and Innovative Technologies, U.S. General Services Administration;
- The Honorable Steven VanRoekel, U.S. Chief Information Officer, Office of Management and Budget; and
- Mr. David Powner, Director, Information Technology Management Issues, U.S. Government Accountability Office.

[92] Hearing page: http://oversight.house.gov/hearing/data-centers-and-the-cloud-part-ii-the-federal-governments-take-on-optimizing-new-information-technologies-opportunities-to-save-taxpayers-money/.

[93] "GSA Slammed for Setting a Bad Example," *Federal Computer Week*, July 25, 2013, http://fcw.com/blogs/fcw-insider/2013/07/gsa-mcclure-mica-hearing.aspx.

[94] FedRAMP (the Federal Risk and Authorization Management Program) is a standardized approach to cloud security certification that will save the government money, time, and staff by eliminating redundant individual agency security assessments. GSA claims it will save an estimated $200,000 per authorization. FedRAMP is a critical part of OMB's cloud-first policy.

[95] Initiated in March 2012, the OMB PortfolioStat initiative is a tool that agencies use to make decisions on eliminating duplication and moving to shared solutions to maximize the return on IT investments across the enterprise. Through the PortfolioStat process, agencies are expected to develop a clearer picture of where duplication exists across their respective bureaus and components. This analysis should inform the budget process and help agency Deputy Secretaries eliminate waste and duplication within the IT portfolio. OMB projects PortfolioStat will save $2.5B through FY2015.

[96] TechStat Accountability Sessions (TechStats) are evidence-based reviews of each investment aimed at turning around or stopping troubled investments. In December 2010, OMB stated that these sessions resulted in $3 billion in reduced life-cycle costs and subsequently incorporated the TechStat model into its 25-point plan for reforming Federal IT management.

c11173008

"Data Centers and the Cloud: Is the Government Optimizing New Information Technologies to Save Taxpayers Money?" May 14, 2013[97]

Highlights

This hearing was held by the Committee on Oversight and Government Reform's Subcommittee on Government Operations to discuss the status of the status of FDCCI, including its relation to the federal government's migration to cloud services. The hearing coincided with the release of GAO's third report on the status of federal agency data center closures. In the report, GAO stated that "federal agencies have made some progress toward reaching the initiative's goal of closing 1,253 data center closures by 2015. Yet only $63 million in documented savings and cost avoidance would be achieved by the end of fiscal year 2013." The report also highlighted the lack of leadership from the three bodies charged with overseeing the initiative: OMB, GSA, and the FDCCI joint task force. Further, GAO found that

> [c]ost savings have not been tracked effectively because OMB, the agency responsible for tracking the initiative's goals, has not determined a consistent and repeatable method for doing so throughout the government, the report found. Of all 24 agencies that fall under FDCCI, only one—the Defense Department—has detailed any planned savings through the end of fiscal year 2014, and it expects to save $575 million. The other 23 agencies did not report any cost savings to GAO through FDCCI, and the initiative's recent integration to PortfolioStat in March further muddied the reporting waters.[98]

Witnesses

- Mr. David Powner, Director, Information Technology Management Issues, U.S. Government Accountability Office;
- Mr. Bernard Mazer, Chief Information Officer, U.S. Department of Interior;
- Mr. Kenyon Wells, Vice President of U.S. Federal, CGI Federal;
- Mr. Steve O'Keeffe, Founder, MeriTalk; and
- Ms. Teresa CarlsonVice President, World Wide Public Sector, Amazon Web Services.

"Time to Reform Information Technology Acquisition: The Federal IT Acquisition Reform Act," February 27, 2013[99]

Highlights

This hearing was held by the House Committee on Oversight and Government Reform to discuss issues related to the Federal IT Acquisition Reform Act (FITARA). FITARA addresses a number of IT acquisition issues, including cloud computing (and the related issue of data center consolidation). Discussion focused on the need to establish only one CIO in each agency who

[97] Hearing page: http://oversight.house.gov/hearing/data-centers-and-the-cloud-is-the-government-optimizing-new-information-technologies-to-save-taxpayers-money/.

[98] "GAO: Metrics, Leadership Leave Savings Unclear in Data Center Consolidation," *Federal Computer Week*, May, 14, 2013, http://fcw.com/articles/2013/05/14/data-center-hearing.aspx.

[99] Hearing page: http://oversight.house.gov/hearing/data-centers-and-the-cloud-is-the-government-optimizing-new-information-technologies-to-save-taxpayers-money/.

c11173008

would have "real authority to spend the money better and be accountable for that money," including the authority to cancel underperforming or failing projects. Representative Gerry Connolly gave several examples of "high-cost, low-performance IT programs that were not canceled quickly enough. The Air Force, for example, spent six years and $1 billion on an enterprise resource planning system that failed to deliver a usable product. 'Nearly 17 years after the enactment of the Clinger-Cohen Act, it is clear that agency [CIOs] often lack the necessary authority and resources to efficiently analyze, track, and evaluate the risks and results of major IT programs. We have to have somebody who has the authority and responsibility in each agency to manage these IT programs and investments.'"[100]

Witnesses

- Mr. Richard Spires, Chief Information Officer, Department of Homeland Security;
- Ms. Cristina Chaplain, Director, Acquisition and Sourcing Management, Government Accountability Office;
- The Honorable Daniel Gordon, Associate Dean for Government Procurement Law Studies at the George Washington University Law School, and Former Administrator, Office of Federal Procurement Policy, Office of Management and Budget;
- Mr. Stan Soloway, President and CEO, Professional Services Council; and
- Mr. Paul Misener, Vice President, Global Public Policy, Amazon.com.

"Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?" January 22, 2013[101]

Highlights

The hearing was held by the House Committee on Oversight and Government Reform to examine perceived problems with IT procurement and what could be done to rectify them. Representative Darrell Issa, the Committee Chairman, noted that "the U.S. government will spend nearly $80 billion on IT this year, making it the largest purchaser of such products on the planet, but a significant amount is wasted through duplication, unsuccessful implementations, and other problems." Throughout the hearing, Members "urged government officials to clamp down on bad IT contracts and limit duplication across projects, with an estimated one quarter of federal spending on IT wasted every year." Representative Issa noted further that "about three quarters of large federal IT programs are plagued with failures or cost overruns and about 47 percent of agencies' IT budgets go toward maintaining 'obsolete and deficient' resources." Members and witnesses proposed several ideas for reducing waste in federal IT contracts. For example, Tom Davis, a former Republican congressman, said that Congress should give agency CIOs more budget authority and agencies should provide more training for IT procurement officers.

[100] "Issa, Spires sketch visions for IT reform and CIO authority," Federal Computer Week, February 27, ,2013, http://fcw.com/articles/2013/02/27/spires-issa-cio.aspx.

[101] Hearing page: http://oversight.house.gov/hearing/wasting-information-technology-dollars-how-can-the-federal-government-reform-its-it-investment-strategy/.

c11173008

Chairman Issa and other committee members questioned why there were nearly 250 people with CIO titles in the U.S. government, inlcuding 40 just at the Department of Justice. Witnesses Davis and Steven VanRoekel, the federal government's top CIO, suggested the number of CIO titles wasn't as much of a problem as a lack of authority. They stated that many CIOs need to ask permission before they can move forward on innovative IT ideas.

Other issues discussed included OMB's attempts to improve the federal IT procurement process through the IT dashboard, which tracks projects and looks for those at risk, as well as how to address known deficiencies in the dashboard; how to address the perceived agency resistance to migrating their systems to the cloud, and the problem of spending too much money maintaining outdated or obsolete sytems.[102]

Witnesses

- Mr. Steven VanRoekel, Federal CIO, OMB;
- Mr. David Powner, Director, IT Management Issues, GAO;
- Mr. Douglas Bourgeois, Vice President, Chief Cloud Executive, VMware, Inc.;
- Mr. Michael Klayko, Advisor and Former CEO, Brocade Communications Systems, Inc.; and
- Mr. Chris Niehaus, Director, Office of Civic Innovation, Microsoft Corporation.

Implementation of the Federal Cloud Computing Initiative: Options for Oversight by Congress

The appropriate congressional committees may move to monitor the progress of the departments or agencies under their jurisdictions. They may do this by holding hearings; requesting review of an agency's status through either the agency itself or a GAO study; and/or assessing the department or agency's progress and projected goals against the stated goals of the FCCI.

Hearings

OMB oversees the management of the FCCI at the agency level. As such, it is the central point of information regarding the status of agency planning and implementation. More importantly, if OMB management practices are lacking in any way, the impact will be far reaching, potentially having a negative impact on the performance of all agencies as they implement their FCCI plans. Consistent congressional review of OMB's management practices could help detect and correct problems sooner than they might without such review. Committees may also wish to hold hearings to receive status reports directly from the CIOs of the agencies under their jurisdictions.

[102] "Lawmakers Look to Reduce Waste in US Government IT Contracts," CIO.gov, January 22, 2103, http://www.cio.com/article/727172/Lawmakers_Look_to_Reduce_Waste_in_US_Government_IT_Contracts.

c11173008

Review of Agency Cloud Computing Plans and Implementation Assessments

As plans to migrate to cloud services within the federal government are created and implemented, policymakers may choose to monitor how agencies are following federal directives and responding to GAO assessments. Such monitoring can be achieved through assessments conducted internally by the department or agency itself or externally by GAO or the committee of jurisdiction. A model for such internal assessments and reporting could be based on the FDCCI.

Review of External Status Reports

Congress may also request that GAO conduct regular reviews of agency FCCI progress. GAO reported on the status of the progress of the FCCI by selected agencies in its July 2012 report, but has not conducted any department or agency-specific reports. Such reports might be able to be produced more quickly and released as they are completed, rather than in one report containing the status of all the departments and agencies.

Further, Congress may monitor individual agencies' implementation of the FCCI by requiring them to address shortcomings identified in reports such as those produced by GAO.

Author Contact Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

Eric A. Fischer
Senior Specialist in Science and Technology
efischer@crs.loc.gov, 7-7071

c11173008