United States Government Accountability Office

GAO

Testimony

Before the Committee on Oversight and Government Reform and Its Subcommittee on Government Management, Organization, and Procurement, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, July 1, 2010

INFORMATION SECURITY

Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing

Statement of Gregory C. Wilshusen
Director, Information Security Issues

July 2010

INFORMATION SECURITY

Government wide Guidance Needed to Assist Agencies in Implementing Cloud Computing

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-855T, a testimony before the Committee on Oversight and Government Reform and its Subcommittee on Government Management, Organization, and Procurement, House of Representatives

Why GAO Did This Study

Cloud computing, an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Internet-based technologies, reportedly has the potential to provide information technology services more quickly and at a lower cost, but also to introduce information security risks. Accordingly, GAO was asked to testify on the benefits and risks of moving federal information technology into the cloud. This testimony summarizes the contents of a separate report that is being released today which describes (1) the models of cloud computing, (2) the information security implications of using cloud computing services in the federal government, and (3) federal guidance and efforts to address information security when using cloud computing. In preparing that report, GAO collected and analyzed information from industry groups, private-sector organizations, and 24 major federal agencies.

What GAO Recommends

In the report being released today, GAO recommended that the Office of Management and Budget, the General Services Administration, and the Department of Commerce take steps to address cloud computing security, including completion of a strategy, consideration of security in a planned procurement of cloud computing services, and issuance of guidance related to cloud computing security. These agencies generally agreed with GAO's recommendations.

View GAO-10-855T or key components.
For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. They include a private cloud, operated solely for an organization; a community cloud, shared by several organizations; a public cloud, available to any paying customer; and a hybrid cloud, a composite of deployment models.

Cloud computing can both increase and decrease the security of information systems in federal agencies. Potential information security benefits include those related to the use of virtualization and automation, broad network access, potential economies of scale, and use of self-service technologies. In addition to benefits, the use of cloud computing can create numerous information security risks for federal agencies. Specifically, 22 of 24 major federal agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include dependence on the security practices and assurances of a vendor, and the sharing of computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation.

Federal agencies have begun efforts to address information security issues for cloud computing, but key guidance is lacking and efforts remain incomplete. Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance. Agencies have also identified challenges in assessing vendor compliance with government information security requirements and clarifying the division of information security responsibilities between the customer and vendor. Furthermore, while several governmentwide cloud computing security initiatives are under way by organizations such as the Office of Management and Budget and the General Services Administration, significant work needs to be completed. For example, the Office of Management and Budget has not yet finished a cloud computing strategy, or defined how information security issues will be addressed in this strategy. The General Services Administration has begun a procurement for expanding cloud computing services, but has not yet developed specific plans for establishing a shared information security assessment and authorization process. In addition, while the National Institute of Standards and Technology has begun efforts to address cloud computing information security, it has not yet issued cloud-specific security guidance. Until specific guidance and processes are developed to guide the agencies in planning for and establishing information security for cloud computing, they may not have effective information security controls in place for cloud computing programs.

Chairman Towns, Chairwoman Watson, and Members of the Committee and Subcommittee:

Thank you for the opportunity to participate in today's hearing on federal guidance and efforts to address information security when using cloud computing. My statement today is based on our report titled *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing* (GAO-10-513), which provides a fuller discussion of our results and is being released at this hearing.[1]

Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers. Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer. The current administration has highlighted cloud computing as having the potential to provide information technology (IT) services more quickly and at a lower cost than traditional methods.

We have previously reported that cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing.[2] Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. Further, the increasing interconnectivity among information systems, the Internet, and other infrastructure presents increasing opportunities for attacks. For example, in 2009, several media reports described incidents that affected cloud service providers such as Amazon and Google.

Given the potential risks, you requested that we examine the security implications of cloud computing. In response to your request, our report and my statement provide (1) a description of the models of cloud

[1]GAO, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, GAO-10-513 (Washington, D.C. May 27, 2010).

[2]GAO, *Continued Efforts Are Needed to Protect Information Systems From Evolving Threats*, GAO-10-230T (Washington D.C.: Nov. 17, 2009) and *Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, GAO-09-661T (Washington, D.C.: May 5, 2009).

computing, (2) a description of the information security implications of using cloud computing services in the federal government, and (3) an assessment of federal guidance and efforts to address information security when using cloud computing. In conducting the work for our report, we collected and analyzed information from industry groups, private-sector organizations, the National Institute of Standards and Technology (NIST), and 24 major federal agencies.[3] Our work for the report was performed in accordance with generally accepted government auditing standards.

Cloud Computing Is a Form of Shared Computing with Several Service and Deployment Models

Cloud computing is a new form of delivering IT services that takes advantage of several broad evolutionary trends in information technology, including the use of virtualization.[4] According to NIST, cloud computing is a means "for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST also states that an application should possess five essential characteristics to be considered cloud computing; on-demand self service, broad network access, resource pooling, rapid elasticity, and measured service.

Cloud computing offers three service models: infrastructure as a service, where a vendor offers various infrastructure components; platform as a service, where a vendor offers a ready-to-use platform on which customers can build applications; and software as a service, which provides a self-contained operating environment used to deliver a complete application such as Web-based e-mail.

In addition, four deployment models for providing cloud services have been developed: private, community, public, and hybrid cloud. In a private

[3]The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services , Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

[4]Virtualization is a technology that allows multiple software-based virtual machines with different operating systems to run in isolation, side-by-side on the same physical machine. Virtual machines can be stored as files, making it possible to save a virtual machine and move it from one physical server to another.

cloud, the service is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the premises. In a community cloud, the service is set up for related organizations that have similar requirements. A public cloud is available to any paying customer and is owned and operated by the service provider. A hybrid cloud is a composite of the deployment models.

Cloud Computing Has Both Positive and Negative Information Security Implications

The adoption of cloud computing has the potential to provide benefits related to information security. The use of virtualization and automation in cloud computing can expedite the implementation of secure configurations for virtual machine images. Other advantages relate to cloud computing's broad network access and use of Internet-based technologies. For example, several agencies stated that cloud computing provides a reduced need to carry data in removable media because of the ability to access the data through the Internet, regardless of location. Additional advantages relate to the potential economies of scale and distributed nature of cloud computing. In response to our survey, 22 of the 24 major agencies identified low-cost disaster recovery and data storage as a potential benefit. The self-service aspect of cloud computing may also provide benefits. For example, 20 of 24 major agencies identified the ability to apply security controls on demand as a potential benefit.

In addition to benefits, the use of cloud computing can create numerous information security risks for federal agencies. In response to our survey, 22 of 24 major agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. Several of these risks relate to being dependent on a vendor's security assurances and practices. Specifically, several agencies stated concerns about:

- the possibility that ineffective or non-compliant service provider security controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information;
- the potential loss of governance and physical control over agency data and information when an agency cedes control to the provider for the performance of certain security controls and practices;
- the insecure or ineffective deletion of agency data by cloud providers once services have been provided and are complete; and

- potentially inadequate background security investigations for service provider employees that could lead to an increased risk of wrongful activities by malicious insiders.

Multitenancy, or the sharing of computing resources by different organizations, can also increase risk. Twenty-three of 24 major agencies identified multitenancy as a potential information security risk because one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information. Another concern is the increased volume of data transmitted across agency and public networks. This could lead to an increased risk of the data being intercepted in transit and then disclosed.

Although there are numerous potential information security risks related to cloud computing, these risks may vary based on the particular deployment model. For example, NIST states that private clouds may have a lower threat exposure than community clouds, which may have a lower threat exposure than public clouds. Several industry representatives stated that an agency would need to examine the specific security controls of the vendor the agency was evaluating when considering the use of cloud computing.

Federal Agencies Have Begun Efforts to Address Information Security Issues for Cloud Computing, but Specific Guidance Is Lacking and Efforts Remain Incomplete

Federal agencies have begun to address information security for cloud computing; however, they have not developed the corresponding guidance. About half of the 24 major agencies we asked reported using some form of public or private cloud computing for obtaining infrastructure, platform, or software services. These agencies identified measures they are taking or plan to take when using cloud computing. These actions, however, have not always been accompanied by development of related policies or procedures to secure their information and systems.

Most agencies have concerns about ensuring vendor compliance and implementation of government information security requirements. In addition, agencies expressed concerns about limitations on their ability to conduct independent audits and assessments of security controls of cloud computing service providers. Several industry representatives agreed that compliance and oversight issues are a concern and raised the idea of having a single government entity or other independent entity conduct security oversight and audits of cloud computing service providers on behalf of federal agencies. Agencies also stated that having a cloud service provider that had been precertified as being in compliance with

government information security requirements through some type of governmentwide approval process would make it easier for them to consider adopting cloud computing. Other agency concerns related to the division of information security responsibilities between customer and vendor. Until these concerns are addressed, the adoption of cloud computing may be limited.

Several Governmentwide Cloud Computing Information Security Initiatives Have Been Started, but Key Guidance and Efforts Have Not Been Completed

While several governmentwide cloud computing security activities are under way by organizations such as the Office of Management and Budget (OMB) and the General Services Administration (GSA), significant work remains to be completed. For example, OMB stated that it began a federal cloud computing initiative in February 2009; however, it does not yet have an overarching strategy or an implementation plan. According to OMB officials, the initiative includes an online cloud computing storefront managed by GSA and will likely contain several pilot cloud computing projects, each with a lead agency. However, as of March 2010, a date had not been set for the release of the strategy or for any of the pilots. In addition, OMB has not yet defined how information security issues, such as a shared assessment and authorization process, will be addressed in this strategy.

Federal agencies have stated that additional guidance on cloud computing security would be helpful. Addressing information security issues as part of this strategy would provide additional direction to agencies looking to use cloud computing services. Accordingly, we recommended that OMB establish milestones for completing a strategy for implementing the cloud computing initiative and ensure the strategy addresses the information security challenges associated with cloud computing, such as needed agency-specific guidance, controls assessment of cloud computing service providers, division of information security responsibilities between customer and provider, a shared assessment and authorization process, and the possibility for precertification of cloud computing service providers. OMB agreed with our recommendation and noted that it planned to issue a strategy over the next 6 months that covers activities for the next 5 to 10 years based on near term lessons learned. OMB also identified several federal activities planned in the short term to address security issues in cloud computing.

GSA Has Established Program Office and Cloud Computing Storefront, but Has Not Yet Developed Plans for a Shared Assessment and Authorization Process

GSA has established the Cloud Computing Program Management Office that manages several cloud computing activities within GSA and provides administrative support for cloud computing efforts by the Federal Chief Information Officers (CIO) Council. Specifically, the program office manages a storefront, www.apps.gov, established by GSA to provide a central location where federal customers can purchase software as a service cloud computing applications. GSA has also initiated a procurement to expand the storefront by adding infrastructure as a service cloud computing offerings such as storage, virtual machines, and Web hosting.

Establishing both an assessment and authorization process for customers of these services and a clear division of security responsibilities will help ensure that these services, when purchased and effectively implemented, protect sensitive federal information. GSA officials stated that they need to work with vendors after a new procurement has been completed to develop a shared assessment and authorization process, but have not yet developed specific plans to do so. Accordingly, we recommended that GSA ensure that full consideration is given to the information security challenges of cloud computing, including a need for a shared assessment and authorization process as part of their procurement for infrastructure as a service cloud computing technologies. GSA agreed and identified plans for ensuring issues such as a shared assessment and authorization process would be addressed.

Federal CIO Council Has Established Cloud Computing Executive Steering Committee but Has Not Finalized Key Process or Guidance

The Federal CIO Council established the Cloud Computing Executive Steering Committee to promote the use of cloud computing in the federal government. Under this committee, the security subgroup has developed the Federal Risk and Authorization Management Program, which is a governmentwide program to provide joint authorizations and continuous security monitoring services for all federal agencies, with an initial focus on cloud computing.

The subgroup is currently working with its members to define interagency security requirements for cloud systems and services and related information security controls. However, a deadline for completing development and implementation of a shared assessment and authorization process has not been established. We recommended that OMB direct the CIO Council Cloud Computing Executive Steering Committee to develop a plan, including milestones, for completing a governmentwide security assessment and authorization process for cloud services. OMB agreed and identified current activities of the CIO Council which are intended to address the recommendation.

NIST Is Coordinating Activities with CIO Council but Has Not Established Cloud-Specific Guidance

NIST is responsible for establishing information security guidance for federal agencies to support FISMA; however, it has not yet established guidance specific to cloud computing or to information security issues specific to cloud computing, such as portability and interoperability, and virtualization.

The NIST official leading the institute's cloud computing activities stated that existing NIST guidance in SP 800-53 and other publications applies to cloud computing and can be tailored to the information security issues specific to cloud computing. However, both federal and private sector officials have made clear that existing guidance is not sufficient. Accordingly, we recommended that NIST issue cloud computing guidance to federal agencies to more fully address key cloud computing domain areas that are lacking in SP 800-53 areas such as virtualization, and portability and interoperability, and include a process for defining roles and responsibilities of cloud computing service providers and customers. NIST officials agreed and stated that the institute is planning to issue guidance on cloud computing and virtualization this year.

In summary, the adoption of cloud computing has the potential to provide benefits to federal agencies; however, it can also create numerous information security risks. Federal agencies have taken steps to address cloud computing security, but many have not developed corresponding guidance. OMB has initiated a federal cloud computing initiative, but has not yet developed a strategy that addresses the information security issues related to cloud computing, and guidance from NIST to ensure information security is insufficient. While the Federal CIO Council is developing a shared assessment and authorization process, which could help foster adoption of cloud computing, this process remains incomplete, and GSA has yet to develop plans for a shared assessment and authorization process for its procurement of cloud computing infrastructure as a service offerings. Until federal guidance and processes that specifically address information security for cloud computing are developed, agencies may be hesitant to implement cloud computing, and those programs that have been implemented may not have effective information security controls in place.

Chairman Towns, Chairwoman Watson, and Members of the Committee and Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions.

For questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Individuals making key contributions to this testimony included Season Dietrich, Vijay D'Souza, Nancy Glover, and Shaunyce Wallace.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548