

**GAO**

Testimony

Before the Subcommittee on Cybersecurity,  
Infrastructure Protection, and Security  
Technologies, Committee on Homeland Security,  
House of Representatives

---

For Release on Delivery Expected  
at 10:00 a.m. EDT  
Thursday, October 6, 2011

## INFORMATION SECURITY

# Additional Guidance Needed to Address Cloud Computing Concerns

Statement of Gregory C. Wilshusen  
Director, Information Security Issues



---

Chairman Lungren, Ranking Member Clarke, and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on the security implications of cloud computing. My statement today summarizes our report issued last year, titled *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*<sup>1</sup> and describes actions taken by federal agencies to implement our report's recommendations.

Cloud computing, an emerging form of delivering computing services, can, at a high level, be described as a form of computing where users have access to scalable, on-demand information technology (IT) capabilities that are provided through Internet-based technologies. 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. Cloud computing can potentially deliver several benefits over current systems, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities. However, along with these benefits are the potential risks that any new form of computing services can bring, including information security breaches, infrastructure failure, and loss of data. Media reports have described security breaches of cloud infrastructure and reports by others have identified security as the major concern hindering federal agencies from adopting cloud computing services.

My statement today will provide a description of (1) the information security implications of using cloud computing services in the federal government, (2) our previous reporting on federal efforts and guidance to address cloud computing information security, and (3) our recommendations and subsequent actions taken by federal agencies to address federal cloud computing security issues. In preparing this statement, we summarized the content of our May 2010 report on cloud computing security. In conducting the work for that report, we collected and analyzed information from industry groups, private sector organizations, the National Institute of Standards and Technology (NIST),

---

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

---

and 24 major federal agencies.<sup>2</sup> In addition, we followed up with agencies to determine the extent to which the recommendations made in that report have been implemented. The work for the report on which this statement is based was performed in accordance with generally accepted government auditing standards.

---

## Background

We have previously reported that cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing.<sup>3</sup> 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.

In addition, the increasing interconnectivity among information systems, the Internet, and other infrastructure presents increasing opportunities for attacks. For example, since 2010, several media reports described incidents that affected cloud service providers such as Amazon, Google, and Microsoft. Additional media reports have described hackers exploiting cloud services for malicious purposes. The adoption of cloud computing will require federal agencies to implement new protocols and technologies and interconnect diverse networks and systems while mitigating and responding to threats.

Our previous reports and those by agency inspectors general describe serious and widespread information security control deficiencies that continue to place federal assets at risk of inadvertent or deliberate misuse, mission-critical information at risk of unauthorized modification or

---

<sup>2</sup>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.

<sup>3</sup>GAO, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*, [GAO-11-463T](#) (Washington D.C.: Mar. 16, 2011) and *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure*, [GAO-11-865T](#) (Washington, D.C.: July 26, 2011).

---

destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. We have also reported that weaknesses in information security policies and practices at major federal agencies continue to place confidentiality, integrity, and availability of sensitive information and information systems at risk. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,<sup>4</sup> a designation that remains in force today.<sup>5</sup> To assist agencies, GAO and agency inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve control deficiencies and information security program shortfalls.

---

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

Cloud computing delivers IT services by taking advantage of several broad evolutionary trends in IT, including the use of virtualization.<sup>6</sup> 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. Figure 1 illustrates each service model.

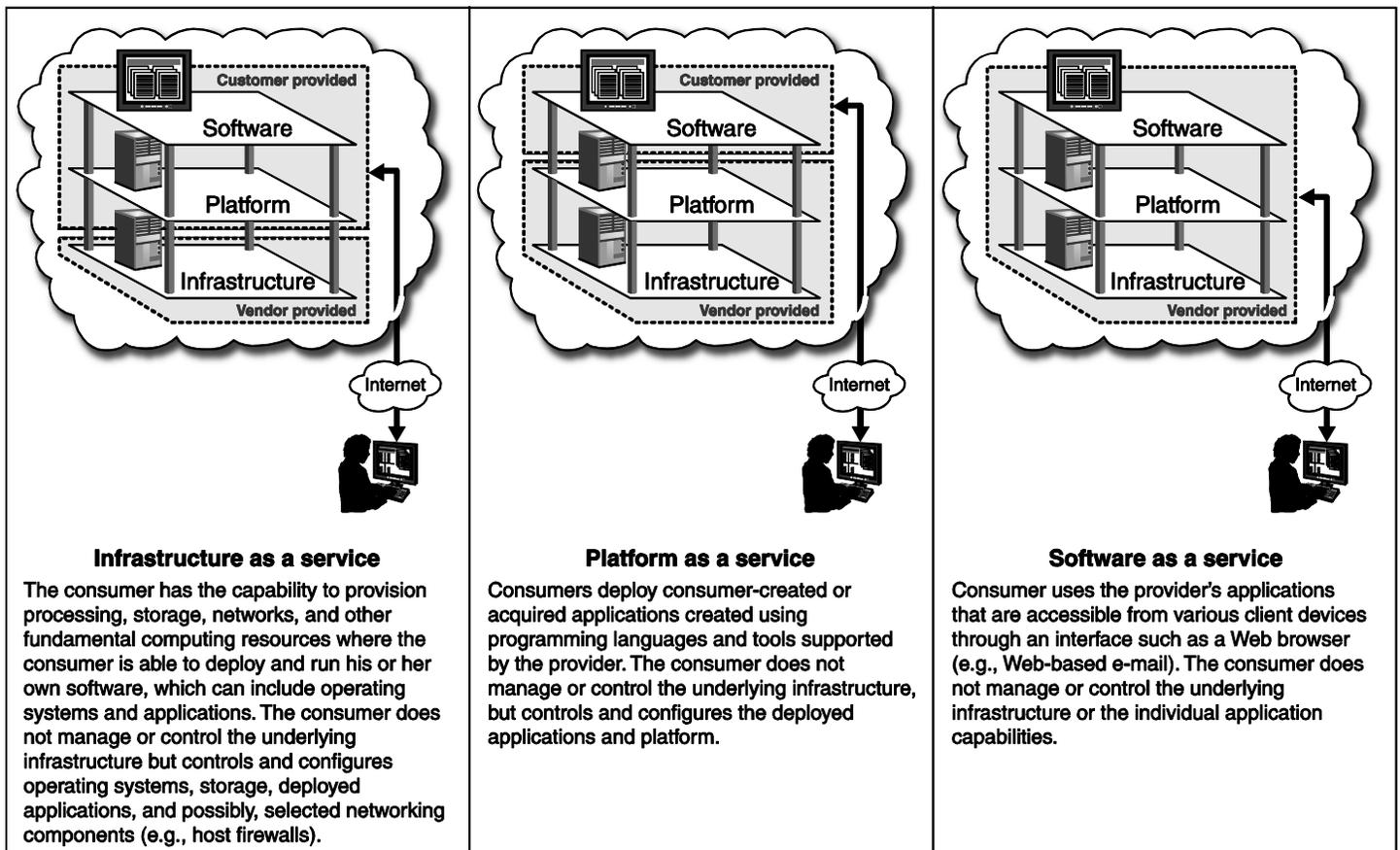
---

<sup>4</sup>GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

<sup>5</sup>GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

<sup>6</sup>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.

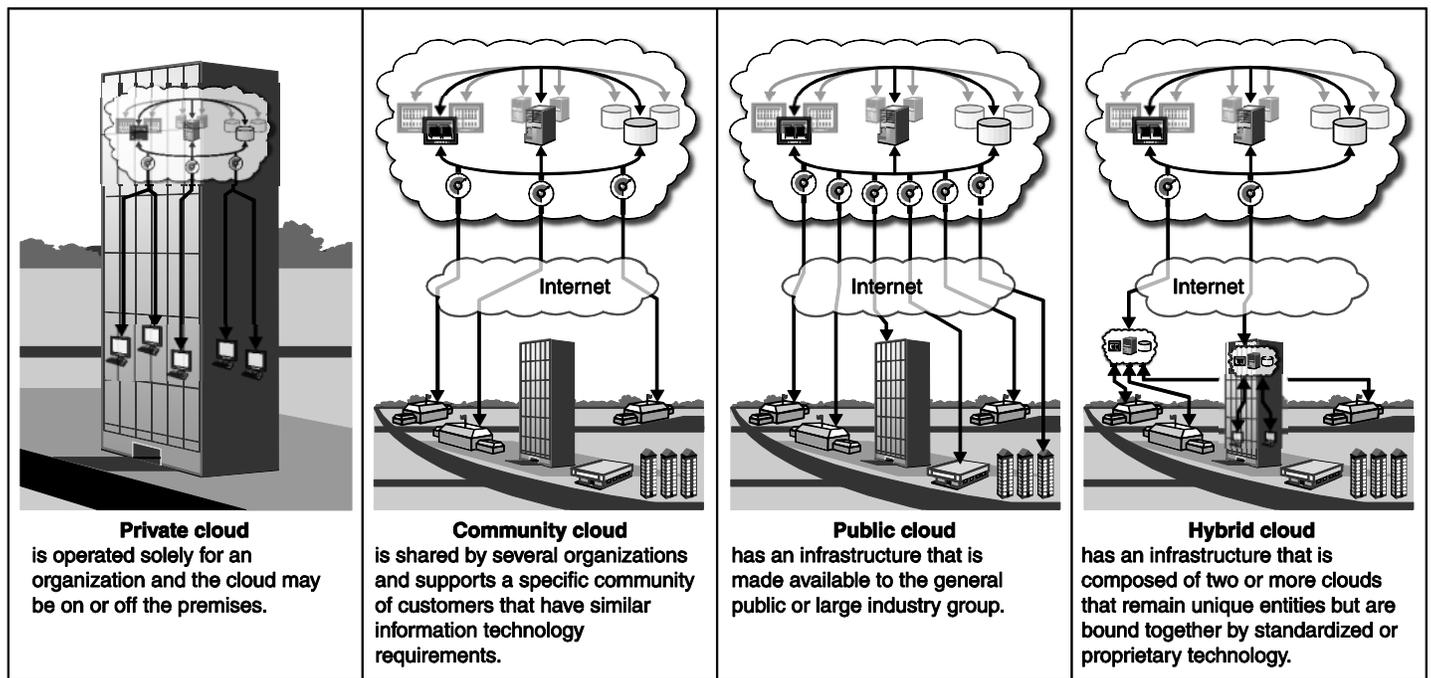
**Figure 1: Cloud Computing Service Models**



Source: GAO analysis of NIST data.

In addition, four deployment models for providing cloud services have been developed: private, community, public, and hybrid cloud. In a private 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. Figure 2 further illustrates each model.

Figure 2: Cloud Computing Deployment Models



Source: GAO analysis of NIST data.

## Cloud Computing Has Both Positive and Negative Information Security Implications

Cloud computing can both increase and decrease the security of information systems. Potential information security benefits include the use of virtualization and automation to 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. In response to the survey we conducted for our 2010 report, 22 of the 24 major agencies also identified low-cost disaster recovery and data storage as a potential benefit.

The use of cloud computing can also 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 noncompliant 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; and
- potentially inadequate background security investigations for service provider employees that could lead to an increased risk of wrongful activities by malicious insiders.

Of particular concern was dependency on a vendor. All 24 agencies specifically noted concern about the possibility of loss of data if a cloud computing provider stopped offering its services to the agency. For example, the provider and the customer may not have agreed on terms to transfer or duplicate the data.

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, under this type of arrangement, one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information. Agencies also stated concerns related to exchanging authentication information on users and responding to security incidents. Identity management and user authentication are a concern for some government officials because customers and a provider may need to establish a means to securely exchange and rely on authentication and authorization information for system users. In addition, responding to security incidents may be more difficult in a shared environment because there could be confusion over who performs the specific tasks—the customer or the provider.

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 stated 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 provider the agency was evaluating when considering the use of cloud computing.

---

---

## Federal Agencies and Governmentwide Initiatives Had Begun to Address Information Security Issues for Cloud Computing, but Remained Incomplete

In our report, we noted that federal agencies had begun to address information security for cloud computing; however, they had not developed corresponding guidance. About half of the 24 major agencies reported using some form of public or private cloud computing for obtaining infrastructure, platform, or software services. These agencies identified measures they were taking or planned to take when using cloud computing. These actions, however, had not always been accompanied by development of related policies or procedures.

Most agencies had 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 were in agreement that compliance and oversight issues were 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 provider. As a result, we reported that the adoption of cloud computing by federal agencies may be limited until these concerns were addressed.

---

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

In our May 2010 report, we also noted that several governmentwide cloud computing security activities had been undertaken by organizations such as the Office of Management and Budget (OMB), General Services Administration (GSA), the federal Chief Information Officers (CIO) Council, and NIST; however, significant work remained to be completed. Specifically, OMB had stated that it had begun a federal cloud computing initiative in February 2009; however, it did not have an overarching strategy or an implementation plan. In addition, OMB had not yet defined how information security issues, such as a shared assessment and authorization process, would be addressed.

GSA had established the Cloud Computing Program Management Office, which manages several cloud computing activities within GSA and provides administrative support for cloud computing efforts by the CIO Council. The program office manages a storefront, [www.apps.gov](http://www.apps.gov),

---

established by GSA to provide a central location where federal customers can purchase software as a service cloud computing applications. GSA had 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. However, GSA officials reported challenges in addressing information security issues as part of the procurement. As a result, in early March 2010, GSA canceled the request and announced plans to begin a new request process. GSA officials stated that they needed to work with vendors after a new procurement was completed to develop a shared assessment and authorization process for customers of cloud services purchased as part of the procurement, but had not yet developed specific plans to do so.

In addition to GSA's efforts, the CIO Council had established a cloud computing Executive Steering Committee to promote the use of cloud computing in the federal government, with technical and administrative support provided by GSA's Cloud Computing Program Management Office, but had not finalized key processes or guidance. A subgroup of this committee had developed the Federal Risk and Authorization Management Program (FedRAMP), 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 had worked 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 had not been established.

NIST is responsible for establishing information security guidance for federal agencies to support the Federal Information Security Management Act of 2002 (FISMA); however, at the time of our report, it had not yet established guidance specific to cloud computing or to information security issues specific to cloud computing, such as portability, interoperability, and virtualization. The NIST official leading the institute's cloud computing activities stated that existing NIST guidance in Special Publication (SP) 800-53 and other publications applied to cloud computing and could be tailored to the information security issues specific to cloud computing. However, both federal and private sector officials had made clear that existing guidance was not sufficient.

---

## Agencies Have Made Progress in Implementing GAO Recommendations, But Additional Actions Are Needed to Assist Agencies in Securely Implementing Cloud Computing

In our May 2010 report, we made several recommendations to OMB, GSA, and NIST to assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing. These agencies generally agreed with our recommendations. Specifically, we recommended that the Director of OMB establish milestones for completing a strategy for implementing the federal cloud computing initiative; ensure the strategy addressed the information security challenges associated with cloud computing, such as needed agency-specific guidance, the appropriate use of attestation standards for control assessments of cloud computing service providers, division of information security responsibilities between customer and provider, the shared assessment and authorization process, and the possibility for precertification of cloud computing service providers; and 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.

In response, in February 2011, OMB issued its *Federal Cloud Computing Strategy*,<sup>7</sup> which references the establishment of a shared assessment and authorization process for cloud computing. In addition, the strategy discusses other steps to promote cloud computing in the federal government, including ensuring security when using cloud computing, streamlining procurement processes, establishing standards, recognizing the international dimensions of cloud computing, and establishing a governance structure. However, the strategy does not address other security challenges such as needed agency-specific guidance, the appropriate use of attestation standards for control assessments of cloud computing service providers, and the division of information security-related responsibilities between customer and provider. Until these challenges are addressed, agencies may have difficulty readily adopting cloud computing technologies.

We also recommended that the Administrator of GSA, as part of the procurement for infrastructure as a service cloud computing technologies, ensure that full consideration be given to the information security challenges of cloud computing, including a need for a shared assessment and authorization process.

---

<sup>7</sup>OMB, *Federal Cloud Computing Strategy* (Washington, D.C: February 2011).

---

In response, GSA issued a request for quote relating to its procurement for cloud services that included the need to use FedRAMP once it is operational. FedRAMP was further developed by GSA, in collaboration with the Cloud Computing Executive Committee, as a shared assessment and authorization process to provide security authorizations and continuous monitoring for systems shared among federal agencies. The CIO Council, in collaboration with GSA, issued a draft version of the shared assessment and authorization process in November 2010;<sup>8</sup> however, the process has not yet been finalized. GSA officials stated that they intend to release additional information on FedRAMP once OMB issues a policy memorandum related to cloud computing, expected in the first quarter of fiscal year 2012.

Lastly, to assist federal agencies in implementing appropriate information security controls when using cloud computing, we recommended that the Secretary of Commerce direct the Administrator of NIST to issue cloud computing information security guidance to federal agencies to more fully address key cloud computing domain areas that are lacking in SP 800-53, such as virtualization, data center operations, and portability and interoperability, and include a process for defining roles and responsibilities of cloud computing service providers and customers.

NIST has also taken steps to address our recommendations. In January 2011, it issued SP 800-125, *Guide to Security for Full Virtualization Technologies*.<sup>9</sup> Virtualization is a key technological component of cloud computing. SP 800-125 discusses the security characteristics of virtualization technologies, provides security recommendations for virtualization components, and highlights security considerations throughout the system life cycle of virtualization solutions. In July 2011, NIST issued SP 500-291, *NIST Cloud Computing Standards Roadmap*,<sup>10</sup> and in September 2011, SP 500-292, *NIST Cloud Computing Reference*

---

<sup>8</sup>CIO Council, *Proposed Security Assessment and Authorization for U.S. Government Cloud Computing*, Draft version 0.96 (Washington, D.C.: November 2010).

<sup>9</sup>NIST, *Guide to Security for Full Virtualization Technologies*, SP 800-125 (Gaithersburg, Md.: January 2011).

<sup>10</sup>NIST, *NIST Cloud Computing Standards Roadmap*, SP 500-291 (Gaithersburg, Md.: July 2011).

---

*Architecture*.<sup>11</sup> Collectively these documents provide guidance to help agencies understand cloud computing standards and categories of cloud services that can be used governmentwide. Among other things, these publications address cloud computing standards for interoperability and portability.

NIST also issued a draft publication on cloud computing, SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*,<sup>12</sup> which addresses the security concerns associated with data center operations and the division of responsibilities among providers and customers. In addition, the guide discusses the benefits and drawbacks of public cloud computing, precautions that can be taken to mitigate risks, and provides guidance on addressing security and privacy issues when outsourcing support for data and applications to a cloud provider. According to NIST officials, SP 800-144 will be finalized in the first quarter of fiscal year 2012.

---

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. Since our report, federal agencies have taken several steps to address our recommendations on cloud computing security, but more remains to be done. For example, OMB has issued a cloud computing strategy; however the strategy does not fully address key information security challenges for agencies to adopt cloud computing. The CIO Council and GSA have also developed a shared assessment and authorization process, but this process has not yet been finalized. In addition, NIST has issued several publications addressing cloud computing security guidance. Although much has been done since our report, continued efforts will be needed to ensure that cloud computing is implemented securely in the federal government.

---

<sup>11</sup>NIST, *NIST Cloud Computing Reference Architecture*, SP 500-292 (Gaithersburg, Md.: September 2011).

<sup>12</sup>NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, Draft SP 800-144 (Gaithersburg, Md.: January 2011).

---

Chairman Lungren, Ranking Member Clarke, and Members of the Subcommittee, this concludes my prepared statement. I am pleased to respond to any questions.

---

## Contact and Acknowledgments

For questions about this statement, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov). Individuals who made key contributions to this testimony include Vijay D'Souza, Nancy Glover, and Shaunyce Wallace.

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

---

## 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 website ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://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 website, <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.

---

## Connect with GAO

Connect with GAO on [facebook](#), [flickr](#), [twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto: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](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

