Congressional Research Service
Informing the legislative debate since 1914

Cloud Computing: Background, Status of Adoption by Federal Agencies, and Congressional Activities

December 12, 2019

Congressional Research Service
https://crsreports.congress.gov
R46119

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46119

December 12, 2019

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Cloud Computing: Background, Status of Adoption by Federal Agencies, and Congressional Activities

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. 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.

As cloud computing has developed, varied and sometimes nebulous descriptions of what it is and what it is not have been commonplace. Such ambiguity can create uncertainties that may impede innovation and adoption. The National Institute of Standards and Technology (NIST) has developed standardized language describing cloud computing to help clear up that ambiguity:

> 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.

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 achieve two goals: reduce the total investment by the federal government in information technology (IT), which currently stands at about $90 billion each year, and realize other stated advantages of cloud adoption: efficiency, accessibility, collaboration, rapidity of innovation, reliability, and security. However, challenges remain as agencies shift to cloud services. According to a survey conducted in September 2018, federal IT managers expressed concerns about security in certain cloud environments, the complexity of migrating existing ("legacy") applications to the cloud, a lack of skilled staff to manage certain cloud environments, and uncertain funding.

Planning for cloud adoption by federal agencies began with the 2010 publication of "A 25-Point Implementation Plan to Reform Federal IT Management." More recently, in the 2017 "Report to the President on Federal IT Modernization," the Office of Management and Budget (OMB) pledged to update the government's legacy Federal Cloud Computing Strategy ("Cloud First"). Fulfilling this requirement, the Administration developed a new strategy, Cloud Smart, which was published on September 24, 2018. The new strategy is founded on what the Administration considers the three key pillars of successful cloud adoption: security, procurement, and workforce.

In the 116th Congress, there has been one cloud-related bill introduced and one cloud-related hearing held. The Federal Risk and Authorization Management Program (FedRAMP) Authorization Act (H.R. 3941) was introduced on July 24, 2019, by Representative Gerald Connolly. The bill would formally establish within the General Services Administration a risk management, authorization, and continuous monitoring process to "leverage cloud computing services using a risk-based approach consistent with the Federal Information Security Modernization Act of 2014." On July 17, 2019, the House Committee on Government Reform Subcommittee on Government Operations held a hearing, "To the Cloud! The Cloudy Role of FedRAMP in IT Modernization." The purpose of the hearing was to examine the extent to which FedRAMP has reduced duplicative efforts, inconsistencies, and cost inefficiencies associated with the cloud security authorization process.

Contents

Introduction 1
What Is Cloud Computing? 1
Characteristics of Cloud Computing 2
Deployment Models 2
Public 3
Private 3
Community 3
Hybrid 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
Federal Agency Cloud Adoption 5
The Cloud Smart Strategy 6
2019 GAO Report 8
Congressional Activity 9
116th Congress: Legislation 9
116th Congress: Hearings 9
Options for Congress 9
Hearings 9
Review of Agency Cloud Computing Plans and Implementation Assessments 11
Review of External Status Reports 11

Tables

Table 1. Completed Cloud Smart Actions 6
Table 2. Uncompleted Cloud Smart Actions 7

Contacts

Author Information 11

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 achieve two goals: reduce the total investment by the federal government in information technology (IT), which currently stands at about $90 billion each year,[1] and realize other stated advantages of cloud adoption, including efficiency, accessibility, collaboration, reliability, and security.[2] However, challenges remain as agencies shift to cloud services. According to a survey conducted in September 2018, federal IT managers continue to express long-held concerns about security in certain cloud environments, the complexity of migrating existing ("legacy") applications to the cloud, a lack of skilled staff to manage certain cloud environments, and uncertain funding.[3]

This report explains what cloud computing is, including different models for cloud deployment and services, and describes the federal government's planning for IT reform. It also provides information on assessments that have been conducted on agency cloud adoption. Finally, the report provides a summary of recent congressional action and presents some 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. Cloud computing services are delivered through a network, usually the internet. Some analysts see this approach as analogous to the networked delivery of electricity, water, and other utilities through the electric grid, water delivery systems, and other distribution infrastructure.[4] In some ways, cloud computing is reminiscent of computing before the advent of the personal computer, when 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 nearly ubiquitous.

Cloud computing differs from local computing, in which local machines perform most tasks and store the relevant data. Some cloud services are adaptations of familiar applications, such as email and word processing. Others are new services that never existed as a local application, such as social networks.

As cloud computing has developed, varied and sometimes nebulous descriptions of what it is and what it is not have been commonplace. Such ambiguity can create uncertainties that may impede innovation and adoption. The National Institute of Standards and Technology (NIST) has developed standardized language describing cloud computing to help clear up that ambiguity:

---

[1] Government Accountability Office, "Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked," April 2019, https://www.gao.gov/products/GAO-19-58. Hereinafter, "*Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked.*"

[2] IBM, "Benefits of Cloud Computing," undated, https://www.ibm.com/cloud/learn/benefits-of-cloud-computing.

[3] "Federal Cloud Readiness Report," FedScoop, January 2019, https://www.fedscoop.com/download-research-study-federal-cloud-readiness-report/.

[4] 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.

> 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.[5]

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, described below.

Characteristics of Cloud Computing[6]

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. An analogy is that a television viewer or radio listener can change stations at will.
- *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 is that homeowners and businesses do not need to know which specific power plants generated the electricity they are using [although some do care, and specifically buy power from "green" sources].
- *Rapid elasticity:* Users can quickly increase or decrease their use of a computing resource in response to their immediate needs. An analogy is that electricity customers can use as little or as much power 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 the metered use of electricity, water, natural gas, and other utilities.

Deployment Models[7]

NIST has identified four standard models, or types, of cloud computing that can be implemented to satisfy the 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. An extensive list of deployment model adoption by federal agencies is in the April 2019 report by the Government Accountability Office, *Cloud*

[5] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[6] *The NIST Definition of Cloud Computing.*

[7] *The NIST Definition of Cloud Computing.*

Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked.[8]

Public

In *public cloud* (sometimes called *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 these 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[9] and web-based media services.[10] Public clouds may have price and flexibility advantages over other deployment models, but security and other concerns could restrict federal use. The public cloud deployment model is used predominantly by businesses with low privacy concerns.

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. It is a cloud used by a company itself—rather than its customers. Private clouds may provide services that are similar to those provided by public cloud providers, but potentially with fewer 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. Just like private cloud, community cloud is technically no different from public cloud. The only difference is who is allowed to use it.

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

---

[8] *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*. See specifically, Appendix V, "Description of Cloud Computing Investments Provided by Selected Agencies for Fiscal Year 2018." The 16 agencies were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Justice, Labor, State, Treasury, Transportation, and Veterans Affairs, the General Services Administration, the Small Business Administration, and the Social Security Administration.

[9] Examples include Dropbox (https://www.dropbox.com), Microsoft OneDrive (https://onedrive.live.com), Apple iCloud (https://www.apple.com/icloud), and Google Drive (https://drive.google.com).

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

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. By combining different deployment models, users can choose the right balance for their organization between legal compliance, security, and scalability.

Service Models[11]

Cloud computing can provide various kinds of services, ranging from basic computing tasks to the provision of sophisticated applications. While these services can be categorized in different ways, the NIST definition uses three basic *service models,* described below.[12]

Software as a Service (SaaS)

In the SaaS[13] 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 and simplest service model to the end user. In many cases, SaaS applications are accessible through hardware or software "thin clients."[14] Examples include web-based services such as Google Apps and online storage such as DropBox.

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. Facebook is one example of such an application.[15] 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 desire, as they might otherwise do on desktop computers or local servers. The provider maintains

[11] *The NIST Definition of Cloud Computing*. The generic term for cloud service models is *X*aaS. While the three described in this section 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 both SaaS and IaaS.

[12] 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.

[13] SaaS is sometimes called *Applications as a Service.*

[14] 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 communicate with 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.

[15] "Demystifying SaaS, PaaS, and IaaS," Skytap, November 28, 2017, https://www.skytap.com/blog/demystifying-saas-paas-and-iaas/.

the underlying cloud infrastructure. Examples of IaaS are Amazon Web Services and Microsoft Azure.

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 *software* is needed. By providing these infrastructure, platform, and software services remotely, a cloud provider frees its customers from having to provide local infrastructure and support. In the case of IaaS, the user need not have a local workstation, using instead a thin client with minimal need for computing power.

Federal Agency Cloud Adoption[16]

Planning for cloud adoption by federal agencies began with the 2010 publication by the Federal Chief Information Officer (CIO) of "A 25-Point Implementation Plan to Reform Federal IT Management."[17] The reforms put forth in the plan were focused on eliminating barriers that were impeding effective management of IT programs throughout the federal government. In the plan, the Federal CIO recognized that too many past federal IT projects had run over budget, fallen behind schedule, or failed to deliver promised functionality. The plan stated that the federal government would shift to a "Cloud First" strategy, which it stated would be more economical, faster, and more flexible.

Increased cloud adoption is also a stated goal of the Federal Information Technology Acquisition Reform Act (FITARA), enacted on December 19, 2014.[18] Among other provisions, FITARA required the Federal CIO, in conjunction with federal agencies, to refocus the Federal Data Center Consolidation Initiative (FDCCI) to include adoption of cloud services.[19] The FDCCI was superseded by the Data Center Optimization Initiative (DCOI) in August 2016.[20]

In the 2017 "Report to the President on Federal IT Modernization,"[21] the Office of Management and Budget (OMB) pledged to update the federal government's legacy Federal Cloud Computing

[16] One of the most notable recent federal cloud contracts has been for the Department of Defense (DOD) Joint Enterprise Defense Infrastructure (JEDI). JEDI is intended to be a DOD-wide system capable of supporting Unclassified, Secret, and Top Secret requirements. It has also proven to be quite controversial. Additional information about JEDI can be found in CRS Report R45847, *The Department of Defense's JEDI Cloud Program*, by Heidi M. Peters, CRS In Focus IF11264, *DOD's Cloud Strategy and the JEDI Cloud Procurement*, by Heidi M. Peters, and CRS Insight IN11203, *Amazon Protest of the Department of Defense's JEDI Cloud Contract Award to Microsoft*, by Heidi M. Peters.

[17] Vivek Kundra, U.S. Chief Information Officer, *A 25-Point Implementation Plan to Reform Federal IT Management*, December 9, 2010, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/25-point-implementation-plan-to-reform-federal-it.pdf. ("25-Point Plan").

[18] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, P.L. 113-291.

[19] For additional information about FITARA, see CRS Report R44462, *The Federal Information Technology Acquisition Reform Act (FITARA): Frequently Asked Questions*, by Patricia Moloney Figliola.

[20] Memorandum For Heads Of Executive Departments And Agencies: Data Center Optimization Initiative (M-16-19), Office of the U.S. Chief Information Officer, August 1, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_19_1.pdf.

[21] Report to the President on Federal IT Modernization, Office of Management and Budget, December 13, 2017, https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf ("Federal IT Modernization Report").

Strategy ("Cloud First"). Fulfilling this requirement, the Administration developed a new strategy, Cloud Smart, published as a draft on September 24, 2018.

The DCOI was updated in June 2019.[22] Among other requirements, the updated DCOI placed a freeze on funds or resources to build new agency-owned data centers or significantly expand existing agency-owned data centers without approval from OMB. It also requires agencies to evaluate options for the consolidation and closure of existing data centers, in alignment with the Cloud Smart Strategy.

The Cloud Smart Strategy

On June 24, 2019, the Federal CIO issued the Cloud Smart Strategy[23] to provide agencies with practical implementation guidance to achieve the potential of cloud-based technologies. The new strategy is founded on three pillars:

- Security: Modernize security policies to focus on risk-based decisionmaking, automation, and moving protections closer to data.
- Procurement: Improve the ability of agencies to purchase cloud solutions through repeatable practices and sharing knowledge.
- Workforce: Upskill, retrain, and recruit key talent for cybersecurity, acquisition, and cloud engineering.

Across these areas, the strategy identifies 22 "action items" to be completed not later than December 2020. As of November 2019, over half had been completed. (See **Table 1** and **Table 2**.)[24]

Table 1. Completed Cloud Smart Actions

The Chief Information Officer (CIO) Council, Office of Management and Budget (OMB), and General Services Administration (GSA) will work together to consolidate information into a central location to share guidance and best practices on cloud topics. (Action 1)[a]	The CIO Council will work with OMB, GSA, and agency and industry experts to develop methods to optimize agency use of cloud services. (Action 2)[b]
OMB will release updated policy on infrastructure optimization, in alignment with Cloud Smart. This will update the Data Center Optimization Initiative established in M-16-19. (Action 3)[c]	OMB will publish an updated Identity, Credential, and Access Management Policy. (Action 5)[d]
OMB will work with GSA to expedite the authorization of low risk Software-as-a-Service offerings through the effective implementation of Federal Risk and Authorization Management Program Tailored. (Action 7)[e]	OMB, in coordination with GSA, will develop a Strategic Plan to evolve the Authorization to Operate process. (Action 8)[f]
OMB will work with GSA and the CIO Council to create a first-of-its kind view of agency requirements across the federal security enterprise. (Action 9, Ongoing)[f]	The Information Technology Category Manager (ITCM) and Cloud Solutions Category Team (CSCT) will work with OMB to contribute to the portal in Action 1. (Action 10)[a]

[22] Memorandum for Heads of Executive Departments and Agencies: Update to Data Center Optimization Initiative, (M-19-19), Office of the U.S. Chief Information Officer, June 25, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-19-Data-Centers.pdf.

[23] https://cloud.cio.gov/strategy/.

[24] https://cloud.cio.gov/strategy/actions/.

The GSA CSCT will implement supplier-relationship management through active engagement with industry partners. (Action 11)[g]	The government-wide ITCM at GSA will establish a government-wide CSCT. (Action 12)[g]
OMB will provide direction to agencies to improve the security and visibility for systems and data managed in the cloud. (Action 15)[h]	Each agency CIO and Chief Human Capital Officer (CHCO) must identify two position or skill segment priorities and incorporate them into to the agency's Human Capital Operating Plan. (Action 17)[i]
OMB, supported by OPM, will consider positions affected by cloud migration as part of the strategic workforce planning efforts laid out in the President's Management Agenda. (Action 18)[j]	The CIO Council and the CHC Council will jointly develop and execute on strategies and initiatives that expand the use of career fairs, national hiring events, etc. (Action 20)[k]

Source: Cloud Smart Initiative, Office of the U.S. Chief Information Officer, June 24, 2019, https://cloud.cio.gov/strategy/.

a. https://hallways.cap.gsa.gov/app/#/gateway/cloud-information-center.
b. https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf.
c. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-19-Data-Centers.pdf.
d. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.
e. https://tailored.fedramp.gov/.
f. The CIO Council has created an Authorization to Operate Working Group to further improve the process.
g. https://gsa.gov/cloud.
h. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf.
i. Refer to each agency's Human Capital Operating Plan for specific implementation details.
j. https://www.challenge.gov/challenge/gear-center-challenge/.
k. https://www.cio.gov/reskilling.

Table 2. Uncompleted Cloud Smart Actions

The Office of Management and Budget (OMB) will work with General Services Administration (GSA), Chief Information Officer (CIO) Council, and Department of Homeland Security to update the Trusted Internet Connection Policy to ensure program objectives can be achieved. (Action 4)	OMB will release updated guidance that focuses on accelerating the implementation of the Continuous Diagnostics and Mitigation program across the Government. (Action 6)
The Cloud Solutions Category Team will evaluate and recommend government-wide contract vehicles for cloud services based on a thorough evaluation of each contract. (Action 13)	OMB and GSA will create or leverage existing, cross-government working groups to identify agency Service Level Agreements not addressed by existing commercial industry offerings specific to unique government requirements. (Action 14)
The Office of Personnel Management (OPM), with support from the OMB and the Department of Homeland Security, will identify critical skill gaps across the federal enterprise. (Action 16)	OMB, in coordination with the Federal Acquisition Institute, will continue to conduct its biennial acquisition workforce competency survey to identify skill and talent gaps within the acquisition workforce. (Action 19)
OMB, in collaboration with OPM, will work with agencies that have managed successful migration efforts to collect a set of best practices and strategies for effective employee communication, engagement, and transition. (Action 21)	OMB, CIO Council, and Chief Human Capital Officers Council, will develop a market-informed pay and compensation strategy. (Action 22)

Source: Cloud Smart Initiative, Office of the U.S. Chief Information Officer, June 24, 2019, https://cloud.cio.gov/strategy/.

2019 GAO Report

In April 2019, the Government Accountability Office (GAO) published a report examining the status of cloud adoption at 16 agencies.[25] GAO found that 10 of the agencies reported increasing their use of cloud services from FY2016 through FY2019. All 16 agencies had made progress in implementing cloud services, meaning they had established assessment guidance, performed assessments, and implemented services, but the extent of their progress varied. For example, not all had followed OMB guidance that directs agencies to review all IT investments for compatibility with cloud services. GAO also found that

- 16 agencies reported an increase in their cloud service spending since 2015.
- 13 of the 16 agencies saved a total of $291 million to date from using cloud services.
- 15 of the 16 agencies identified significant benefits from acquiring cloud services, including improved customer service and the acquisition of more cost-effective options for managing IT services.
- 15 of the 16 agencies identified nine cloud investments that enhanced the availability of weather-related information; facilitated collaboration and information sharing among federal, state, and local agencies related to homeland security; and provided benefits information to veterans.

In collecting the information requested by GAO, agency CIOs identified the following challenges:

- Spending data were not consistently tracked.
- Different methods were used to calculate cloud spending costs.
- Interpreting changes in OMB and related guidance created confusion regarding what spending data should be tracked.

As a result of these challenges, GAO concluded that agency-reported cloud spending and savings figures were likely underreported.

GAO made one recommendation to OMB on cloud savings reporting, and 34 recommendations to the 16 agencies on cloud assessments and savings. To OMB, GAO recommended that agencies be required to explicitly report, at least on a quarterly basis, the savings and cost avoidance associated with cloud computing investments. The 34 recommendations to the agencies included directing CIOs to

- establish guidance to assess new and existing IT investments for suitability for cloud computing services;
- complete an assessment of existing IT investments for suitability for migration to a cloud computing service; and
- establish a consistent and repeatable mechanism to track savings and cost avoidances from the migration and deployment of cloud services.

[25] *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*.

Congressional Activity

Congress has conducted ongoing oversight of IT acquisitions, including cloud computing activity, for many years. This section summarizes cloud-related legislation and hearings in the 116th Congress and presents some options for future congressional oversight.

116th Congress: Legislation

The Federal Risk and Authorization Management Program (FedRAMP)[26] Authorization Act (H.R. 3941),[27] introduced on July 24, 2019, by Representative Gerald Connolly, would establish a risk management, authorization, and continuous monitoring process to "leverage cloud computing services using a risk-based approach consistent with the Federal Information Security Modernization Act of 2014."[28]

116th Congress: Hearings

Since November 2015, a year after FITARA became law, the House Committee on Oversight and Reform has held two FITARA oversight hearings per year. On July 17, 2019, the committee's Subcommittee on Government Operations held a hearing titled "To the Cloud! The Cloudy Role of FedRAMP in IT Modernization."[29] The purpose of the hearing was to examine the extent to which FedRAMP has reduced duplicative efforts, inconsistencies, and cost inefficiencies associated with the cloud security authorization process.

In addition, the committee's Subcommittees on Information Technology and Government Operations held a FITARA "Scorecard" hearing on June 26, 2019.[30] That hearing was not focused specifically on cloud computing, but it examined related issues, such as whether OMB policies are in compliance with FITARA and the cost savings that could be realized through data center consolidation.

Options for Congress

As Congress monitors the progress of federal departments and agencies in implementing cloud computing, its options for ongoing oversight include holding hearings; requesting review of an agency's status by either the agency itself or the GAO; and assessing the agency's progress and projected goals against the stated goals of the Cloud Smart Strategy.

Hearings

Committees might choose to focus hearings on OMB, which oversees the management of the Cloud Smart Strategy at the agency level. This role makes OMB the central point of information

[26] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[27] https://www.congress.gov/bill/116th-congress/house-bill/3941/.

[28] The Federal Information Security Management Act (FISMA) defines a comprehensive framework to protect government information, operations, and assets against natural or manmade threats. It was enacted as Title III of the E-Government Act of 2002 (P.L. 107-347).

[29] https://oversight.house.gov/legislation/hearings/to-the-cloud-the-cloudy-role-of-fedramp-in-it-modernization.

[30] https://oversight.house.gov/legislation/hearings/fitara-80.

regarding the status of agency planning and implementation. If OMB management practices for cloud computing are lacking, the impact could potentially affect the performance of all agencies.

Consistent congressional review of OMB's management practices with respect to the Cloud Smart Strategy could help to detect and correct problems in a timely manner.

Alternatively, or in addition, committees might choose to hold hearings to receive status reports directly from the CIOs of particular agencies under their jurisdictions.

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 could be achieved through assessments conducted internally by a department or agency itself, externally by GAO, or directly by a committee of jurisdiction. A model for internal assessments and reporting could be based on progress made on the uncompleted items of the Cloud Smart Strategy.

Review of External Status Reports

GAO conducts status reports on cloud adoption across the federal agencies, such as the April 2019 report discussed above, but it has not issued separate reports focused on the status of individual departments or agencies.

When examining shortcomings in individual agencies' implementation of the Cloud Smart Strategy, as identified by GAO, Congress might consider requesting follow-up reviews focused on particular challenges.

Author Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

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.