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

Updated August 14, 2015

Congressional Research Service
https://crsreports.congress.gov
R42887

CRS REPORT
Prepared for Members and
Committees of Congress

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.

Contents

Introduction 1
What Is Cloud Computing? 1
Characteristics of Cloud Computing 2
Deployment Models 2
Public 2
Private 3
Community 3
Hybrid 3
Deployment Model Comparison and Use by Federal Agencies 3
Service Models 4
Software as a Service (SaaS) 4
Platform as a Service (PaaS) 4
Infrastructure as a Service (IaaS) 4
Service Model Comparison 5
Service Model Use and Adoption by Federal Agencies 5
Considerations in Cloud Computing Adoption 5
Cost 6
Energy Efficiency 7
Availability 8
Agility 9
Security 9
The Federal Information Technology Acquisition Reform Act 11
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 14
Federal Cloud Computing Strategy 14
Federal Cloud Computing Strategy: Supporting and Complementary Initiatives, Programs, and Committees 16
Agency Cloud Adoption: Status 19
September 2014 Government Accountability Office Report 19
September 2014 InformationWeek Survey 19
Agency Cloud Adoption: Challenges 20
Agency Cloud Adoption: Drivers 20
Implementation of the Federal Cloud Computing Initiative: Options for Oversight by Congress 21
Hearings 21
Review of Agency Cloud Computing Plans and Implementation Assessments 22
Review of External Status Reports 22

Figures

Figure 1.Survey Results: Current and Target Cloud Adoption Percentages in Federal Agencies 5
Figure 2. Survey Results: Current and Target Cloud Adoption Percentages in Federal Agencies 13

Tables

Table 1. Agency CIO Responsibilities Under the 25-Point Plan 15

Contacts

Author Information 22

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:

> 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

[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.

> 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.

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.

[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.

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.

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

[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).

[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.

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.

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

[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.

wish, as they might otherwise do on desktop computers or local servers. The provider maintains the underlying cloud infrastructure.

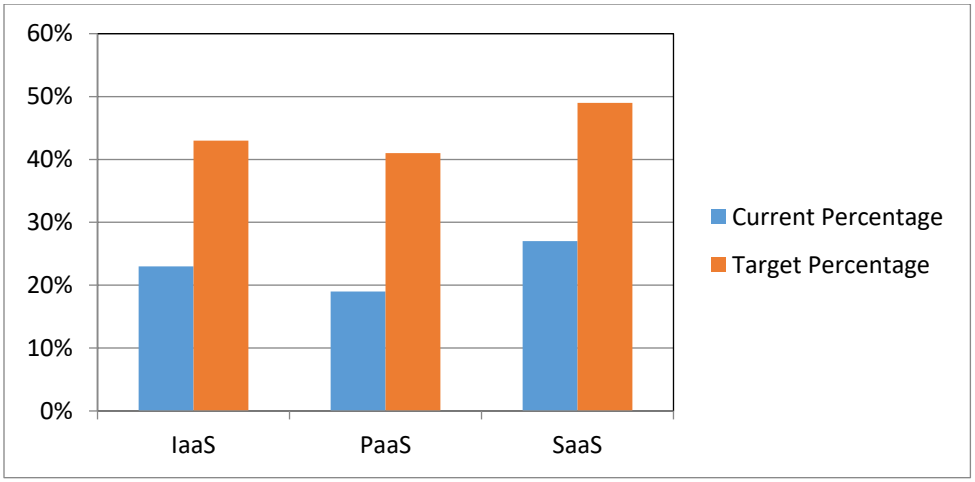
Service Model Comparison

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 and Adoption by Federal Agencies

According to a 2014 survey of 153 federal IT officials, the use of different deployment models within the government varies among the service models.[13] Additionally, the survey found that agencies were not transitioning to the cloud as quickly as they had anticipated.

Figure 1. Survey Results: Current and Target Cloud Adoption Percentages in Federal Agencies



Source: MeriTalk.

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] MeriTalk/NetApp, "Research Report: Cloud Computing," March 20, 2012, http://www.meritalk.com/cloud-control-register.php?. The survey was based on 153 responses. Job position: 9% CIO/CTO, 6% Deputy CIO/CTO, 33% IT Director/Supervisor, 12% IT Systems Engineer, 4% Software/Applications Development Manager, 11% Network Administrator, 5% Data Center Manager, and 20% Other IT Manager. Agency Type: 62% Federal Government Civilian Agency, 38% Federal Government DoD or Intel Agency. 100% of organizations have implemented cloud computing services as part of their IT strategy. 100% of respondents are familiar with their agency's use of or plans for cloud computing. The report has a margin of error of ± 7.89 at a 95% confidence level.

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. 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.[14] Another potential financial benefit of cloud computing is the savings that cloud providers may realize from locating facilities in areas with lower-than-average energy and labor costs.[15]

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 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,[16] and whether the resources will need to be modified.[17] 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.

[14] 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.

[15] Ibid.

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

[17] 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.

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.[18]

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%.[19] 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.[20] 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.[21]

Energy Efficiency

Computers, servers, and related devices require large amounts of energy to manufacture,[22] and they account for a growing share of world energy consumption.[23] "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.[24] Google has projected that a small

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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-

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.[25]

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.[26]

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.[27] 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 be more expensive and no more efficient, in part because of the special needs associated with scientific computing.[28]

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.

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.

---

inherently-green-33331.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

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.[29] 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,[30] and some other countries have devoted resources to facilitate ubiquitous access to high speed Internet.[31]

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*.[32] If a user wishes to switch to a new 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.[33]

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.

---

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

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

[31] 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.

[32] 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).

[33] 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.

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.[34] 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.[35] 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.[36] With 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.[37]

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.[38] 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

[34] 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.

[35] 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.

[36] 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/security/229700151).

[37] 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.

[38] 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.

for privacy and auditability.[39] Within the United States, different federal laws apply to different kinds of data, for example health and financial information. State requirements also vary.[40]

The Federal Information Technology Acquisition Reform Act

In December 2014, the Federal Information Technology Acquisition Reform Act (FITARA) was signed into law (P.L. 113-291). The law is intended to improve and streamline the federal IT acquisition process. With respect to cloud computing, as well as data center consolidation, FITARA requires agencies to adhere to federal guidelines, including applicable FedRAMP provisions and other guidance published by the National Institute of Standards and Technology.[41]

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.[42] 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 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).[43]

[39] 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.

[40] 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/.

[41] Section 834 of the FY2015 National Defense Authorization Act, https://www.congress.gov/bill/113th-congress/house-bill/3979/text/pl. See also H. Rept. 113-360, http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT92738/pdf/CPRT-113HPRT92738.pdf.

[42] 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).

[43] 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.

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.[44] 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)[45] governs the privacy of electronic communications.[46] 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 protections available under ECPA for the wide range of cloud computing activities.[47] 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.

---

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

[45] 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.

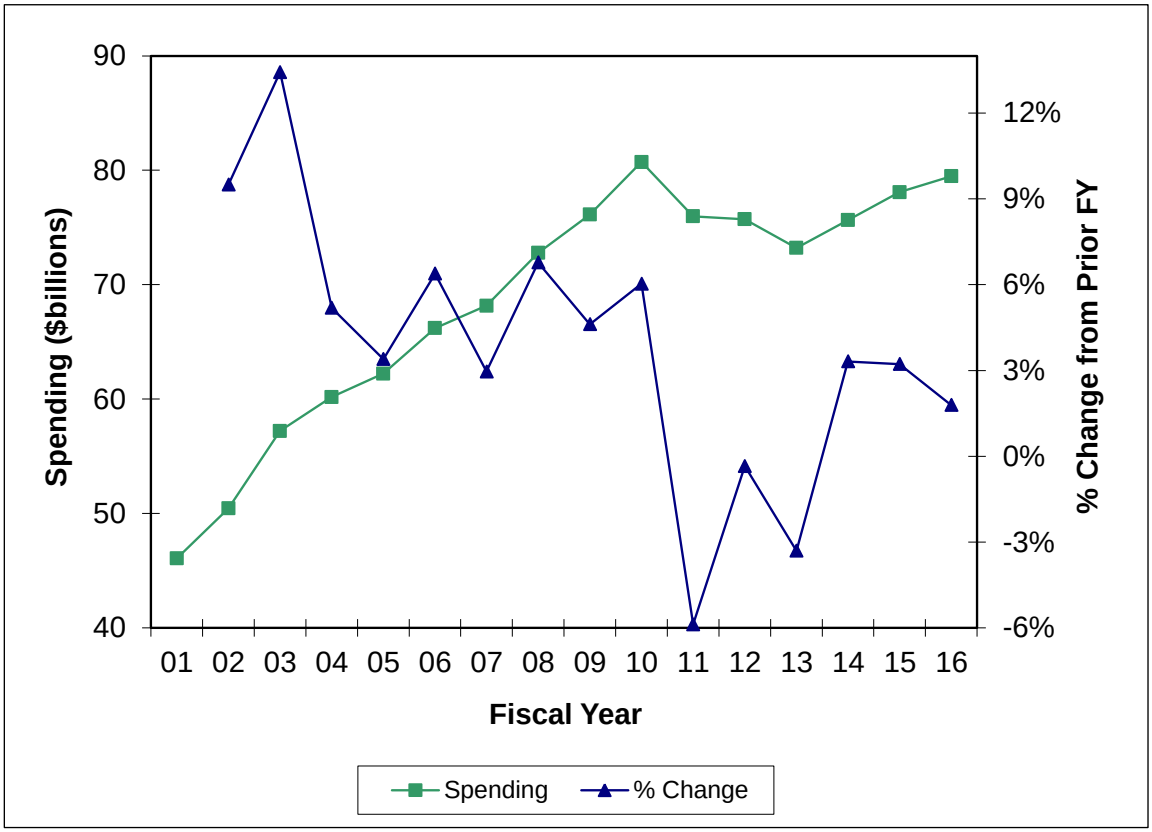
[46] See also CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle; CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle; and *Cloud and Mobile Privacy: The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

[47] 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.

Trends in Total Federal Investment in Information Technology

The FY2016 planned IT spending is estimated to be $86.4 billion. Annual federal investment in information technology increased at 7.1% annually between 2001 and 2009. Since that time, that growth has slowed to 1.5%.[48] Total annual spending from FY2001 to FY2016, along with the percent difference from the previous year is shown in **Figure 2**.

Figure 2. Survey Results: Current and Target Cloud Adoption Percentages in Federal Agencies



Source: Spreadsheets on federal IT spending for Fiscal Years (FY) 2003-2016, available at Office of Management and Budget, "Federal IT Dashboard, 2016 Edition," August 13, 2015, https://itdashboard.gov/.

Note: Data are for actual expenditures, except FY2015 (enacted) and FY2016 (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 FY2016 in the OMB spreadsheet is $79.5 billion, whereas that in the FY2016 budget request was $86.4 billion. (Office of Management

[48] 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).

and Budget, "Fiscal Year 2016 Analytical Perspectives of the U.S. Government," January 26, 2015, p. 281, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/spec.pdf).

Federal Planning and Activity

The Federal Cloud Computing Initiative (FCCI) was announced in September 2009[49] to implement cloud computing within the federal government and improve operational efficiencies, optimize common services across organizations, and enable more government transparency.[50] 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.

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"[51] 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").[52] To implement that policy, the Administration developed the Federal Cloud Computing Strategy (FCCS).[53] The strategy describes the—

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

[49] 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/.

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

[51] 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")

[52] 25-Point Plan, pp. 6-8.

[53] 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")

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.

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.[54]

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.[55]

Federal Data Center Consolidation Initiative[56]

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.[57] 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.

Since its inception, the FDCCI had been intended to be one part of a larger effort to curb waste and inefficiency in federal IT spending. To achieve that goal, OMB formally rolled the FDCCI into the PortfolioStat program in FY2013 (PortfolioStat is described on p. 18.). This move was aimed at allowing data center inventories to be categorized with more specificity, including the capability of differentiating data center optimization activity from data center consolidation activity.

Federal Risk and Authorization Management Program[58]

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 became 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 goals of FedRAMP are to—

- ensure that cloud-based services have adequate information security;

[54] "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")

[55] 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/).

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

[57] 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.

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

- 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 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[59]

The TechStat initiative, managed by OMB, is intended to provide evidence-based reviews—conducted between OMB and agency leadership—of agency IT investments, including plans to migrate to cloud services. Sessions are face-to-face meetings intended to determine whether IT investments that are failing or are not producing results should be terminated or could be saved. These meetings involve OMB and agency leadership and are intended to increase accountability and transparency, and improve performance.

The federal CIO began leading TechStat sessions in January 2010 and OMB reported that federal agencies achieved over $3 billion in cost savings or avoidances as a result of these sessions in 2010. Subsequently, OMB delegated to agency CIOs the responsibility to hold TechStat sessions within their respective agencies.

However, GAO reported that as of March 2015, OMB has not conducted any TechStat reviews (the last TechStat was held in March 2013). Further, GAO found that OMB has not listed any savings from TechStats in any of its required quarterly reporting to Congress since June 2012. OMB had reported conducting TechStats at 23 federal agencies covering 55 investments, 30 of which were considered medium or high risk. However, these reviews accounted for less than 20% of medium- or high-risk investments government-wide.[60]

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

[60] "Additional Actions and Oversight Urgently Needed to Reduce Waste and Improve Performance in Acquisitions and Operations," Statement of David A. Powner, Director, Information Technology Management Issues, Office of Management and Budget, Testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives, June 10, 2015, GAO-15-675T, http://www.gao.gov/assets/680/670745.pdf.

Apps.gov[61]

Apps.gov is a GSA program 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.[62] 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[63]

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.[64] 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.

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[65] 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[66]

PortfolioStat, managed by OMB, requires agencies to review IT spending in six areas: collaboration, unified communications, enterprise content management, search, reporting and analysis, and content creation. However, since the program's inception, federal agencies have significantly reduced the amount of planned projected savings on IT investment. Agencies were supposed to save $5.8 billion between fiscal years 2013 and 2015, but have since reduced that amount to $2 billion, a 68 percent decrease. The DoD and DHS accounted for most of the

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

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

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

[64] 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.

[65] 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.

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

difference. DoD reduced its planned savings by about $2.6 billion, to about $561 million, and DHS reduced its planned savings by about $925 million, to about $447 million.[67]

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.[68]

September 2014 Government Accountability Office Report

In September 2014, the Government Accountability Office (GAO) reported to the Senate on its findings concerning the Office of Management and Budget's (OMB's) "Cloud First" policy.[69] For this report, GAO examined the status of cloud adoption at seven agencies: Agriculture, Health and Human Services, Homeland Security, State, and the Treasury; and the Administrators of the General Services Administration and Small Business Administration.

Since the last examination in 2012, the number of cloud services implemented by the agencies increased by 80 services, from 21 to 101. The agencies also increased their cloud expenditures by $222 million, from $307 million to $529 million and increased the percentage of their IT budgets allocated to cloud services; however, this amounted to an increase of only 1%. In all, the agencies reported cost savings of about $96 million from the implementation of 22 of the 101 cloud services. These savings included both one-time and multiyear savings.

For all the agencies, GAO recommended that to ensure continued progress in the implementation of cloud computing services, they—

- ensure that all IT investments are assessed for suitability for migration to a cloud computing service; and
- establish evaluation dates for those investments identified in this report that have not been assessed for migration to the cloud.

September 2014 InformationWeek Survey

In addition to the September 2014 GAO report,[70] that same month, InformationWeek surveyed 153 federal government IT executives closely involved in their agencies' cloud deployments.[71] Some of the findings were:

- Only 44% of agencies have "mature" data governance practices in the cloud and agencies continue to manage 71% of data themselves, whereas cloud vendors manage just 29%.

[67] "Fed Agencies Reduce Planned PortfolioStat Savings as GAO Questions Past IT Reform Savings," FierceGovernemtIT.com, April 20, 2015, http://www.fiercegovernmentit.com/story/fed-agencies-reduce-planned-portfoliostat-savings-gao-questions-past-it-ref/2015-04-20.

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

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

[70] Cloud Computing: Additional Opportunities and Savings Need to Be Pursued, GAO, September 2014, http://www.gao.gov/assets/670/666133.pdf.

[71] 2014 Federal Government Cloud Computing Survey, "Cloud Control: Moving to the Comfort Zone," InformationWeek, September 11, 2014. ("2014 InformationWeek Survey")

- Security was stated as a concern, with only one in five respondents completely confident in her cloud vendor's security.
- Only a third of agencies have complied with the Federal Risk and Authorization Management Program (FedRAMP), but 9 out of 10 are taking steps to manage trust with their cloud vendors, such as keeping security functions on premise (42%) and requiring certification of security measures (41%).
- Agencies that were actively improving their data governance programs were more likely to be comfortable with turning their IT services over to cloud vendors. At this time, 56% of agencies are currently implementing data stewardship or a more formal data governance program for cloud services/vendors. More than half (55%) of those surveyed said cloud computing will make data management easier.
- The respondents largely believe that the cloud will deliver tighter security with quicker access to information, support of virtual staff, access from any location, and easier configuration management, among other benefits.

Agency Cloud Adoption: Challenges

There are a number of reasons cloud adoption is not occurring more rapidly. In its 2014 study, GAO found five challenges in implementing cloud services. Two, meeting federal security requirements and overcoming cultural barriers within agencies, remained from the 2012 study, and three new challenges also emerged: meeting new network infrastructure requirements; having appropriate expertise for acquisition processes; and funding for implementation.

- **Meeting federal security requirements.** Meeting these requirements was a continuing challenge because the requirements for new services are a moving target, meaning the requirements are regularly being updated to address new threats, vulnerabilities, and technologies. Vendors may not be able to meet those standards.
- **Overcoming cultural barriers within agencies.** Shifting to a new business model from a legacy model requires cultural change, which continues to be a challenge at many agencies.
- **Meeting new network infrastructure requirements.** Current network infrastructure and configuration and bandwidth (data transmission rate) is often not adequate to meet new needs when agencies transition to cloud services.
- **Having appropriate expertise for acquisition processes.** Migrating legacy systems to cloud services requires a knowledgeable acquisition staff and appropriate processes.
- **Funding for implementation.** Funding for the initial implementation of a cloud service can be a significant cost to agencies.

Agency Cloud Adoption: Drivers

The two main drivers of cloud adoption by federal agencies continue to be 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.[72] 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.[73] 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 FDCCI[74] 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.[75] 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.

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.

[72] 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%).

[73] "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.

[74] 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.")

[75] 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.

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 September 2014 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 Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Eric A. Fischer
Senior Specialist in Science and Technology

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.