The Heritage Foundation
LEADERSHIP FOR AMERICA

BACKGROUNDER

No. 2705 | JUNE 27, 2012

Getting Cyber Serious: Mastering the Challenges of Federal Cloud Computing

Steven P. Bucci, PhD

Abstract

The federal government could realize significant savings by migrating many information technology functions to the cloud. While the government should take full advantage of the advantages of cloud computing, it should take care to avoid common cloud computing pitfalls. Congress and the Administration also need to update the laws on cybersecurity, privacy, and information, which have become outdated.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2705**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Cloud computing is an emerging idea that seeks to replace the large databases and servers maintained by many companies and government agencies with Internet-based solutions. The private sector has increasingly adopted this idea, and the federal government has shown interest because of potential cost savings and security benefits.

With potential savings of more than $10 billion in information technology (IT) budgets, it was inevitable that the Obama Administration would pursue cloud computing for the federal government. However, Congress and the Administration should move forward carefully and deliberately to avoid potential pitfalls. If done correctly, federal migration to cloud computing offers streamlined efficiency that would make better use of U.S. tax dollars.

What Is Cloud Computing?

Cloud computing is described as "a broad movement to treat information technology (IT) services as a commodity with the ability to dramatically increase or decrease capacity to match usage needs."[1] Essentially, cloud computing is the movement of IT capabilities away from individual computers and servers to centralized providers that

Key Points

- Cloud computing offers a compelling and effective means of reducing federal information technology (IT) infrastructure costs while providing additional benefits such as scalability, increased security, and improved access to innovation.
- Moving some government services to cloud computing could save more than $10 billion in federal IT costs and assist in making the government more responsive to the public and better connected to innovation.
- A disorganized adoption strategy or no strategy will be dangerous.
- To ensure proper security, efficiency, and viability, Congress and the Administration should undertake agency-level cloud readiness assessments, determine appropriate configuration and deployment models, ramp up FedRAMP, promote the organic creation of common cloud standards, use effective service-level agreements with service providers, and update cyber and privacy laws to reflect advances in technology.

manage IT resources for their users via the Internet.[2] In this way, cyber clouds are similar to utilities in that they provide IT services to multiple consumers. As a result, cloud service providers (CSPs) can benefit from economies of scale and provide services at lower costs to consumers.[3]

Cloud computing fundamentally challenges what is regarded as a "computer." Over the past 50 years, "we have witnessed the megatrends, from the mainframe era of the 1960s to the advent of minicomputers in the 1970s, the personal computer in the 1980s, the growth of the Internet and the web in the 1990s, and the explosion of cell phones and other smart, web-connected devices in the past 10 years." However, with the expansion of the cloud, future consumers may need machines with only the ability to drive basic functions such as a screen, keyboard, and Internet browser. In this manner, cloud computing represents a shift from a "device-centric" system to an "information-centric" system.[4]

Although all clouds depend on the Internet, clouds vary widely and are organized in two ways. First, clouds can be organized by service models, which depend on the capabilities and services provided by the cloud.

- **Software as a Service (SaaS)**, the most basic cloud model, provides the user with access to on-demand applications and software running on a cloud infrastructure through interfaces such as Web browsers and Web-based e-mail. However, the user does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, storage, and individual application capabilities.

- **Platform as a Service (PaaS)** is an expansion of SaaS to provide the user with the ability to add consumer-created or customer-acquired applications to the cloud infrastructure, using program tools, such as java or python, supported by the cloud provider. The user still does not manage the cloud infrastructure but does control the applications and some other application-related details.

- **Infrastructure as a Service (IaaS)** is the furthest expansion of the cloud. It provides the user with near total control over the cloud. The user does not manage or control the cloud's most basic infrastructure but does control the applications, operating systems, storage, and possibly networking elements such as firewalls.[5]

Additionally, cloud services can be organized according to deployment model.

- **Private cloud.** "The cloud infrastructure is operated solely for an individual organization. It could be managed by the organization or a third party" and operated in-house or offsite.

- **Community cloud.** The cloud is used by several organizations that share similar missions, security requirements, or compliance considerations, and one of the organizations can manage it for the other parties.

- **Public cloud.** The cloud is available to the public or a large industry but is owned and operated by a CSP.

- **Hybrid cloud.** The cloud is a mix of two or more cloud types, all of which remain separate entities but are connected by standardized technology that allows data and software transferability.[6]

In the past few years, cloud computing has grown rapidly—at a rate estimated at more than 20 percent per year—and the industry is projected to be worth as much as $150 billion by 2013.[7] Web-based applications such as Gmail, Facebook, Google Docs, YouTube, and many other services are examples of how prevalent the cloud has already become. This trend will likely continue. A recent Pew Internet poll

[1] Vivek Kundra, "Federal Cloud Computing Strategy," U.S. Chief Information Officers Council, February 8, 2011, p. 5, http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf (accessed March 13, 2012).

[2] David C. Wyld and Robert Maurin, "Moving to the Cloud: An Introduction to Cloud Computing," IBM Center for the Business of Government, 2009, p. 6, http://www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf (accessed March 13, 2012).

[3] Ibid., p. 5.

[4] Ibid., pp. 15–16.

[5] Ibid., p. 6.

[6] Ibid., p. 5.

[7] Ibid., p. 13.

found that 72 percent of expert respondents believe that "by 2020, most people won't do their work with software running on a general-purpose PC. Instead they will work in Internet based applications such as Google Docs, and in applications run from smartphones."[8]

The public sector is lagging behind the private sector in cloud computing, but governments are trying to narrow the gap. Vivek Kundra, chief information officer (CIO) of the District of Columbia, moved the District government to Gmail and Google apps after seeing that "when employees go home, they have access to more technology at home than they do at work."[9]

After becoming the first U.S. CIO, Kundra led the effort to promote cloud computing throughout the federal government, tripling spending on cloud computing from $277 million in 2008 to an anticipated $792 million in 2013. Today, the General Services Administration (GSA), NASA, Defense Information Systems, the Army, the National Security Agency, and other federal agencies are experimenting with various levels of cloud computing. Some government agencies, such as the U.S. Census Bureau and the Federal Reserve, already use private-sector cloud services to host public data sets.[10]

The Federal Migration Vision

On February 6, 2010, Kundra sent a memorandum to all federal agency CIOs that highlighted the exponential growth in the number of federal data centers in recent years.[11] At the time, the federal government was operating more than 2,096 federal data centers, nearly four times the number in operation a decade earlier.[12]

With the Federal Data Center Consolidation Initiative (FDCCI), Kundra and the Office of Management and Budget (OMB) put forth a plan to stem the unsustainable growth of federal data centers in an effort to reduce costs and energy use while increasing efficiency. In studying data center usage, the federal government found that utilization was as low as 7 percent of total capacity for many servers.[13] Yet in fiscal year 2010, data center infrastructure accounted for roughly 30 percent of federal IT spending.[14] Similarly, in 2010, projections estimated that federal data centers would soon consume more than 12 billion kilowatt hours of electricity per year[15]—enough to power more than one million homes for a year.[16]

IN THE PAST FEW YEARS, CLOUD COMPUTING HAS GROWN RAPIDLY—AT A RATE ESTIMATED AT MORE THAN 20 PERCENT PER YEAR—AND THE INDUSTRY IS PROJECTED TO BE WORTH AS MUCH AS $150 BILLION BY 2013.

25 Point Implementation Plan. Later in 2010, Kundra also released the 25 Point Implementation Plan to Reform Federal Information Technology Management, a plan to increase IT productivity and efficiency in the federal government. In the plan, Kundra echoed the federal government's commitment to consolidate federal data centers, restating the Administration's commitment to reduce the number of federal data centers by at least 800 by 2015.[17]

A large part of the problem with server utilization stems from

[8] Janna Anderson and Lee Rainie, "The Future of Cloud Computing," Pew Internet and American Life Project, June 11, 2010, http://pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings/Main-findings.aspx (accessed March 13, 2012).

[9] Wyld and Maurin, "Moving to the Cloud," p. 19.

[10] Ibid., p. 23.

[11] Vivek Kundra, "Federal Data Center Consolidation Initiative," memorandum for chief information officers, U.S. Office of Management and Budget, February 26, 2010, http://www.cio.gov/documents/Federal_Data_Center_Consolidation_Initiative_02-26-2010.pdf (accessed June 18, 2012).

[12] Andrew R. Hickey, "Feds to Shutter 100 Data Centers in 'Cloud First' Push," *CRN*, April 19, 2011, http://www.crn.com/news/cloud/229401860/feds-to-shutter-100-data-centers-in-cloud-first-push.htm;jsessionid=WW3uJwsVxdKZhhliLDLfLQ**.ecappj03 (accessed March 13, 2012).

[13] Darrell West, Vivek Kundra, Conrad R. Cross, and David C. Wyld, "The Economic Gains of Cloud Computing," The Brookings Institution, April 7, 2010, http://www.brookings.edu/~/media/Files/events/2010/0407_cloud_computing/20100407_cloud_computing.pdf (accessed March 13, 2012).

[14] David Perera, "Kundra Releases Federal Cloud Computing Strategy," *FierceGovernmentIT*, February 13, 2011, http://www.fiercegovernmentit.com/story/kundra-releases-federal-cloud-computing-strategy/2011-02-13 (accessed March 13, 2012).

[15] Kundra, "Federal Data Center Consolidation Initiative."

[16] U.S. Energy Information Administration, "Frequently Asked Questions," December 6, 2011, http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3 (accessed March 13, 2012).

[17] Vivek Kundra, "25 Point Implementation Plan to Reform Federal Information Technology Management," U.S. Office of Management and Budget, December 9, 2010, http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf (accessed March 13, 2012).

agencies' ability to purchase dedicated servers to store and process data. This is akin to each home in a community having its own power generator rather than drawing power from a shared electric grid. Similarly, under current IT systems, federal agencies must consider and allot resources for the maximum data processing capacity that may be needed, even though this capacity may be rarely used.[18]

To reduce these server silos and increase operational efficiency within federal IT, the 25 Point Implementation Plan called for a shift to a "cloud first" policy. This policy would "revolve around using commercial cloud technologies where feasible, launching private government clouds, and utilizing regional clouds with state and local governments where appropriate." Specifically, the cloud-first policy dictated that every federal agency must identify three services to migrate to the cloud. Of these, it was required to fully migrate at least one service within 12 months and the remaining services within 18.[19]

Federal Cloud Computing Strategy. In February 2011, the Administration released the Federal Cloud Computing Strategy to accelerate federal migration to the cloud. The strategy brought together all of the components of the earlier plans and policies just two months after the release of the 25 Point Implementation Plan. The strategy begins by defining cloud computing and explaining that "by leveraging shared infrastructure and economies of scale, cloud computing presents a compelling business model for federal leadership."[20] However, it goes beyond simply laying out the benefits and considerations of federal migration to the cloud to providing a decision framework and case examples for federal agency CIOs.

The federal strategy called upon agency CIOs to select services to be moved to the cloud based on value and readiness. High-value, high-readiness services should be the first candidates for cloud migration. Yet both characteristic are difficult to define. Value could be considered a factor of efficiency, agility, and innovation, while readiness must consider security requirements, interoperability, scalability, performance, reliability, and much more.[21]

After selecting services for migration, CIOs need to work to provision services effectively by aggregating demand, integrating the new cloud services into agency IT portfolios, and carefully contracting cloud services. CIOs also need to shift their IT mindset from asset management to service management. This requires shifting focus from input to output metrics and greater tracking of usage rates and service-level agreements (SLAs).[22]

To accelerate federal cloud service adoption, the Federal Cloud Computing Strategy outlined cloud computing "accelerators." These included leveraging cloud computing business cases and examples, developing security controls and guidance, streamlining procurement processes, and establishing standards for cloud computing.

Finally, the Federal Cloud Computing Strategy also outlined the role of each key government player in federal cloud computing migration.

- "*National Institute of Standards and Technology (NIST)* will lead and collaborate with Federal, State, and local government agency CIOs, private sector experts, and international bodies to identify and prioritize cloud computing standards and guidance."
- "*General Service Administration (GSA)* will develop government-wide procurement vehicles and develop government-wide, cloud-based application solutions where needed."
- "*Department of Homeland Security (DHS)* will monitor operational security issues related to the cloud."
- "*Agencies* will be responsible for evaluating their sourcing strategies to fully consider cloud computing solutions."
- "*Federal CIO Council* will drive government-wide adoption of

[18] Afzal Bari, "Federal Cloud Computing and Data Center Consolidation," Bloomberg Government Briefing, March 2011, http://www.actgov.org/events/managementofchange/MOC2011/MOC%202011%20Documents%20and%20Presentations/federal%20cloud%20computing%20and%20data%20center%20consolidation.pdf (accessed March 13, 2012).

[19] Kundra, "25 Point Implementation Plan."

[20] Kundra, "Federal Cloud Computing Strategy."

[21] Ibid.

[22] Ibid.

cloud, identify next-generation cloud technologies, and share best practices, reusable example analyses, and templates."

- "*The Office of Management and Budget (OMB)* will coordinate activities across governance bodies, set overall cloud-related priorities, and provide guidance to agencies."[23]

Cloud Migration Implementation

Currently, each federal agency conducts its own IT security assessments and authorizations, even if another agency has already done the same for a given technology. This process is duplicative and inefficient. To overcome these issues in cloud computing implementation, the federal government adopted a "do once, use many times" framework for security assessments, authorization, and continuous monitoring.[24]

Through this framework, the Federal Risk and Authorization Management Program (FedRAMP) seeks to enhance the economies of scale offered by federal migration to the cloud through shared security assessment and authorization based on government-wide security standards. Under this program, run by the GSA's Office of Citizen Services and Innovative Technology, CSPs must meet security controls outlined by FedRAMP's Joint Authorization Board (JAB), which is composed of the CIOs for the Department of Defense, the DHS, and the GSA. Fulfillment of these security requirements must then be confirmed by a security assessment conducted by an independent third-party assessment organization. The JAB could then review the security assessment and provide a provisional authorization.[25] Federal agencies could leverage these pre-authorizations to speed acquisition of cloud-based services.

FedRAMP is currently in a pilot phase with initial operational capacities scheduled to go online in June 2012. It will focus first on infrastructure and e-mail service. Full implementation and mandatory FedRAMP usage will occur in 2014. As the government implements its migration to cloud computing, many key benefits and concerns should be considered.

Government Cloud Computing Benefits

As the federal government begins to use cloud computing, it can take advantage of the cloud's many benefits:

- Reduced costs due to increases in efficiency,
- Improved scalability and flexibility,
- Improved access to innovation, and
- Enhanced security and disaster recovery capabilities.

Reduced Costs. Perhaps the most alluring benefit of cloud computing is lower costs due to increased efficiency. By switching to the cloud, government agencies can take greater advantage of economies of scale. When CSPs purchase large quantities of computing power and storage space, they can buy it at a lower price per server than smaller organizations can. Thus, CSPs can pass on some of the savings to their customers in the private or public sectors. The same applies to most maintenance, operations, and upgrade costs, which can be handled more efficiently and at lower cost by a cloud provider than is possible if the IT staff of each agency and department must deal with these issues by itself.

IN 2010, THE GOVERNMENT OPERATED ALMOST 2,100 DATA CENTERS WITH A UTILIZATION RATE OF LESS THAN 30 PERCENT OF CAPACITY FOR MOST SERVERS.

Cloud computing also allows improved asset utilization. In 2010, the government operated almost 2,100 data centers with a utilization rate of less than 30 percent of capacity for most servers.[26] Taxpayers are thus paying for more than 70 percent of computing capacity to sit idly on standby so that it can be used if greater processing capacity is needed. By moving to the cloud, the government will pay for only as much processing power and storage space as it needs at a given moment. Duplicative data centers and capabilities can be removed because the cloud can scale resources on demand more cheaply and efficiently.

The federal government has identified $20 billion (25 percent of its IT budget) that could be moved to the cloud. A variety of other reports have

[23] Ibid. (italics in original).

[24] U.S. General Services Administration, "FedRAMP: Overview," December 8, 2011, http://www.gsa.gov/portal/category/102371 (accessed March 13, 2012).

[25] U.S. General Services Administration, "About FedRAMP," February 7, 2012, http://www.gsa.gov/portal/category/102375 (accessed March 13, 2012).

[26] Kundra, "25 Point Implementation Plan," p. 5, and Kundra, "Federal Cloud Computing Strategy," p. 7.

estimated savings ranging from 25 percent to more than 90 percent.[27] Even if only the lower estimates of 25 percent to 50 percent are realized, the government could save between $5 billion and $10 billion.

Increased Scalability. The ability to access greater capacity when needed is critical to reducing excess government computing capacity. Cloud computing provides this ability by offering computing resources on demand. As long as appropriate SLAs are instituted, the government should be able to rapidly increase its capacity in times of need to avoid shortages while not paying for those same resources when they are not needed.[28]

A great example of how scalability could make a great difference in the federal government is the U.S. Census Bureau. Every 10 years, the bureau needs to ramp up resources rapidly to deal with the level of data it needs to process and analyze for the decennial census. However, during the other nine years, the bureau needs significantly fewer resources. In a similar way, many agencies require extra resources during certain times of the year, such as the IRS during tax season or FEMA during national emergencies. Rather than procuring extra capacity and not using it for long periods, the cloud allows government agencies to pay only for what they use and provides nearly instantaneous access to additional resources when and if they are needed.

Improved Access to Innovation. The current system of legacy technology involves buying hardware and software every time an upgrade is needed. Upgrading technology can often take years, at which point the "new" technology may have become obsolete. By moving to the cloud, government agencies can focus on managing needed services rather than trying to predict future server and software needs. Because managing the hardware and key software elements belongs to the CSP, the government can take greater advantage of private-sector innovation. The cloud provider will likely incorporate new technology and innovations into its system faster than the government could.[29]

Additionally, the cloud allows for more aggressive testing of new IT ideas. Instead of purchasing large amounts of technology and testing whether it works, the cloud will allow the government to test new projects with much smaller initial investments. Worthwhile projects can be expanded, while underperforming ones can be cancelled with only minimal losses.

Enhanced Security and Disaster Recovery. Cloud computing also offers benefits in security and continuity of operations (COOP). Cloud providers can likely defend their cloud—potentially made up of hundreds or thousands of clients—better than each client can defend itself on its own. By handling cybersecurity for all of its clients, the CSP can hire additional security experts, employ more sophisticated security tools, and increase security more easily by deploying enhanced security software more quickly and efficiently. Studies have shown that antivirus software performed better in detecting viruses and malware after virus protection was moved from "individual PCs to the cloud that connected them."[30]

Another often overlooked security improvement is that the cloud provides a solution to theft or loss of laptops and other hardware. Currently, if a laptop or USB drive is stolen or lost, the information saved on the device is protected only by the defenses on the machine, which cannot keep out a dedicated hacker indefinitely. Cloud computing changes the situation because the data are no longer stored on individual computers, but on the cloud. If a laptop that uses the cloud falls into the wrong hands, the criminal is left with a machine with no critical information. Similarly, cloud computing would reduce the use and, therefore, thefts of USB drives because all information is easily shareable on the cloud.[31]

Finally, because cloud computing means access from anywhere there is Internet access, COOP is improved. With traditional IT systems, a natural disaster or enemy attack could cripple a government agency. With a cloud system, government employees can leave the building, city, or state and still work to maintain essential

[27] West et al., "The Economic Gains of Cloud Computing," p. 2.

[28] Ibid.

[29] Kundra, "Federal Cloud Computing Strategy."

[30] Wyld and Maurin, "Moving to the Cloud," p. 37.

[31] Ibid.

services during emergencies.[32] Because the data on the cloud are stored on multiple servers, an attack on cloud servers is less likely to cause a total loss of data. With the increasing use of cloud services, government agencies should integrate cloud capabilities into their COOP plans to take full advantage of the cloud's potential.

Cloud Concerns

While the cloud has many benefits, a 2010 Lockheed Martin poll of government IT executives found that 60 percent were neutral or did not trust the cloud.[33] Several concerns regarding shifting government IT resources to the cloud need to be addressed:

- Security,
- Privacy,
- Data storage and retrieval,
- Vendor lock-in,
- Standards and outdated regulations and laws, and
- Cultural and IT staff resistance.

Security. Security was listed as a benefit because cloud computing improves security in some ways, particularly because one cloud provider can defend information better than individual clients can defend their own networks. However, moving government capabilities to the cloud does present three security concerns: the risk that aggregating important government data can make government clouds larger, more attractive targets; concerns that entire CSP servers could become compromised; and potential principal–agent problems between CSPs and customers.

WITH A CLOUD SYSTEM, GOVERNMENT EMPLOYEES CAN LEAVE THE BUILDING, CITY, OR STATE AND STILL WORK TO MAINTAIN ESSENTIAL SERVICES DURING EMERGENCIES.

One risk is that a large, focused attack might compromise government cloud servers. With government databases centralized on the cloud, cloud servers become larger, more important targets for cyber attacks. In this manner, a successful cyber attack could compromise massive amounts of government data or take down entire networks. The potentially dangerous results make government cloud servers prime targets for hackers. One possible solution would be to maintain the most critical data and operations on private clouds or not on clouds at all. This solution would allow less sensitive operations to take advantage of the benefits of the cloud while keeping critical data isolated and secure.

Government agencies should also consider how CSPs will deal with multitenancy—securing the data of multiple users on the cloud. Because public and community clouds have multiple organizations on one network, a security breach in one organization could have security consequences for the rest.[34]

Finally, a security concern emerges from the principal–agent problem. Although a cloud provider (i.e., the agent) can provide enhancements in security more effectively, the CSP has the incentive to maximize profit. This incentive may result in lower security than the consumer (the principal) wants.[35] Careful contracting could combat this problem. Many SLAs contain worrisome provisions, which allows the CSPs to change the contracts unilaterally, delete data on certain grounds, determine which service outages are compensated, issue disclaimers regarding security of customer data, and so forth.[36] Writing SLAs to address the needs and unique position of the government can mitigate the principal–agent problem significantly.

Privacy. Privacy concerns about the cloud revolve around problems with current privacy rules that were outlined by the Electronic

[32] Kundra, "Federal Cloud Computing Strategy," p. 14.

[33] Lockheed Martin and Market Connections, "Getting Secure in the Cloud: How to Meet IT Mandates, Ensure Security and Achieve Cost Savings for Your Government Agency," July 2011, p. 5, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Getting-Secure-in-the-Cloud.pdf (accessed June 18, 2012).

[34] Allan A. Friedman and Darrell M. West, "Privacy and Security in Cloud Computing," *Issues in Technology Innovation*, No. 3, October 2010, p. 3, http://www.brookings.edu/~/media/Files/rc/papers/2010/1026_cloud_computing_friedman_west/1026_cloud_computing_friedman_west.pdf (accessed March 13, 2012).

[35] Ibid., p. 5.

[36] Simon Bradshaw, Christopher Millard, and Ian Walden, "The Terms They Are A-Changin'…: Watching Cloud Contracts Take Shape," *Issues in Technology Innovation*, No. 7, March 2011, p. 10, http://www.brookings.edu/~/media/Files/rc/papers/2011/03_cloud_computing_contracts/03_cloud_computing_contracts.pdf (accessed March 13, 2012).

Communications Privacy Act of 1986.[37] When these rules were adopted, the Internet had not been truly established, and e-mail, social networking, and the cloud were not widely used, if they existed at all. Current law gives stronger privacy protections to information stored locally than to information stored with a third-party vendor.[38] True protection of data stored in the cloud will remain a source of concern until Congress addresses this problem.

Data Storage and Records Management. As the federal government expands its use of cloud services, the flow of data through and stored on the cloud will increase. Depending on the type of cloud and the service provider, these data may be transmitted and stored in any number of locations. In terms of disaster recovery and continuity of operations, this fact may be a benefit. However, if the servers exist outside U.S. borders, export control laws have strong implications. As one expert explains:

> [T]here is an inherent tension between cloud computing and export control. While the concept of the cloud is centered on the premise of removing the need to track the details of data movement among various destinations, export control regulations are built largely around restrictions tied to those very movements.[39]

Under the Export Administration Regulations (EAR) and the International Trafficking in Arms Regulations (ITAR), controlled technical data (i.e., data related to the production or development of a controlled item such as certain electronics and weaponry) cannot be transmitted to foreign nations under penalty of fines of up to $1 million.[40] In migrating data to the cloud, federal agencies—particularly agencies that work with a high level of export-controlled data, such as many agencies in the Department of Defense—must be aware of whether data will be transmitted to overseas servers.

Similarly, record management and data retrieval are also key areas of concern. Federal records stored on the cloud, just like all other government data, must comply with federal records management regulations as largely outlined by Title 44 of the U.S. Code and Title 36 of the Code of Federal Regulations. These regulations stipulate that no record can be destroyed without the permission of the National Archives and Records Administration.[41]

Relying on a third party or one agency to store the data of another agency creates key uncertainties, including establishing who is responsible for record keeping.[42] Agencies must ensure that data retrieval capabilities exist so that they can respond to Freedom of Information Act requests.

Current Standards, Regulations, and Laws. Current cyber cloud standards, regulations, and laws are sources of additional concerns. The NIST has determined that Federal Information Security Management Act (FISMA) regulations, created by the E-Government Act of 2002, apply to cloud computing. FISMA requires each agency to "implement an agency-wide program to provide security for information and information systems that support the operations and assets of the agency."[43] These security programs must then be certified, but each agency uses its own standards. As a result, each agency must certify each new IT capability even though other agencies may already have approved it.

Without a uniform certification process, FISMA erects a barrier to using new capabilities and divides government-wide efforts to buy and use these new systems, driving up costs. Updating the E-Government Act would help to ease the implementation of cloud systems.

Congress should also examine other laws, including the Computer Fraud and Abuse Act of 1986, which provides for a penalty of up to

[37] Darrell M. West, "Steps to Improve Cloud Computing in the Public Sector," *Issues in Technology Innovation,* No. 1, July 2010, p. 5, http://www.brookings.edu/~/media/Files/rc/papers/2010/0721_cloud_computing_west/0721_cloud_computing_west.pdf (accessed March 13, 2012).

[38] Friedman and West, "Privacy and Security in Cloud Computing," p. 5.

[39] John Villasenor, "Addressing Export Control in the Age of Cloud Computing," The Brookings Institution, Center for Technology Innovation, July 25, 2011, http://www.brookings.edu/papers/2011/0725_cloud_computing_villasenor.aspx (accessed March 13, 2012).

[40] Michael Biddick, "The Business Case for Government Clouds," *InformationWeek Analytics*, May 2010, http://storage-brain.com/wp-content/uploads/papers/CloudCompliance_in_Gvmt.pdf (accessed March 13, 2012).

[41] Ibid.

[42] Ibid.

[43] Ibid., p. 12.

$250,000 and five years in jail for an unwarranted intrusion. However, it is unclear how that law would apply if a cloud data center was hacked. The law might allow for only one penalty even though multiple cloud users' data were compromised.[44]

Also worth consideration is the need for standards in cloud systems. These standards include common structures and data transfer protocols, which would improve the interaction between cloud systems. The Federal Cloud Computing Strategy describes the need for cloud computing standards as "critical for the successful adoption and delivery of cloud computing" and for ensuring that "clouds have an interoperable platform so services provided by different cloud providers can work together."[45]

The current lack of standards needs to be remedied before implementation of greater migration to the cloud. However, the government should not dictate standards, but instead should promote their natural creation through efforts like the Open Cloud project.[46] Additionally, it would be wise to move slowly on standards because technology changes quickly and statically written standards could stifle innovation.

Vendor Lock-In. Another concern is the potential for "vendor lock-in." The costs in time, money, and effort of moving from one cloud to another could be substantial. Although this is certainly a cause for concern, it is not specific to the cloud. Whether updating a traditional IT system or moving from one cloud to a different one, moving from one system to another often threatens high costs. The fear of being locked into a cloud server is likely heightened because the cloud is not directly controlled by the consumer.[47]

Once again, the answer is likely to be found in contracts and service-level agreements. IT staffs should insist on specifics in their SLAs that describe how to end the relationship with the cloud provider and move the data to another provider or back to the agency itself. This can reduce the costs of the unknown and mitigate lock-in risks.[48]

Additionally, promotion of standards would increase the use of common cloud structures and improve the transferability, or portability, of data and applications between clouds.[49] This step would reduce the costs of moving data and, thus, the fear of being locked in.

Culture Shifts and IT Resistance. A final concern is how individuals and IT staff would respond to this dramatic change in the way the government does business. One of the greatest hindrances to greater adoption of cloud computing is lack of understanding. In 2008, almost 70 percent of American adults used a cloud computing system in one form or the other, and 40 percent used two. Webmail services such as Gmail, Hotmail, and Yahoo Mail led the way, while online photo storage and online applications such as Google Documents were also commonly used.[50]

A large portion of these users probably do not realize that their Gmail or Photobucket accounts are examples of cloud computing. As understanding of cloud computing grows, more computing services will likely be sent to the cloud because it provides the same, if not superior, services in a way that will look very similar to the way individuals currently use their computers and Internet.[51]

However, traditional IT staffs will likely hesitate to move to the cloud. Their experience and jobs are tied to legacy systems, and they will likely be concerned about the reliability and security of the cloud because they do not directly control it. On the other hand, newer IT staffers, who may better understand and use Web-based tools, will likely be more willing to move to the cloud than their traditional counterparts are.[52] The presence of these newer staffers will help companies move to the cloud

[44] West, "Steps to Improve Cloud Computing," p. 7.

[45] Kundra, "Federal Computing Strategy," p. 29.

[46] Wyld and Maurin, "Moving to the Cloud," p. 40.

[47] Ibid., p. 39.

[48] Ibid.

[49] Ibid.

[50] News release, "Cloud Computing Takes Hold as 69% of All Internet Users Have Either Stored Data Online or Used a Web-Based Software Application," Pew Research Center, September 12, 2008, http://www.pewinternet.org/Press-Releases/2008/Cloud-computing-takes-hold-as-69-of-all-internet-users-have-either-stored-data-online-or.aspx (accessed March 14, 2012).

[51] Wyld and Maurin, "Moving to the Cloud."

[52] Ibid.

and mitigate the concerns of traditional staffers.

Reaching for the Cloud

Cloud computing is an emerging technology that offers substantial savings in efficiency and cost. It will assist in making the government more responsive to the public and better connected to innovation. However, government migration to the cloud must be done correctly. To ensure proper security, efficiency, and viability, Congress and the Administration should:

- **Undertake agency-level cloud readiness assessments.** The federal cloud computing strategy has called upon agency CIOs to select services to be moved to the cloud based on value and readiness. High-value, high-readiness services should be the first candidates for cloud migration. However, these characteristics are not easily defined. Agency CIOs need to establish rules for what can and cannot be migrated to the cloud. Executive branch agencies should conduct detailed assessments to determine the present state of their cyber capabilities and needs as a first step toward making sensible decisions on what can and should be moved to a cloud configuration and what type of cloud model would be most advantageous.

- **Determine appropriate cloud configuration and deployment models.** The Administration should direct the Federal CIO Council to determine which agencies can set up their own cloud and which should group together in a joint cloud. Government agencies with nonsensitive information can group together and take advantage of economies of scale by migrating to a joint cloud. For agencies with greater security concerns, private or hybrid clouds may be more appropriate.

- **Ramp up FedRAMP.** Having each federal agency conduct its own IT security assessments and authorizations is duplicative and inefficient. The government's proposal under FedRAMP to overcome this issue with a "do once, use many times" framework for security assessments, authorization, and continuous monitoring offers an excellent solution. However, FedRAMP has not yet been fully implemented. The Administration should make every effort to fully realize the benefits of the program.

- **Promote the organic creation of common cloud standards.** To promote transferability and avoid vendor lock-in, the Administration should promote the creation of common cloud architectures and transfer protocols. However, the government should not force top-down standards on cloud providers, because these standards may inhibit cloud innovation and growth. Instead, it should allow and promote the natural creation of standards through efforts like the Open Cloud project.

- **Use effective service-level agreements with cloud service providers.** Agencies should pursue proper SLAs with their CSPs that include provisions to secure their data with appropriate backup and data retrieval capabilities, prevent lock-in issues, and address agency-specific security considerations.

- **Update cyber and privacy laws to account for advances in technology.** The laws on cybersecurity, privacy, and information are outdated. The Electronic Communications Privacy Act of 1986 gives greater protection to information stored locally than it gives to information stored with a third-party vendor and should be changed to reflect the modern technological world. Other laws, such as the E-Government Act of 2002, should be updated to remove duplicative procedures.

The Future of the Federal Cloud

Cloud computing offers a compelling and effective means of reducing federal IT infrastructure costs while providing additional benefits such as scalability, increased security, and improved access to innovation. The government should proceed in a manner that avoids common cloud computing pitfalls and takes full advantage of all that the cloud has to offer.

*—**Steven P. Bucci, PhD,** is Senior Research Fellow for Defense and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. The author is grateful to Heritage research assistant David Inserra for his help in preparing this study.*