Testimony of Mike Bradshaw, Director, Google Federal, Google Inc.
before the House Committee on Oversight and Government Reform and the
Subcommittee on Government Management, Organization, and Procurement
Hearing on "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"
July 1, 2010

Chairman Towns, Chairwoman Watson, Ranking Members Issa and Bilbray, and members of the Committee.

Thank you for the opportunity to discuss with you the benefits of migrating more federal agencies to cloud computing. I lead the Google team that provides cloud computing services to the federal government.

Cloud computing is a relatively new term for some, but the cloud is being used today by significant numbers of consumers, businesses, and – increasingly – the public sector. In fact, more than two million businesses use our cloud service, Google Apps. In the cloud, everyday processes and information that are typically run and stored on local computers – email, documents, calendars – can be accessed securely anytime, anywhere, and with any device through an Internet connection. The cloud enables government agencies to replace in-house information technology – which is costly and complex to own, maintain, and secure – with externally provided computing power that offers better and secure performance at dramatically reduced costs.

Google's cloud service allows users to store data or run programs on our geographically distributed, well-secured data centers. Businesses increasingly are choosing to use Google's data centers the same way they now use their desktop computers or on-premise file servers, and in the process are saving money, becoming more efficient, and improving their security. For example, more than 50,000 companies, including 15 percent of the Fortune 500, rely on Google's cloud security service to filter billions of emails against malicious attacks.

In my testimony this morning I would like to make three basic points.

- First, government agencies are finding that the cloud can provide better information security than they have today. Agencies face significant challenges with lost or stolen laptops that contain sensitive data. The cloud enhances security by enabling data to be stored centrally with continuous and automated network analysis and protection. When vulnerabilities are detected they can be managed more rapidly and uniformly. Cloud security is able to respond to attacks more rapidly by reducing the time it takes to install patches on thousands of individual desktops or hundreds of uniquely configured on-premise servers.

- Second, the cloud offers cost savings, efficiency, improved collaboration, and scalability.

By using multi-tenant cloud infrastructure, the costs of computing are spread out over many users instead of just the few users at a particular agency. Government data centers today are typically underutilized, which means they often waste money and energy.

- Finally, although the federal government is starting to adopt cloud computing, more could be done to broaden and accelerate the government's adoption of the cloud. Already, a path to cloud adoption exists, and federal government initiatives like Apps.gov and the Federal Risk and Authorization Management Pilot Program (FedRAMP) are making – or soon will make – progress towards accelerating cloud adoption. We support these efforts and thank the committee for the opportunity to explain the aspects of the government transition to cloud that are working as well as those that can be made even better.

We are excited about the cloud, and we are proud of our achievements in this space. But it is important to note that many companies are offering cloud services. Salesforce.com and Microsoft are just two of the many companies driving innovation and competition in cloud computing. Though most of my testimony will focus on Google products – which are the products I'm most familiar with – there are many cloud solutions out there. And, though we think we offer the best ones, we welcome and encourage the competition and innovation that we see every day in this space.

Cloud Computing Enhances Security

One of the key benefits that cloud computing can provide to the federal government is improved security compared to the status quo model of desktop-centric and on-premise computing.

How we use banks is analogous to cloud computing. Under traditional computing models, we store our critical data on our computers either at home or at work. This is the equivalent of keeping cash under your mattress. Storing data with a cloud computing service provider is like keeping cash in a bank. These companies are security professionals and they typically provide much more consistent security than their customers can on their own.

In today's model of traditional desktop computing there is significant government data stored on portable devices like laptops and USB thumb drives, which can – and often do – get lost or stolen. There are dozens of examples of government computers having been lost or stolen. In 2007, a Transportation Security Administration external hard drive that contained the names, bank records, Social Security numbers, and payroll information of up to 100,000 TSA employees went missing. An Army National Guard laptop that contained the personal information of 131,000 soldiers reportedly was stolen in 2007. A Department of Veterans Affairs portable hard drive that contained sensitive VA-related information on approximately 535,000 individuals was also stolen in 2007. As these examples demonstrate, government agencies have struggled with security under the traditional desktop computing model.

A 2009 Government Accountability Office report on existing government security deficiencies confirmed that many of the data losses occurring at federal agencies over the past few years have been the result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

> *At least nine agencies also lacked effective controls to restrict physical access to information assets. We have previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.*
>
> *In addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction.* (GAO Report GAO-09-701T, at page 6).

Cloud computing can protect against these security vulnerabilities. Moving data across portable devices becomes unnecessary, as cloud computing enables data to be accessed securely from anywhere with an Internet connection.

The most important component of feeling comfortable with one's data in the cloud is trusting a cloud services provider and the practices and policies they have in place. Most people probably do not realize that they have been doing this for years with web-based e-mail or common services like online banking. With Google products, users can set fine-grained access controls for documents, calendars, and other types of information commonly stored in the cloud.

Another important security benefit in the cloud is that agencies and other organizations can control security updates much more consistently and easily. Our research shows most organizations take between 25 and 60 days to deploy security patches, and some corporate chief information officers admit it can take up to six months. Google's cloud service allows everyone to get security updates as soon as they are available, not weeks or months later.

At Google data centers, data is stored on custom-built machines maintained by proprietary software that continually monitors systems. If a threat is found, the system can respond automatically. This structure provides scalability and helps make patching and upgrades more efficient. We can detect security threats across the web early and prepare appropriate defenses, sometimes even before anti-virus companies know about them.

Security is at the core of Google's design and development process; it is built into the DNA of our products. Google is a company that came of age in the Internet era and consistently defends against and adjusts to Internet security threats. We use a combination of people, process, and technology to help secure our systems.

Google employs a dedicated, full-time security team with some of the world's foremost experts in information, application, and network security. The security team can collectively anticipate and fix security issues more quickly and effectively than most single companies or individuals.
This team is responsible for maintaining the company's networks, developing security review processes, and building customized security infrastructure. It also has a key role in developing,

documenting, and implementing Google's security policies and standards. Also, Google's security professionals are empowered by the design of our cloud – we are able to update all of our servers at once.

Google uses an access model designed to only grant as-needed access to customer data. Data centers themselves are equipped with security technologies like thermal imaging cameras, electronic card access systems, 24/7 guard coverage, video analytics, and access logs, among others. Data is obfuscated and split across numerous servers and data centers, making an attack much more difficult because no single user's data resides on a single disk or server.

The data in Google's cloud is stored in geographically distributed data centers. The data is replicated several times so that it will still be available if we are confronted with a power outage in one part of the country. If, for example, a hurricane or earthquake strikes one data center, the application keeps running in the other data centers, and the data stays safe. This has important implications for backup and disaster recovery from a continuity of government perspective. For example, the City of Los Angeles noted that for them, because of their location in an earthquake zone, Google Apps could provide more affordable and efficient backup and recovery solutions than they could otherwise have procured.

Cost Savings, Efficiency, and Other Benefits

Beyond enhanced security, the shift to cloud computing brings demonstrable benefits for saving the government money and increasing the efficiency and functionality of government services. In January 2009, Forrester Research, an independent technology research company, calculated that Google's cloud-based email service, Google Apps Gmail, costs businesses only $8.47 per user per month, versus $25.18 for traditional on-premise email. In case after case, real world examples show that cloud computing costs far less than the traditional desktop model.

For example, in 2009 the City of Orlando was facing aging infrastructure and budget cuts that led it to reconsider managing an in-house email system and running its own servers. In just two months, Orlando was able to switch its 3,000 employees over to a cloud computing service that cut the annual cost per employee from $133 to $50. Now, Orlando employees, from city planners to police officers, will use a web-based email system similar to Google's popular Gmail, but with more storage (25 Gigabytes) and more customized features.

Federal agencies also can reap these significant cost savings. Booz Allen Hamilton, a strategy and technology consulting firm, reported in October 2009 that federal agencies could save 85 percent of their yearly IT infrastructure budgets by moving operations to external cloud providers. In April of this year, the Brookings Institution found that government agencies that switched to some form of cloud computing saw up to 50 percent savings. To put that in context, the federal government is currently spending $76 billion per year on IT, with $20 billion of that devoted to hardware, software, and file servers. That's billions of dollars of taxpayer money.

Cost savings from switching to the cloud are especially relevant given the current under-utilization of government IT resources. The Office of Management and Budget emphasizes that while government data centers increased in number from 400 to 1,100 in a decade, server utilization at those data centers is on average a mere seven percent of full capacity. The cloud will be instrumental in reducing this kind of waste across the federal government's IT infrastructure.

In addition to being more cost efficient, the cloud is also more energy efficient. The City of Los Angeles, which contracted with Google to provide cloud-based email in October 2009, estimates that it will save $750,000 over the next five years simply from the reduction in energy costs.

For its part, the federal government, with over 1,200 of its own data centers, could significantly lower spending and energy consumption by moving some applications to the cloud. The Environmental Protection Agency estimated in 2007 that consolidated, energy-efficient servers and storage systems could cut electricity use by 55 percent. By 2011, the agency estimates that the cut in electricity use could save up to 74 billion kilowatt hours of electricity, $5.1 billion, and 47 million metric tons of carbon dioxide emissions.

Another way the federal government can help to reduce energy consumption is by promoting telework to reduce federal worker commute times and the energy consumed in that commute. As the series of snowstorms that blanketed the Washington, DC region this February showed, teleworking can prevent the government from shutting down completely in an emergency. Teleworking and the cloud can be important components of federal agencies' Continuity of Operations Plans. The cloud can allow teleworkers to easily and securely access their data and work from wherever they happen to be. During the February 2010 snowstorms, the Office of Personnel Management and GSA used cloud computing to share the load with other computer networks in order to keep OPM's Status Alert website running.

The cloud also brings increased functionality. Federal employees can collaborate more easily and effectively because information and applications run in a shared, secure space online, making it easy for people to work together on documents. Two or more people can, for example, edit a web-based document together in real-time while they are hundreds or thousands of miles away from each other – rather than sending it back and forth as an attachment and going through the laborious process of incorporating edits on top of edits. Running applications online means that they can be accessed more easily and securely from any device – a netbook, a smartphone, or any desktop computer where a user happens to be located.

The Federal Government Risks Falling Behind the Private Sector

Today the private sector is using cloud computing to allow employees to access their information and run software applications from anywhere they might be, anytime they need it, from virtually any device that's connected to the Internet. With cloud, it is easier to communicate and work together on documents, calendars, and other collaborative projects. A 2010 report by Gartner, a leading IT research and advisory firm, confirms an acceleration of adoption of cloud computing with the scale of deployments growing. More than 3,000 businesses sign up for Google Apps every day. Businesses are able to save money by spending less on building and managing their own, often under-utilized, IT systems. The same benefits are available for the federal government, with the cost savings ultimately going to taxpayers.

Every day hundreds of millions of consumers use the cloud when they use email services like Microsoft's Hotmail, Yahoo! Mail, or Gmail, which are being run and stored on the Internet rather than locally on a specific computer. Similarly, consumers are using the cloud when they use online banking to look up bank records, balance check books, manage funds, or pay bills. A June 2010 Pew Research Center study projects that within ten years most Internet users will be doing the majority of their computing in the cloud instead of with software that runs and stores programs on a specific computer.

Businesses large and small are rapidly embracing cloud computing. Companies like Amazon.com, Salesforce.com, and Google are providing cloud platforms to allow business customers to improve efficiency and collaboration, lower operating costs, and secure data in ways that are simply not possible using the traditional, desktop-focused IT model.

Though the federal government is adopting at a slower rate compared to industry, we are beginning to see government cloud initiatives and pilot programs. The public sector is already adopting cloud at all levels of government to better serve citizens, reduce costs, lower energy consumption and make more effective use of taxpayer dollars overall. Federal entities currently using the cloud include the Department of Energy, Department of Defense, Department of the Interior, the National Aeronautics and Space Administration, the Social Security Administration, the Security and Exchange Commission, and the General Services Administration.

The DOE cloud computing migration is a good example of progress that is already being made. In 2009, DOE's Lawrence Berkeley National Labs (LBL) began exploring how to use cloud computing and LBL has already moved over 2,300 email accounts to Google Apps and will transition 5,000 accounts later this summer. This cloud deployment uses an identity management system to improve security. Also, the LBL cloud is empowering DOE scientific research teams to foster collaboration and community documentation through the use of Google Docs and other tools.

Simply put, cloud computing is already here and being used every day by individuals, business, and government. But we believe that the federal government could move more quickly, and by doing so it could reap benefits similar to those enjoyed by the private sector. The opportunity to switch to the cloud means that the approximately $80 billion per year market for federal government IT will see more innovation and competition – along with cost and energy savings, which are critical in today's environment.

Conclusion

We would like to thank Chairman Towns, Chairwoman Watson, Ranking Members Issa and Bilbray, and the members of the Committee for holding this hearing on the use of cloud computing by the federal government. The cloud can help agencies at all levels increase productivity, cut costs, keep pace with technology innovation, and improve security. We look forward to working with you and other government officials to continue to make cloud computing more efficient, cost-effective, and secure.