AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CLOUD COMPUTING: WHAT ARE THE SECURITY IMPLICATIONS?

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

OCTOBER 6, 2011

Serial No. 112–50

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

73–737 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ALAN CARROLL, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies 1
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security 3

WITNESSES

PANEL I

Mr. Richard Spires, Chief Information Officer, U.S. Department of Homeland Security:
Oral Statement 5
Prepared Statement 6
Mr. David McClure, Ph.D., Associate Administrator, Office of Citizen Services and Innovative Technologies, U.S. General Services Administration:
Oral Statement 12
Prepared Statement 14
Mr. Gregory C. Wilshusen, Director of Information Security Issues, Government Accountability Office:
Oral Statement 18
Prepared Statement 19

PANEL II

Mr. James W. Sheaffer, President, North American Public Sector, Computer Sciences Corporation:
Oral Statement 38
Prepared Statement 40
Mr. Timothy Brown, Senior Vice President and Chief Architect for Security, CA Technologies:
Oral Statement 43
Prepared Statement 45
Mr. James R. Bottum, Vice Provost for Computing and Information Technology and Chief Information Officer, Clemson University:
Oral Statement 52
Prepared Statement 54
Mr. John Curran, Chief Executive Officer, American Registry of Internet Numbers:
Oral Statement 62
Prepared Statement 64

APPENDIX

Questions From Honorable William Keating For Richard Spires 73

CLOUD COMPUTING: WHAT ARE THE SECURITY IMPLICATIONS?

Thursday, October 6, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:02 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, Walberg, Marino, Clarke, Richardson, Keating, and Thompson.

Also present: Representative Duncan.

Mr. LUNGREN. We have been informed that we are probably going to have votes at 8—I mean, at 10:20, or something, and then have about four or five votes, and so we will have a delay for our hearing for about 45 minutes. So we are going to try and get started very quickly, get our opening statements in and begin your testimony, and then we will have to break and beg your indulgence on that.

The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee is meeting today to examine the security implications of cloud computing. I would recognize myself for an opening statement.

We welcome our witnesses today and look forward to their testimonies regarding cloud computing phenomena. According to NIST, cloud computing delivers I.T. services and applications to users by enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources.

Cloud computing enables organizations and individuals to access website data and on-line programs without concern about the server's physical location, thereby promising cheaper, faster, more flexible, more effective information technology. Most organizations already utilize some form of cloud computing. On-line shopping and banking are prime examples of how cloud computing has transformed the way in which companies interact with and provide on-line services to customers.

Improved technologies over the years have increased our computing capabilities and reduced costs. This new cloud technology also promises greater I.T. capability at reduced cost.

The administration has issued a Cloud First policy to accelerate the pace at which Government evaluates safe and secure cloud

computing options before making any new I.T. investment. Republican Members of Congress, and I hope our Democratic colleagues, are always looking for ways to reduce Government spending, so any savings from cloud computing would, indeed, be welcome.

However, in spite of this projected I.T. savings, we cannot ignore our responsibility as Members of this Cybersecurity Subcommittee to assure that Government information will be secure in the cloud. GAO reported last spring that security incidents at Government agencies rose 650 percent over the last 5 years.

Our concern is the cloud offers—that the cloud offers a rich target for hackers, criminals, terrorists, and rogue nations. With cyber-espionage affecting every sector of our economy, aggregating important information in one location is a legitimate security concern. You might say it is a target-rich environment.

Security implications cannot be an afterthought. Obviously, they need to be considered as cloud technology is being developed and deployed.

Yesterday we Republicans released our House task force recommendation for cybersecurity legislation. We intend to work with our colleagues on the other side of the aisle because this is not a partisan issue; it is one that we need more work on, and I do believe there is a bipartisan commitment to provide that work. Speaker Boehner has made cybersecurity a top priority, and our committee will be a key player in drafting House legislation.

So as we address our numerous cyber vulnerabilities we must scrutinize new technologies and their attendant risks to ensure that further vulnerabilities will not be created. Cloud advocates argue that even sensitive data can be secure in the cloud. They argue that the cloud providers have the resources to invest at sophisticated security—in sophisticated security systems if necessary.

Different security levels can be designed for the various cloud configurations. The private cloud is appropriate for classifying the most sensitive of personnel data, we are told. Sensitive data can be—can use the hybrid model; nonsensitive data can use the public cloud.

While I.T. savings are important, we cannot ignore the information security risk created by cloud technology. Assessing those risks responsibly will be critical if cloud computing is ever going to be widely accepted.

The Federal cloud computing strategy is designed to ensure the security of Government information and establish a transparent security environment between cloud service providers and the Federal Government. NIST and the General Services Administration have developed the Federal Risk and Authorization Management Program, FedRAMP, to facilitate and lead the development of standards for security, interoperability, and portability.

The strategy states that the transition to a cloud computing environment is an exercise in risk management that entails identifying and assessing risk and taking steps to reduce it to an acceptable level. We look forward to the testimony of Dr. McClure, from GSA, will outline this important FedRAMP program.

Today we intend to examine the benefits and risks of cloud computing, and hopefully identify its security implications. I look for-

ward to the testimony of all of our witnesses this morning regarding this new cloud technology.

I would now recognize the Ranking Member of the full committee, Mr. Thompson, for any statement that he might make.

Mr. THOMPSON. Thank you very much, Mr. Chairman. Before I begin my statement, let me take off on your comments about the Republican caucus' release of its cyber task force recommendations yesterday.

As you know, cyber is an emerging homeland security threat that warrants timely bipartisan action from Congress. The stakes are high and Federal networks alone have seen a 650-fold increase in cyber attacks over the past 5 years.

As you know, the President has submitted to Congress a comprehensive plan, including a legislative proposal. Taking your comments that you look forward to a bipartisan effort on this issue, I can assure you from our side of this committee, we will do just that.

With respect to this morning's hearing on security implications of cloud computing, cloud computing can and does mean different things to different people. The National Institute of Standards and Technology, NIST, has published a definition that provides a starting place for discussing and defining security needs, but not everyone agrees with or conforms to NIST's definition. So as of today, the Federal Government and industry have not reached agreement about how uniform rules and standards that should be adopted to secure the information in the cloud.

This is not something that can be left up in the air. While I embrace technological progress, I also know that every new technology presents great possibilities as well as great challenges. In our eagerness to jump on the bandwagon we often forget to ask about the destination of the wagon, the cost of the journey, and the roads which we will take along the way.

As we embark on this new journey of migrating information to the cloud we must not repeat mistakes of the past. We must be about some of the claims that are made.

For instance, I am told that the cloud will produce cost savings and create efficiencies. I am told that these benefits will be achieved by eliminating the need for data centers, computer hardware, and other public and private sector operations that employ thousands of people. I have to ask about these displaced people.

While every new technology creates displacement, it also provides opportunities. So we must ask what new opportunities will be provided and who will benefit?

Finally, as cloud computing increases the Federal Government's ability to communicate effectively, we must ask how to increase the ability to communicate will affect the security of Government operations.

Mr. Chairman, without clear standards and uniform rules we cannot begin to evaluate how the security of Government data will be affected by cloud computing. Additionally, we must remember that cloud computing must be aligned with the Federal Information Security Management Act, FISMA.

Given that the Federal Government currently uses the services of external vendors to manage its cloud operations, we must ask

how these businesses will comply with FISMA regulations governing auditing and security requirements. Industries cannot effectively compete without understanding the potential regulatory environment that will be caused by widespread use of cloud computing in the Federal Government.

Mr. Chairman, there are many questions that must be resolved. However, I am certain that our witnesses today will be able to shine some light on the cloud.

I yield back.

Mr. LUNGREN. Thank you very much, Ranking Member, for that poetic opening statement.

When the Ranking Member of the subcommittee appears we will give her an opportunity to make her opening statement. Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a very distinguished panel of witnesses before us today on this important topic.

Richard Spires was appointed as the chief information officer of the Department of Homeland Security 2009. He has extensive knowledge in senior level operations and information technology issues through working both the public and the private sectors. Previously oversaw I.T. responsibilities for the Internal Revenue Service as deputy commissioner for operations support, chief information officer and associate information officer for business systems modernization respectively.

Before joining the IRS he served as the president, chief operation officer, and director of Mantas, Inc., a software product vendor. He also spent more than 16 years at SRA International, a systems integration company.

Welcome.

Dr. David McClure was appointed associate administrator of the U.S. General Services Administration's Office of Citizen Services and Innovative Technologies in 2009. Dr. McClure most recently served as the managing vice president for Gartner, Inc.'s government research team.

Before working at Gartner, Dr. McClure served as vice president for e-government and technology at the Council for Excellence in Government. He has also had an 18-year career with the Government Accountability Office.

Greg Wilshusen—is that the proper——

Mr. WILSHUSEN. Perfect.

Mr. LUNGREN. Thank you—is director of information security services at the Government Accountability Office. He has spent over 28 years of auditing, financial management, and information systems prior to this date.

Prior to joining GAO in 1997, he was the senior systems analyst at the Department of Education and served as the comptroller for the North Carolina Department of Environment, Health, and Natural Resources; and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency.

Thank you, gentleman, for all being here. We have the rule of a 5-minute testimony. We have your written statements; they will be included in their totality in the record. We would ask you to go in the order in which I introduced you.

So, Mr. Spires, the Chairman would now recognize you.

STATEMENT OF RICHARD SPIRES, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SPIRES. Chairman Lungren, Mr. Thompson, and Members of the subcommittee, thank you and good morning. Today I will discuss the changes cloud computing is having within the Government and at the Department of Homeland Security. Also, I will discuss how DHS is addressing the security challenges associated with cloud computing.

Simply, cloud computing enables Federal agencies to purchase on-demand I.T. services using a consumption-based business model. Liken cloud computing to the electric power or telecommunications markets: we, as customers, pay for the usage of the service itself, whether it be so much per kilowatt-hour for electric power or minutes of usage for the use of our cell phone. As I.T. matures, many services are becoming commoditized and lend themselves to such a usage-based model.

Cloud computing is truly transforming the I.T. business because it does provide significant benefits to customers. The cloud provides scalability and rapid deployment, full transparency for managing operational costs, and controlling and reducing capital expenses.

Further, cloud computing simplifies the overall administration and cost of I.T. infrastructure. Early projections for DHS look to yield cost avoidance savings of 8 to 10 percent once we transition to cloud infrastructure services.

DHS is taking an aggressive approach to the use of cloud computing, with 12 DHS offerings either in production, awarded, or in the acquisition phase. DHS is currently focused on two deployment models: Our private cloud and the use of the public cloud.

For the DHS private cloud, we manage sensitive information within our two enterprise data centers and use our internal wide-area network. A few examples of DHS private cloud offerings include our Email as a Service, which we expect to have more than 100,000 users live by the end of fiscal year 2012.

SharePoint as a Service will support more than 90,000 users by the end of this calendar year. Development and Test as a Service provides a development and test environment linked to the production environment we enable—to enable successful deployment of new applications. We expect to provision new servers within 1 business day with this new capability, while the legacy model averaged up to 6 months.

WorkPlace as a Service will provide secure, virtual desktop access that seamlessly support mobile devices, to include cell phones and tablets. This service will better enable a mobile DHS workforce to support telework and continuity of operations.

We are embracing the use of public cloud services to manage nonsensitive information. DHS has successfully deployed Self Check in the public cloud, and over the next 2 years will consolidate its public-facing websites, like dhs.gov, to the public cloud.

To effectively manage security risks of cloud computing DHS is leveraging our private cloud environment to enable services to manage sensitive information. The model bolsters information security through our defense-in-depth strategy.

By hosting in the enterprise data centers the DHS private cloud can leverage the existing enterprise security controls as well as leverage the use of our continuous monitoring capabilities and trusted internet connections. By embedding enhanced enterprise security controls in our private cloud, DHS will provide security assurance exceeding that of our existing legacy systems.

For public clouds there is a visibility gap between the provider and customer in which they cannot see into each other's management, operational procedures, and technical infrastructure. To address security concerns of public cloud offerings, this visibility gap must be reduced through a series of requirements for contractual reporting and technical auditing and continuous monitoring data feeds to verify that the provider and customer are meeting their responsibilities.

The FedRAMP program will help Federal agencies address these challenges as they leverage public cloud providers or establish their own private cloud. Continued work on the information security challenges will increase the defensive capabilities of cloud offerings, increasing the assurance level and the ability for Federal agencies to use public cloud computing for more sensitive information.

Looking ahead 5 years, the cloud service commodity market appears poised to grow exponentially. Federal CIOs must focus on preparing departments and agencies to welcome innovation and changes in the way we do business. Already, at DHS we are seeing reduced time to market for new capabilities, reducing our capital expenditures, and gaining transparency into our operational expenses, all while providing improved service.

The benefits of cloud computing far outweigh the challenges.

Thank you.

[The prepared statement of Mr. Spires follows:]

PREPARED STATEMENT OF RICHARD SPIRES

OCTOBER 6, 2011

Chairmen Lungren, Ranking Member Clarke, and Members of the subcommittee, thank you and good morning. Today, I will discuss the changes Cloud Computing is having within the Government and industry and how the Department of Homeland Security (DHS) is pursuing this capability to enhance mission performance and gain efficiencies in Information Technology (IT). This testimony also will provide an overview of the current state of cloud computing at the Department of Homeland Security, outlining the Department's initiatives to move data to the cloud in order to implement the White House's "Cloud First" policy as specified in the "Federal Cloud Computing Strategy" issued February 8, 2011, and the "25 Point Implementation Plan to Reform Federal Information Technology Management" issued December 9, 2010. Finally, I will address the IT security challenges associated with cloud computing and how DHS is addressing such challenges.

MOVING TO THE CLOUD

First, allow me to explain what cloud computing is and why it is so vital. The legacy IT model of separate IT infrastructures for each system—both within the Federal Government and industry—must evolve to meet the growing customer demands within a budget-constrained environment. The traditional model is not well-positioned to reduce time to market for new services or provide transparency for operational expenses. It also introduces higher risk due to up-front capital expenditures. Additionally, customized applications hosted in traditional data center environments cannot scale fast enough to support urgent demand in real-time. These challenges, in addition to potential security vulnerabilities, present a call to action for the Federal Government and industry.

Fortunately, we are experiencing an exciting change within the IT industry—the rise of cloud computing. This evolutionary transformation is fast replacing the legacy IT model not only within private industry but also within the Federal Government.

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, provides the following definition of cloud computing in NIST Special Publication 800–145 (NIST SP 800–145):

"Cloud computing is as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

Cloud computing provides the rapid delivery of computing resources inexpensively to multiple users from a centralized source of related and unique service offerings that is shared by many customers. To provide further context, this model is similar to business models deployed in the electric power, cable, or telecommunications markets. That is, within this model, customers do not fund up-front costs to fully stand up environments, or fund on-going operations and maintenance costs. Instead these capital costs are borne by industry, while the customer only pays for services received in the consumption-based model.

NIST prescribes the following five primary characteristics of cloud computing:

1. On-demand self-service.—A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

2. Broad network access.—Capabilities are available over the network and accessed through standard mechanisms.

3. Resource pooling.—The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4. Rapid elasticity.—Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

5. Measured Service.—Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

NIST also identifies three discrete service offerings, each of a unique value to the customer. As customers move up this offering chain, they gain greater efficiencies, yet more standardization is required:

1. Cloud Infrastructure as a Service (IaaS).—The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). This model provides the most flexibility for the customer, however will not provide all the potential efficiencies gained at the Software as a Service model.

2. Cloud Platform as a Service (PaaS).—The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

3. Cloud Software as a Service (SaaS).—The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Finally, NIST identifies four primary deployment models, which are generally accepted across Government. These deployment models range from models that are

more secure to those that are more available. Federal agencies will employ models based on risk-based decisions that address their financial, operational, and security needs. The four models include:

1. Private cloud.—The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on-premise or off-premise.

2. Community cloud.—The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on-premise or off-premise.

3. Public cloud.—The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud.—The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

DHS is currently focused on two of the four deployment models, private cloud and public cloud. DHS will house our private cloud computing capabilities within our two enterprise data centers, while our public cloud will be hosted by organizations selling cloud services. I will provide more detail on these momentarily, but first allow me to briefly address the differences between the cloud and the traditional IT business model.

THE BENEFITS AND RISKS OF CLOUD COMPUTING

Cloud computing is truly transforming the IT business. It is difficult to say which is more compelling—the cloud's significant scalability and rapid deployment, or full transparency for managing operational costs. For many, controlling and reducing capital expense (the expenditures used to acquire physical assets, including both equipment and office space) is uppermost, while others argue meeting demand is the foremost concern. The cloud addresses both and is clearly becoming vital to how we align IT to support mission and business requirements.

For example, the deployment of private cloud services at DHS enables the Department's many components to outsource hosting and other services capabilities to DHS's two Enterprise Data Centers (EDCs). This model enables components to pay on a per-use basis, rather than standing up isolated capabilities throughout the organization that duplicate efforts and costs. In fact, early projections for these services look to yield cost avoidance savings of 8 to 10 percent once we fully transition to private cloud infrastructure services.

As DHS moves more of its operations to cloud computing models, it will simplify the overall administration and oversight of its IT infrastructure. DHS will move from having to manage operations of its infrastructure at the server level, to one in which DHS ensures that cloud-based service level agreements (SLAs) are being met by the service provider. Such simplification will enable discretionary resources to be moved to better understanding and fulfilling customer needs, so that IT organizations can focus more of their efforts on addressing core business and mission needs.

Migration to the cloud, however, is not without information security risks. The Federal Cloud Computing Strategy specifies:

> . . . it is not sufficient to consider only the potential value of moving to cloud services. Agencies should make risk-based decisions which carefully consider the readiness of commercial or government providers to fulfill their Federal needs.

It is important to recognize that many Federal departments and agencies are targeted by Advanced Persistent Threat (APT) campaigns by adversaries that attempt to compromise Government information systems to further their own objectives. These APT campaigns are aggressive, well-financed, and difficult to detect and prevent. APTs target the systems necessary to achieve their goals, regardless of the cloud or traditional computing environments in use by the Federal department or agency. Some cloud environments have capabilities necessary to defend against and provide recovery from these threats, such as advanced monitoring capabilities and cleared information security professionals, while other cloud environments may not, because the increased costs to provide these security capabilities may price their cloud offering outside of the competitive marketplace for their customers. Thus, the security capabilities of the cloud offering must be considered to determine cloud

readiness before use by a Federal department or agency, and why DHS considers use of both public and private cloud computing important, as I will discuss later.

BUILDING THE CLOUD AT DHS

At DHS, we are pursuing private and public cloud offerings. Specifically, we are establishing private cloud services to manage sensitive but unclassified information, while using the public cloud for non-sensitive information. We have already made significant strides through nine DHS cloud service offerings that are either in the planning, acquisition, or sustainment phase.

DHS has committed to nine current and planned private cloud services:

- *Email as a Service (EaaS)*.—DHS is in the process of rolling out our messaging capability across Headquarters and Federal Emergency Management Agency (FEMA). We expect to have more than 100,000 users DHS-wide on this service offering by the end of fiscal year 2012.
- *SharePoint as a Service (SHPTaaS)*.—We are currently migrating Headquarters and United States Citizenship and Immigration Services (USCIS) users to our secure collaboration program. We expect to have nearly 90,000 users DHS-wide on this service by the end of the 2011 calendar year. This migration will significantly improve information-sharing capabilities across DHS.
- *Development and Test as a Service (DTaaS)*.—Establishing development and test offerings in the cloud will have tremendous positive impact on DHS. Currently, DHS has multiple development environments spread across the Department and industry locations. Because all environments are different, moving new releases to production or changes to existing environments presents high-risk and multiple challenges and new releases or changes may not always work in production, leading to significant inefficiencies. Moving and hosting development and test services to our enterprise data centers provides not only a simple path to transition from project creation to implementation, but also accelerated delivery. In fact, we expect to provision new servers within 1 business day with this new capability, while the legacy model averaged up to 6 months to provision one server. Additionally, this service will provide on-demand testing and application management tools, which will significantly improve the quality of our new offerings. DHS plans to roll out DTaaS over the next 60 days.
- *Infrastructure as a Service (IaaS)*.—Complementary to the Development and Test as a Service (DTaaS) offering is our Infrastructure as a Service (IaaS) offering to provide virtualized production services, including operating systems, network, and storage, that is consistent with new industry standards. These services will provide a logical destination for code developed in the development and test environment. We aim to stand up new services in the cloud in less than 1 week, while the legacy model typically averaged up to 12 to 18 months. DHS expects to have initial IaaS capabilities by the end of the 2011 calendar year.
- *WorkPlace as a Service (WPaaS)*.—Enabling a mobile workforce is a priority within the Department. We are working closely with the Department's other line-of-business chiefs to modernize how DHS employees work. This offering will provide robust virtual desktop, remote access, and other mobile services over the next 24 months. This capability enables telework and Continuity of Operations (COOP), not only in the National Capital Region (NCR), but for DHS personnel Nation-wide. Additionally, we expect to reduce our out-year expenditures on traditional desktop and laptops as we consume more mobile enabling technologies.
- *Project Server as a Service (PSaaS)*.—This offering will provide a robust project management platform to publish project schedules that can more easily be shared across offices, divisions, and components. We expect this service to better enable standardization of project management disciplines and directly support our efforts to improve the management of both IT and non-IT programs. DHS plans to make available PSaaS service within the next 30 days.
- *Authentication as a Service (AuthaaS)*.—We have already established a core fundamental offering that provides robust authentication services across 250,000 Federal and contractor employees. This service eliminated the need for duplicative authentication services, while significantly enhancing the Department's information-sharing needs. Nearly 70 DHS applications are using this service today.
- *Case and Relationship Management as a Service (CRMaaS)*.—Over the next 6 months, we will rollout our Case and Relationship Management offering. This offering, leveraging Enterprise License Agreements (ELAs), will better enable CRM and case workflows across DHS. Utilizing these services, the Department

will be piloting a litigation case management capability for ICE, partnering with TSA on modernizing the redress service, improving customer relationship capabilities within USCIS, and deploying a regulations tracking service for DHS.

- *Business Intelligence as a Service (BIaaS)*.—The Department is already piloting an early version of a Business Intelligence capability which started in March 2011 and will run through fiscal year 2012. The Department will leverage this current offering to enhance transparency into departmental programming and expenditures. By the end of fiscal year 2012, we expect the Department will have visibility to information sources across the investment life-cycle, including IT, financial, human resources, asset management, and other information sources. Based on the successful pilot and maturing offerings in service, the Department will look to move to a full Business Intelligence as a Service offering in fiscal year 2013.

Establishing these private cloud services is critical to our success. Our private cloud offerings will provide real value to the organization. As mentioned previously, private cloud services will enable components to outsource secure, commodity IT services to DHS's two enterprise data centers to eliminate redundancy and reduce costs, while ensuring information security. Each service will be rolled out with a minimum "Federal Information Security Management Act of 2002" (FISMA) rating of Moderate or High. Clearly, our private cloud services will streamline our time to market and enhance our security posture, better enabling DHS to accomplish its mission.

But DHS is not wedded to only establishing private cloud services at its two enterprise data centers. We are embarking on a public cloud strategy as well. The Department will leverage public cloud capabilities to enhance Government-to-citizen-services and gain operational and financial efficiencies. In addition, the FedRAMP initiative will address critical security concerns of agency Chief Information Officers (CIOs) over the next few years by having cloud services receive provisional security authorities to operate.

The Department has three public cloud initiatives underway. Two are already deployed, and the third will be piloting in Quarter 1 of fiscal year 2012.

- *Identity Proofing as a Service (IDPaaS)*.—We successfully deployed an innovative identity proofing service in the cloud in March 2011. This offering met USCIS's EVerify Self Check requirement to allow individuals in the United States to check their employment eligibility status before formally seeking employment and is the first on-line E-Verify program offered directly to workers and job seekers. This service is now available in more than 20 States, including the District of Columbia. This voluntary, free, fast, and secure service was developed through a partnership between the DHS and the Social Security Administration (SSA).
- *Enterprise Content Delivery as a Service ECDaaS*.—For the past several years, DHS has used cloud service for Enterprise Content Delivery (ECD) to ensure our public-facing websites are always available. The private sector uses this capability extensively, and DHS adopted EDC for protection against denial of service attacks, to help manage surge requirements, and to significantly reduce hosting costs. This service proved invaluable during the July 4, 2009, denial of service attack on multiple Federal websites. DHS.gov experienced a nearly 100-fold increase in traffic, and no services were lost to the public. The Department has 70% of its externally-facing websites using this service today.
- *Web Content Management as a Service (WCMaaS)*.—Finally, building off our success with our "RestoretheGulf.gov" implementation in the public cloud in late fiscal year 2010, the Department awarded a public cloud hosting contract off the General Services Administration's (GSA) Infrastructure as a Service (IaaS) Blanket Purchase Agreement (BPA). Within this offering, the Department will leverage open source software hosted in the public cloud and consolidate all public-facing DHS websites. We expect to complete this consolidation over the next 2 years. During the next 6 months, the Department will pilot multiple websites in the cloud, including websites from U.S. Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), and Federal the Emergency Management Agency (FEMA).

DHS has taken an aggressive stance regarding the use of both private and public cloud computing services. The Department continues to evaluate its enterprise needs, and we certainly expect to deploy additional cloud services. Further, as the FedRamp model is deployed across the Federal Government, we anticipate that there will be a number of public cloud offerings that have been provisionally certified at the FISMA Low and Moderate levels within the next 2 years. Given DHS's mission, we believe a robust private cloud solution will always be needed for DHS's

most sensitive applications and data. Further leverage of public cloud services will enable the Government to ensure there is robust competition for such services, driving down costs and improving overall service levels.

SECURING THE CLOUD AT DHS

As stated earlier, at DHS, we are pursuing private and public cloud offerings, and the DHS cloud security strategy employs both public and private cloud services as a risk mitigation tool. The move to DHS's private cloud model bolsters information security through the DHS IT security Defense-in-Depth (DiD) strategy. DiD is built upon a robust security architecture and enterprise architecture, and adopts the NIST definition of private cloud computing. Hosting in the enterprise data centers is a primary feature of the DHS private cloud and provides multiple subordinated services, allowing components and systems to inherit the inherent enterprise security controls for system security. The DHS private cloud includes the full DHS enterprise security capabilities outlined in the DiD, including security operations, OneNet, Trusted Internet Connections (TICs), and Policy Enforcement Points (PEPs). The technologies are from the various programs within the layers of the DiD and aids in combating advanced threats, providing enterprise security controls to all users in DHS, regardless of their component and mission function.

For the DHS private cloud, we are leveraging continuous monitoring and migration to common controls at the DHS data centers. Embracing information security controls through an inherited approach allows large, complex organizations like DHS to build on economies of scale in a private cloud infrastructure to reduce the workload for individual system owners. As common controls are defined and vetted by the DHS enterprise and provided as a service to system owners, only the system-specific controls need to be defined and implemented by system owners. By centrally managing the development, implementation, and assessment of enterprise common security controls at the DHS enterprise data centers and through the DHS private cloud, security responsibility can be shared across multiple information systems.

While private clouds incorporate new technologies that may be challenging to secure, public clouds introduce additional risks that must be addressed through controls and contract provisions that ensure appropriate accountability and visibility. Though many distinctions can be drawn between public and private cloud computing, a fundamental measure of readiness is their ability to meet security requirements. By design, FedRAMP provides a common security risk model that supplies a consistent baseline for cloud-based services, including security accreditation designed to vet providers and services for reuse across Government. Reducing risk and bolstering the security of clouds, while ensuring the delivery of the promised benefits, FedRAMP not only applies to public cloud services, but private, too. Ultimately the consumption of cloud services requires acknowledgement of a shared responsibility and governance. From the fact that accountability can never be outsourced from the Authorizing Official (AO) to the need to continue to meet Government requirements, all require acknowledgement of a shared responsibility between the cloud service provider and customer. For public clouds, there is a "visibility gap" between the provider and customer, in which they cannot see into each other's management, operational, and technical infrastructure, and procedures. As such, the visibility gap must be reduced through a series of requirements for contractual reporting and technical auditing and continuous monitoring data feeds. The key to secure use of cloud computing is the shared understanding of the division of security responsibilities between provider and client, and the ability to verify that both are meeting their responsibilities. As DHS advances in the use of public cloud computing, we will be ensuring we have the proper visibility based on a determination of risk given the cloud service and underlying data in order to ensure the security of our information.

NEW CHALLENGES FOR CIOS

While cloud computing is fundamentally changing Federal Government IT, it is not without its challenges. The decision to embrace cloud computing is a risk-based management decision, supported by inputs from stakeholders, including the CIO, Chief Information Security Officer (CISO), Office of General Counsel (OGC), privacy official, and the program owners. From a security perspective, agency CIOs face a number of issues in delivering both private and public cloud capabilities. These issues range from determining different levels of security visibility and responsibilities, ensuring strong authentication, adopting and implementing standards for cloud portability and interoperability, to establishing contingency planning that recognizes cloud computing is a shared capability and identifying new opportunities for

real-time continuous monitoring capabilities but require new audit technologies implemented within the cloud environment.

Cloud computing also leads to significant management and governance shifts for a department or agency. CIOs must work closely with acquisition, procurement, and finance communities to address the new business paradigm represented by cloud computing. While cloud computing requires some technological change, the most significant changes will be to the business and contracting models. Such models will need to ensure that agencies can move forward effectively with cloud solutions while maintaining necessary Federal control and oversight, complying with Federal procurement and competition laws and requirements, and managing funding limitations. CIOs must also address changes to the workforce based on this changing paradigm. As the cloud transforms the way CIOs deliver IT service, the traditional roles of IT specialists change, too. CIOs must provide leadership to update skills for existing personnel and recruit new staff in an environment under significant change.

These challenges are already inherent in the CIO's role. And, they have one thing in common—change. Perhaps above all, the cloud challenges CIOs to lead cultural change within their organization.

THE FUTURE OF THE CLOUD

Looking forward, as FedRAMP and Federal acquisition models mature, the options for Federal agencies to leverage public and community clouds clearly provide real value to citizens. Continued work on information security challenges will increase the defensive capabilities of cloud offerings, increasing the assurance level and the ability for Federal agencies to use cloud computing for more sensitive information.

For example, community clouds could provide agencies with a suite of specialized cloud hosting services that include the standard IaaS, PaaS, and SaaS offerings with a more robust security, business, and mission portfolio offerings such as financials, law enforcement, intelligence, medical/health, and the increased security and privacy controls necessary to process more sensitive information. The value of a community of cloud offerings across a broad suite of verticals for customers may be realized as the true evolution of the cloud in the years to come.

Looking 5 years into the future, the cloud service commodity market appears poised to grow exponentially, creating significant innovation as a result of intense competition. Federal CIOs must focus on preparing departments and agencies to help foster and welcome innovation that changes the way we do business. By embracing the opportunities of cloud computing, we will redefine the role and capabilities of IT in the Federal Government.

While we in the Federal Government face challenges to successfully implementing cloud capabilities to enhance mission performance and realize cost efficiencies, the benefits far outweigh the challenges. Already at DHS we are seeing reduced time to market for new capabilities, and soon, we will begin to reduce our capital expenditures while gaining transparency into our operational expenditures in ways we have never been able to before. In conclusion, we should not think of the cloud as simply a technology opportunity. It is a far more interesting discourse—and a significant change to the fundamental business model for how IT is delivered in the Federal Government.

Thank you.

Mr. LUNGREN. Thank you very much.

Dr. McClure.

STATEMENT OF DAVID MC CLURE, PH.D., ASSOCIATE ADMINISTRATOR, OFFICE OF CITIZEN SERVICES AND INNOVATIVE TECHNOLOGIES, U.S. GENERAL SERVICES ADMINISTRATION

Mr. MCCLURE. Thanks, Mr. Chairman.

Good morning, Mr. Thompson and Mr. Keating.

Thanks for having me here on behalf of GSA to talk about cloud computing and cloud security.

I just wanted to start by making two critical points about cloud computing itself. It really offers a compelling opportunity to substantially improve the efficiency of the Federal Government. When it is implemented with sound security risk management ap-

proaches, cloud computing can ensure more consistent protection of the Government's I.T. infrastructure, our data, and our applications.

Second, the practical use of cloud computing really offers substantial performance benefits for Government. For example, tangible cost reductions resulting from more efficient data storage, web hosting, and even analytics performed on our vast data repositories.

It can enhance productivity by shifting some of our workforce to high-value process improvement activity, problem solving, and customer service excellence. It allows us greater flexibility and scalability, as Richard just talked about—the ability of CIOs to actually stand-up services in hours, days, rather than months, and in some cases, years. It allows or creates an improved self-service environment: On-line, streamlined, commodity-like purchasing for I.T. resources rather than a very long and arduous I.T. acquisition.

We are playing a leadership role in facilitating easy access to cloud-based solutions from commercial providers that meet Federal requirements, such as virtualization technologies for our data centers in the Government, cloud e-mail, disaster recovery and backup, and infrastructure storage. Our Government-wide procurement vehicles enable agencies to evaluate viable cloud computing options that meet their business needs.

Now let me turn to cloud security. Cloud computing, like any technology, presents both known and new risks alongside the benefits that it offers. Different types of cloud services—public, private, community, hybrid—create their own set of security challenges in the Government setting.

To address these risks in a more uniform and comprehensive manner we will soon launch a new Government-wide cloud security program.

Mr. Chairman, you referred to it, the FedRAMP program.

We have worked in close collaboration with cybersecurity and cloud experts in NIST, DOD, DHS, NSA, OMB, the Federal CIO Council, and with private industry. Let me be real clear: The intent of FedRAMP is to strengthen existing security practices associated with cloud computing solutions, which, in turn, will build greater trust between providers and consumers and accelerate appropriate adoption of security cloud solutions across the Government.

FedRAMP ensures consistency and quality of system security certification and accreditation; it creates a transparent and trusted security environment in Government that will incentive more reusability of security testing and authorizations; and it fosters the push toward near real-time security assistance monitoring. It does this by standing up six critical capabilities.

It standardizes a minimal baseline for Government-wide security controls for low and moderate risk cloud systems based upon existing NIST standards and additional controls vetted with all interested parties. It manages a process for accrediting independent third-party assessors to ensure greater competency, consistency, and compliance with required Government security controls.

It creates a joint authorization board, comprised of CIOs and technical representatives from DOD, DHS, and GSA, to grant provisional authorizations for cloud systems that can be leveraged by

multiple agencies. It also allows agencies to focus on their own specific security requirements and address legitimate deltas with the baseline controls rather than repeating work already competently done by another Federal entity.

Consistent with FISMA changes, it requires cloud service providers to perform continuous monitoring, especially for persistent threats, and will eventually automate the exchange of status information on specific controls on a near-time—near real-time basis. In concert with DHS, it controls and manages the incident response, mitigation, and proof of resolution for FedRAMP-authorized cloud systems.

Last, it will create a secure data repository to facilitate Government access to security authorization packages, sample contract language and templates, examples of cloud service-level agreements, best practices, and continuous monitoring information.

So, Mr. Chairman, we think these kinds of steps can really advance more secure cloud computing in the Government. I am happy to answer questions for the subcommittee.

[The prepared statement of Mr. McClure follows:]

PREPARED STATEMENT OF DAVID MCCLURE

OCTOBER 6, 2011

Chairman King, Ranking Member Thompson, and Members of the subcommittee: Thank you for the opportunity to appear before you today to discuss the General Service Administration's (GSA) leadership role in on-going efforts to enable and accelerate adoption of secure cloud computing across the Federal Government. Cloud adoption is a critical component of the administration's plan to improve management of the Government's IT resources. The IT reforms we have underway are enabling agencies to use information more efficiently and effectively, delivering improved mission results at lower cost.

CLOUD COMPUTING ADOPTION IN THE FEDERAL GOVERNMENT

Before I discuss the security of cloud computing, and the Federal Risk Authorization and Management Program (FedRAMP) in particular, I would like to make a two important points. First, cloud computing offers a compelling opportunity to substantially improve the efficiency of the Federal Government. It moves us from buying and managing physical assets to purchasing IT as a commoditized service. Agencies pay for only IT resources they use in response to fluctuating program demands, avoiding the expenses of building and maintaining costly IT infrastructure. When implemented with sound security risk management approaches, cloud computing also ensures more consistent protection of the Government's IT infrastructure, data, and applications.

Second, practical use of cloud computing offers substantial performance benefits for the Government. Federal agencies are moving to consolidate and virtualize the more than 2,000 Federal data centers. Cloud technologies provide an ideal path forward to maximize value in IT investment dollars while substantially lowering costs—an essential focus given Federal budget constraints. Case studies we have collected from agencies point to benefits that include:

"tangible cost reductions (data storage, web hosting and analytics performed on the Government's vast data repositories);
"enhanced productivity (shifting workforce to more high-value process improvements, problem solving, and customer service excellence);
"greater flexibility and scalability (enabling CIOs to be much more responsive to pressing service delivery expectations); and
"improved self-service capabilities (on-line streamlined commodity-like purchasing for IT resources rather than long, arduous IT acquisitions)."

GSA is playing a leadership role in facilitating easy access to cloud-based solutions from commercial providers that meet Federal requirements. This will enable agencies to analyze viable cloud computing options that meet their business and technology modernization needs, while reducing barriers to safe and secure cloud

computing. We are developing new cloud computing procurement options with proven solutions that leverage the Government's buying power. These cloud procurement vehicles ensure effective cloud security and standards are in place to lower risk and foster Government-wide use of cloud computing solutions such as virtualization technologies for Government data centers, cloud e-mail, disaster recovery/backup, and infrastructure storage. Useful information about cloud computing and available solutions is accessible from our web page, *Info.Apps.gov*.

GSA's Federal Cloud Computing Initiative was started and is managed under GSA's e-Government program. In fiscal year 2010 and fiscal year 2011 GSA's Federal Cloud Computing Initiative (FCCI) Program Management Office (PMO) focused on five primary tasks:

- Establishing procurement vehicles that allow agencies to purchase IT resources as commodities, culminating in the award of the Infrastructure as a Service (IaaS) Blanket Purchase Agreement under GSA Schedule 70 to 12 diverse cloud service providers;
- Addressing security risks in deploying Government information in a cloud environment—resulting in the development of the Federal Risk Authorization Management Program (FedRAMP);
- Establishing a procurement vehicle that will allow agencies to purchase cloud-based e-mail services, which created GSA's Email as a Service (EaaS) Blanket Purchase Agreement;
- Supporting the Government-wide collection and assessment of data center inventories, and assisting agencies in the preparation and execution of plans to close and consolidate data centers. Current work includes developing a comprehensive data center Total Cost Model for agencies to use to analyze alternative consolidation scenarios, enables data-driven decision-making for infrastructure cost and performance optimization. Operationalizing a data center marketplace that would help optimize infrastructure utilization across Government by matching agencies with excess computing capacity with those that have immediate requirements is also being pursued.
- Creating apps.gov, an on-line storefront that provides access to over 3,000 cloud-based products and services where agencies can research solutions, compare prices and place on-line orders using GSA's eBuy system.

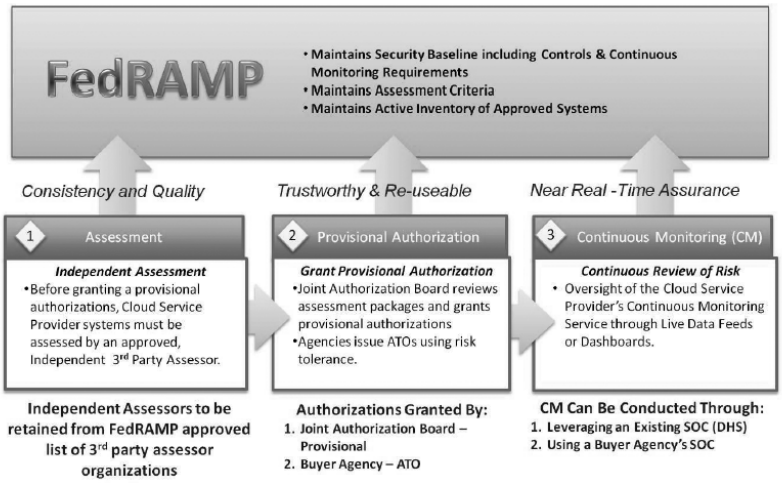
Initial funding provided by the e-Gov Fund has allowed GSA to be an effective catalyst for secure cloud technology adoption Government-wide. However, there are critical activities that still need to be accomplished to fully realize the significant cost savings and productivity improvements that GSA can help agencies achieve. The continuation of these cost-saving initiatives is dependent on fiscal year 2012 eGov Fund budget levels and decisions.

FEDRAMP: ENSURING SECURE CLOUD SYSTEMS ADOPTION

Cloud computing—like any technology—presents both known and new risks alongside the many benefits outlined above. To address these risks in a more uniform and comprehensive manner, we will soon launch a new Government-wide cloud security program—the Federal Risk and Authorization Management Program (FedRAMP). The primary goal of the administration's Cloud First policy is to achieve widespread practical use of secure cloud computing to improve operational efficiency and effectiveness of Government. Today, each agency typically conducts its own security Certification and Accreditation (C&A) process for every IT system it acquires, leading to unnecessary expense, duplication, and inconsistencies in the application of NIST-derived security controls testing, evaluation, and certification procedures. According to the 2009 FISMA report to Congress, agencies reported spending $300 million annually on C&A activities alone.

At GSA, we have worked in close collaboration with cybersecurity and cloud experts in NIST, DHS, DoD, NSA, OMB, and the Federal CIO Council and its Information Security and Identity Management Subcommittee (ISIMC) to develop FedRAMP. An OMB policy memo officially establishing the FedRAMP program is expected shortly. The intent is to strengthen existing security practices associated with cloud computing solutions which, in turn, will build greater trust between providers and consumers and accelerate appropriate adoption of secure cloud solutions across Government. Accordingly, FedRAMP establishes a common set of baseline security assessment and continuous monitoring requirements for FISMA low- and moderate-impact risk levels using NIST standards that must be adhered to by all cloud systems. Figure 1 illustrates how FedRAMP will address three fundamental challenges with how the Federal Government approaches ensuring cloud security.

Figure 1: FedRAMP – Addressing Three Critical Challenges to Cloud Security



Ensuring Consistency and Quality in Cloud Security Certification and Accreditation

FedRAMP approves qualified, independent, third-party security assessment organizations, ensuring consistent assessment and accreditation of cloud solutions based on NIST's long-standing conformity assessment approach. As noted above, security C&As are currently performed with varying quality and consistency. This is true for situations where a third-party service provider is contracted to do a security assessment of a CSP-provided system, product, or service and where Government security organizations perform the work themselves. As a result, trust levels are low for reusing this work across agencies.

To address this challenge, FedRAMP will require that cloud services providers be assessed using these approved, independent, third-party assessment organizations (3PAOs). The 3PAOs will initially apply for accreditation through the FedRAMP PMO and be assessed using established conformity assessment criteria developed by NIST. This will ensure higher-quality assessments, done much more consistently, using agreed-upon FedRAMP security assessment controls. This can save millions of dollars in expenses borne both by Government and industry in running duplicative assessments of similar solutions by each agency.

Building Trust and Re-Use of Existing C&A Work

All IT systems, including cloud solutions, must receive an Authority to Operate (ATO) from the buying agency before they can be made available for purchase and implemented. The ATO is based on a thorough review by agency security professionals of the security packages submitted following the C&A process described above. To accelerate cloud adoption and enable C&A re-use, FedRAMP will provide a single, provisional authorization that can be used by all agencies as the basis for issuing an ATO. If additional security assessment evaluation and testing is needed for specific agency cloud implementations, the C&A should only address any additional controls needed above the existing FedRAMP-approved baseline.

FedRAMP establishes a Joint Authorization Board (JAB) that reviews all cloud systems that have been assessed by approved 3PAOs using FedRAMP controls and processes. The JAB membership consists of CIOs and Technical Representatives from DOD, DHS, and GSA. The JAB reviews the C&A work and decides whether to grant the "provisional authorization"—a seal of approval on the C&A work. The security packages, assessments and documented decisions will be accessible within Government from a secure central repository. While each agency must grant its own ATO for systems under its control, FedRAMP will facilitate greater use of an "approve once, and use often" approach, leveraging more ATOs across Government.

Moving Towards More Real-Time Security Assurance

FedRAMP shifts risk management from annual reporting under FISMA to more robust continuous monitoring, providing real-time detection and mitigation of per-

sistent vulnerabilities and security incidents. Using the expertise of industry, NIST, NSA, DHS, and ISIMC, nine initial continuous monitoring controls have been identified that are among the most common persistent threat vulnerabilities in cloud and non-cloud systems environments. Cloud Service Providers (CSPs) must agree to near-real time reporting of continuous monitoring data feeds to DHS and/or agency Security Operations Centers (SOCs). We are finalizing data reporting details, with the expectation that the process will eventually use automated data feeds to maximize efficiencies and timeliness. When done in addition to the C&A evaluations, this will result in valuable situational cyber awareness—a relevant and timely picture of a CSP's security posture. In addition, this approach provides visibility of prompt mitigation and tangible evidence of resolution; ensuring quick steps are taken to minimize threats to Government data and operations.

In short, FedRAMP offers the following improvements for cloud security assessments conducted in the Federal Government:

- ✓ **Cloud Security Requirements:** Standardizes a minimum, baseline set of government-wide security controls based on *NIST Special Publication 800-53 Revision 3 Risk Management Framework* for low or moderate risk cloud systems.
- ✓ **Assessor Accreditation:** Manages process for accrediting independent, third-party assessors to ensure competency, consistency, and compliance.
- ✓ **Assessment & Authorization:** Validates cloud services provider's security authorization packages to ensure consistent application of standard controls. Empowers a Joint Authorization Board (JAB) comprised of CIOs from DoD, DHS, and GSA, to issue provisional authorization for cloud systems. Agencies can leverage this baseline in granting their own ATOs and focus on their specific requirements "delta" for any additional C&A work.
- ✓ **Continuous Monitoring:** Based on an *initial* set of controls, performs continuous monitoring, automates oversight of government-wide authorized systems, and notifies participating agencies of any system changes to the authorized risk posture.
- ✓ **Incident Response Coordination:** Coordinates control and management of incident response for FedRAMP authorized cloud systems.
- ✓ **Data Repository:** Maintains up-to-date list of all FedRAMP authorized systems; facilitates secure access to security authorization packages; maintains contracting templates, SLAs, etc.

There is strong support and demand for stronger cloud security from agencies seeking to adopt cloud services, as required by the administration's Cloud First policy. Industry cloud services providers need to know the specific cloud security capabilities for which they are accountable. They also desire more efficiency in how C&As and ATOs are leveraged Government-wide to avoid unnecessary, duplicative, costly security evaluations. Ensuring IT security is an on-going challenge. We fully expect to make improvements to the process based on collaboration with all key stakeholders, including industry, lessons learned, and the continuous evolution of security standards and controls based upon the careful, deliberative work of NIST.

FedRAMP will be launched in phases that incrementally build toward sustainable operations and allows for risk management by capturing on-going lessons learned and process improvement. Initial rollout will occur this Fall. Initial Operational Capabilities will have limited scope and cover a relatively small number of cloud service providers. Full operations are expected to begin next Spring with more robust operational capabilities and larger intake of cloud service providers for FedRAMP review and approval. Late in 2012, we expect sustaining operations to scale by demand using a privatized board for 3PAO accreditation. We will discuss the rollout in more depth with the Congress, Government executive branch agencies, industry, and the public prior to the initial launch date.

CONCLUSION

Considerable progress has been made in adopting successful cloud solutions. "Cloud computing" is now an accepted part of the Federal IT lexicon. However, there continues to be a need for more thorough understanding of cloud deployment models, unique security implications, and data management challenges. Agency executives should not focus on cloud technology itself; rather, they should focus on the desired outcome driving the need for cloud adoption delivered in a secure environment.

FedRAMP will provide a sound, cost-effective framework for secure cloud computing. CIOs need to work with their line of business executives and program managers to develop and deploy effective cloud roadmaps that address pressing agency

mission needs, taking into account appropriate security and risk management. Agencies should analyze business needs and identify cloud solutions that best fit their requirements by making secure cloud adoption part of an overall IT portfolio management and sourcing strategy. Consistent with the Federal Cloud Computing Strategy, NIST is currently working on the first draft of a USG Cloud Computing Technology Roadmap, to be released for public comment in November, 2011. If linked to cloud provider products and services, it would greatly assist in this decision-making.

Mr. Chairman, thank you for the opportunity to appear today. I look forward to answering questions from you and Members of the subcommittee.

Mr. LUNGREN. Thank you very much, Dr. McClure.

Now, Mr. Wilshusen.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Lungren, Mr. Thompson, Mr. Keating, thank you for the opportunity to participate in today's hearing on cloud computing security. I believe this is a vitally important topic.

Earlier this week GAO issued a report on Federal information security in which we note that the number of security incidents reported by Federal agencies increased by over 650 percent during the past 5 years. This fact helps to underscore the need for effective security in cloud computing environments.

Today I will describe the information security implications of Federal use of cloud computing services. I will also discuss GAO's previous reporting on Federal efforts and guidance on cloud computing and agencies' actions to implement our recommendations to improve cloud security.

But if I may, Mr. Chairman, I have first like to recognize Assistant Director Vijay D'Souza and Shaunyce Wallace, from my staff, who are here, and also Nancy Glover, who is not here, for their diligent efforts in reviewing cloud security as well as preparing my statement.

Mr. Chairman, cloud computing can have both positive and negative information security implications. Potential security benefits include those related to broad network access, possible economies of scale, and the use of self-service technologies. For example, Federal agencies frequently cited the prospect of on-demand security controls, the consistent application of those controls, and low-cost disaster recovery and data storage as potential benefits.

However, the use of cloud computing can also create numerous information security risks. Twenty-two of the 24 major Federal agencies reported that they were either concerned or very concerned about the potential security risks with cloud computing.

These risks include the ineffective or noncompliant security practices of the service provider, an inability to examine controls of the provider, the prospect of data leakage to unauthorized users, and the loss of data if the cloud service is terminated. These risks generally relate to dependence on the security practices and assurances of the service provider and the sharing of computing resources.

In a report GAO issued last year, we noted that Federal agencies had begun efforts to address information security for cloud computing, but specific guidance was lacking and efforts remained in-

complete. We also reported that OMB and GAO—I am sorry, GSA—had launched Government-wide initiatives but had not completed key actions pertaining to cloud computing security.

For example, OMB had not finished its cloud computing strategy or defined how information security issues would be addressed in that strategy. Accordingly, in that report GAO made recommendations to OMB, GSA, and NIST to take several actions to address these issues.

Since that report was issued in May 2010 these agencies have made progress in implementing our recommendations, but additional actions are still needed to assist agencies in securely implementing cloud computing. For example, in February OMB issued its cloud computing strategy, which does reference the establishment of FedRAMP and other security issues; however, it does not address the need for agency-specific guidance, the use of standards for control assessments of cloud service providers, or the division of security responsibilities between customer and provider.

Consistent with our recommendation, GSA, in collaboration with the CIO Council, further developed FedRAMP, as Mr. McClure has indicated in his opening remarks, and intends to issue additional guidance on FedRAMP later this quarter. In addition, NIST has issued three of four guidance documents related to cloud computing and expect to finalize guidelines on security and privacy in the public cloud computing later this quarter. These actions and the issuance of appropriate guidance will help, yet the true test will be their effective implementation over time.

To summarize, Mr. Chairman, the use of cloud computing offers the promise of efficient service, but it also carries risk. OMB, GSA, and NIST have taken steps to develop a strategy, processes, and guidance on cloud computing security. Nevertheless, continued efforts will be needed to ensure that cloud computing is implemented securely in the Federal Government.

Mr. Chairman, this concludes my statement. Be happy to answer any questions.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

OCTOBER 6, 2011

INFORMATION SECURITY: ADDITIONAL GUIDANCE NEEDED TO ADDRESS CLOUD COMPUTING CONCERNS

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* [1] 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 on-line through a browser, instead of through a local computer. Cloud computing can potentially deliver several benefits over current systems, including faster deployment of com-

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

puting 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), and 24 major Federal agencies.[2] 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.[3] 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 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 Government-wide high-risk area since 1997,[4] a designation that remains in force today.[5] 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.

---

[2] 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.

[3] GAO, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems,* GAO–11–463T (Washington, DC: Mar. 16, 2011) and *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure,* GAO–11–865T (Washington, DC: July 26, 2011).

[4] GAO, *High-Risk Series: Information Management and Technology,* GAO/HR–97–9 (Washington, DC: February 1997).

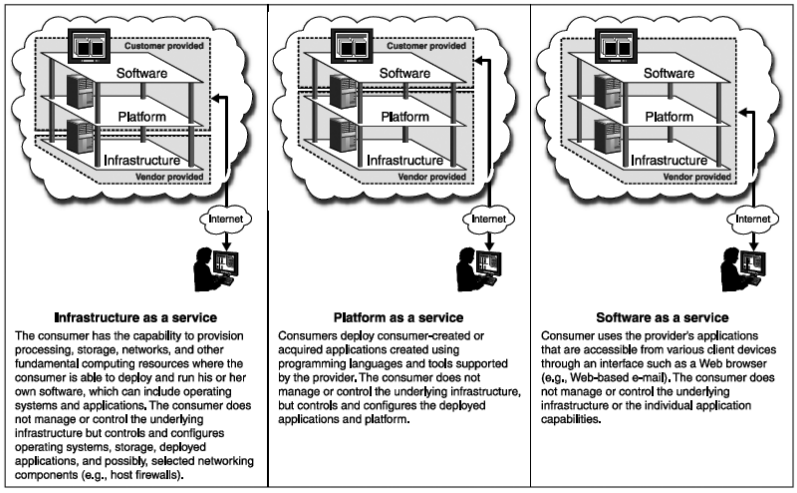
[5] GAO, *High-Risk Series: An Update,* GAO–11–278 (Washington, DC: February 2011).

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.[6] 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.

Figure 1: Cloud Computing Service Models

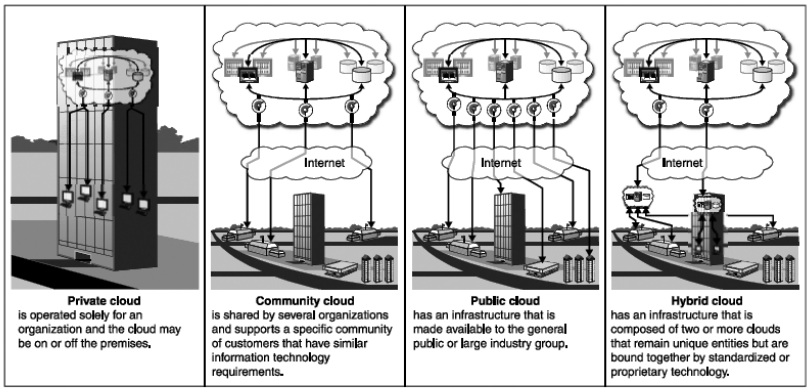


Source: GAO analysis of NIST data.

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.

[6] 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 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 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; 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 GOVERNMENT-WIDE 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 Government-wide 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 Government-wide 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 Government-wide 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,* 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 Government-wide 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 Government-wide security assessment and authorization process for cloud services.

In response, in February 2011, OMB issued its Federal Cloud Computing Strategy,[7] 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.

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;[8] 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.

Last, 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.

---

[7] OMB, *Federal Cloud Computing Strategy* (Washington, DC: February 2011).

[8] CIO Council, *Proposed Security Assessment and Authorization for U.S. Government Cloud Computing,* Draft version 0.96 (Washington, DC: November 2010).

NIST has also taken steps to address our recommendations. In January 2011, it issued SP 800–125, *Guide to Security for Full Virtualization Technologies.*[9] 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,*[10] and in September 2011, SP 500–292, *NIST Cloud Computing Reference Architecture.*[11] Collectively these documents provide guidance to help agencies understand cloud computing standards and categories of cloud services that can be used Government-wide. 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,*[12] 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.

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

Mr. LUNGREN. Thank you very much.

Thank all three of you for that. I understand we are going to have votes in about 10 minutes so we will see if we can get through a couple of 5-minute question periods. I will start.

If I were to summarize what I heard, it is that Mr. Spires and Mr. McClure have the glass-half-full approach, and Mr. Wilshusen, you have the glass-half-empty approach.

Mr. Spires and Mr. McClure, can you tell me which glass I should take up?

Mr. SPIRES. Well, sir, I do have the glass-half-full approach. I believe that cloud computing is going to transform I.T. as things become more commoditized. The world is moving that way; we need to move with it because the advantages are so great.

Mr. LUNGREN. So it is inevitable that we are going to move there?

Mr. SPIRES. I think it is inevitable.

Mr. LUNGREN. So the question we have here is: How secure can we make it?

Dr. McClure, you—if I were to just listen to what you had to say I would be very, very pleased that it is very secure right now or on the process of getting even more secure. But the gentleman to

[9] NIST, *Guide to Security for Full Virtualization Technologies,* SP 800–125 (Gaithersburg, MD: January 2011).

[10] NIST, *NIST Cloud Computing Standards Roadmap,* SP 500–291 (Gaithersburg, MD: July 2011).

[11] NIST, *NIST Cloud Computing Reference Architecture,* SP 500–292 (Gaithersburg, MD: September 2011).

[12] NIST, *Guidelines on Security and Privacy in Public Cloud Computing,* Draft SP 800–144 (Gaithersburg, MD: January 2011).

your left is paid to poke holes in arguments that people like you make, and he has poked some holes.

Sometimes things sound too good to be true, and most of the time I have found that is true. What assurance do we have as we move toward this cloud computing—well, let me put it this way: In the report that we issued yesterday, and this is consistent with what we have heard before this committee, there has been the suggestion that 85 percent of computer intrusions, unwarranted interference, et cetera, could be stopped by good computer hygiene, which suggests that we have a lot to do in terms of public and private awareness.

One of the key aspects to security on cloud computing would be awareness. How am I to be able to tell my colleagues and my constituents that the awareness that evidently isn't there now with the way we are doing things is going to be there as we move to computing? Because isn't that the essential question?

You can set up the best sort of secure systems possible, but if there is not the awareness of what you have to do, both in terms of what we are talking about here, the ultimate user, that is, the Government employee, but also the vendor, and the vendor's employees—it is not going to happen. So is that computed into what you said today, that we have the awareness, we are going to have the awareness, it is built in, or it is easier in a cloud computing atmosphere than what we have had thus far?

Mr. MCCLURE. Well, thank you, Mr. Chairman. As Greg knows, I used to be a hole-poker, as well, because I sat in GAO, so there is no—this is a really challenging area, so I don't think it is a half-full, half-empty glass. We are never done in this area. I think all of us here at the table would agree with that.

We can put the best controls in place, the best policies, the best people, but you are going to always be advancing in your knowledge and in your ability to deter threats and vulnerabilities to your system. So it is a given.

So I think that is one thing we need to do is to dispel the myth that there is some magical control or formula that we are not using and if we just put in place we would—we will be absolutely secure. Security is an on-going exercise.

Mr. LUNGREN. True. But how do we answer the question to those who would be skeptics of what we think we need to do, that if you move in the direction of cloud computing you are necessarily creating greater target-rich environments? That is, if I can invade a cloud that has multiple—more data points than a small network I would target my energies on that, and if I am successful, boy, I really have a tremendous amount of information, and connected information, where I may not have it if it is divided over 2,700 different networks. That is the concern I have expressed to me.

On the other hand, I hear the argument, "Well, wait a second. We can put more capital investment into cloud technology. They can be more up-to-date, more timely. They can find things more quickly because they have a greater observation point." I understand that.

But I think you understand the point about a greater target-rich environment with the concern people then have that you have got

to have a promise that the security of the cloud is going to be measurably better than the security we have in the current system.

Mr. MCCLURE. Yes, and I would absolutely agree, that is the way forward. Our problems in security are not unique cloud computing systems, by the way. So if you look at what we are putting in place in FedRAMP, we need, first of all, agreement on what the baseline controls actually are, and I think we have achieved that by working across a huge community in the Government to have that dialogue.

Second, we have to agree on what are the additional controls that are warranted in a cloud environment, much as you described, where there are extended vulnerabilities that are not necessarily applicable to traditional systems. So we have done that. We have tried to introduce new controls.

Third, we have to move to continuous monitoring. We have to make sure that agencies are applying managerial, technical, and operational controls to their systems for clouds, but we also have to report on a real-time basis the posture of the cloud security provider's environment, and that we have to see and we have to be able to take action, and we have to demand a solution be put in place. Then we can really bump up, I think, our security posture to more tolerable levels.

Mr. LUNGREN. Thank you very much.

Now, I either recognize the gentlelady or Mr. Thompson.

No, whoever you want to——

Mr. THOMPSON. Well, thank you very much.

Mr. LUNGREN. Because we have, I think, 5 minutes, probably, before we have to go vote. Votes have already been called. So——

Mr. THOMPSON. Right. Well, thank you, Mr. Chairman. I appreciate the Ranking Member's indulgence.

Clearly, the cloud is kind of cloudy right now to a lot of us, and we are trying to get better. But as we go forward, I am a little concerned about how our Government moves forward without the necessary safeguards in place.

Mr. Spires, let us talk about one of my concerns. I understand that DHS has contracted with a company called CGI Federal, Inc., to move its public website to the cloud. Now, I understand that this is not a U.S. company. Am I correct or incorrect?

Mr. SPIRES. Actually, sir, CGI Federal—well, you are correct, we are—we have contracted, through the GSA infrastructure as a service vehicle for CGI Federal to provide cloud services so we can move our public-facing websites to the cloud. That is correct.

CGI Federal is a U.S.-based company. The parent company is a Canadian-based company.

Mr. THOMPSON. So it is a U.S.-based company——

Mr. SPIRES. Yes, sir.

Mr. THOMPSON [continuing]. Owned by a Canadian company?

Mr. SPIRES. That is correct, sir.

Mr. THOMPSON. Okay. Does that cause you any concern?

Mr. SPIRES. In awarding the contract, sir, and going through the evaluation, we followed all the proper regulations from the FARR. I worked with our procurement organization, worked with GSA's procurement organizations.

I should also point out, sir, that we put a clause into that contract or that task order that States that everyone that works on

that particular contract needs to be a U.S. citizen unless we grant a waiver, and I don't expect we would be granting a waiver to that, and that all the data that is—that we would use in running those public websites needs to be resident within the United States.

Mr. THOMPSON. Can you provide the committee with a copy of that task order?

Mr. SPIRES. We certainly can, sir.

Mr. THOMPSON. So none of the work—none of the hosting or anything will be done out of the——

Mr. SPIRES. No. The hosting will be done in two geographic diverse data centers that are both located within the United States, sir.

Mr. THOMPSON. Thank you very much.

Dr. McClure, when you testified before the House Oversight and Government Reform Committee last year you called security one of the most significant obstacles to the adoption of cloud computing. Is that still your position or have you modified it?

Mr. MCCLURE. No, and I think it is a—the top challenge. There are others that we have alluded to.

Security, because of these issues we have been bringing up this morning—the lack of consistent standards, the lack of the quality of the work being done to assess cloud systems, the lack of real continuous monitoring, real-time capabilities—it presents real challenges, particularly in cloud environments. But we are addressing those; that is what we are trying to do.

The other two, though—and I think Greg may have mentioned this—are portability—I park my data onto a cloud provider's system; I, either by choice or because they are going out of business, I want to get that data off of their cloud system and into a new one. Can they aggregate and reconstitute that data and give it back to me? It is a huge question that Federal officials have to ask of their cloud service provider.

Mr. THOMPSON. So that is still a concern?

Mr. MCCLURE. Absolutely.

Mr. THOMPSON. Well, I understand that we have 12 companies that have been approved for some services under these contracts, while only four have been—of those 12—have been fully vetted. Is there some issues around security, or what?

Mr. MCCLURE. Absolutely. Once the 12 entities were found to be qualified and awarded business under that BPA, the second step is to go through a security authorization process, which is controls and testing to make sure they meet all Federal requirements. To date, four have, and they are subcontractors, and the remaining are going through the completion of that security authorization.

Mr. THOMPSON. So another Federal agency couldn't pick from the eight at this point?

Mr. MCCLURE. Correct.

Mr. THOMPSON. They can only take the four?

Mr. MCCLURE. They can take the four. They can actually, if they wanted to, enter into business with one of the other eight if they themselves performed the security assessments. We are doing it at GSA in order for all agencies to be leveraging off of that rather than repeating it.

Mr. THOMPSON. Well, and I guess for the GAO person in my last second, I am a little concerned that some of the vetting is not complete with some of the companies. Have you looked at that and whether or not you have some concerns around that, also?

Mr. WILSHUSEN. Well, we haven't specifically looked at GSA's authorization and assessment process yet, but certainly if we haven't—or the GSA or Federal agencies have not yet assessed the security controls over the cloud environment, they are doing—if they use that environment they are doing so at risk, and at an increased risk.

Mr. THOMPSON. Yes. Thank you.

Mr. LUNGREN. All right. We are expected at a series of five votes on the House floor that has already started. We have, I think, 5 minutes to get over there to vote.

The subcommittee will stand in recess until the conclusion of these votes, reconvene immediately following the last vote, which will probably be between 45 minutes to an hour.

[Recess.]

Mr. LUNGREN. With the acceptance of the Minority I am going to ask a few questions, and then, when Ms. Clarke gets here she will have the chance, or Mr. Keating returns from the floor, so we can allow the first panel to go as quickly as possible.

Let me ask you, Mr. Spires, how is the Department evaluating the different needs for different data sets? That is, if we have an agreement that there are different categories of clouds that are appropriate for different levels of security based on the nature of the data, what is the criteria you are using in evaluating those different needs?

Mr. SPIRES. My apologies. Yes, sir. We are using different evaluation—or, using evaluation criteria based on the sensitivity of the data itself. So in our case, we are starting off fairly simple right now.

All of what we would consider sensitive data, including data that would be for official use only and higher sensitivity data—law enforcement sensitive, for instance, in the unclassified realm—right now we are keeping that within what we call our private cloud, and that private cloud is hosted out of our two enterprise data centers. It runs within our own wide-area network, and hence, we are able to control that environment and really have the insights through continuous monitoring into the security stature of that environment.

We are aggressively looking at public cloud for what we would say is nonsensitive data. So the example I used in my testimony of us moving our public-facing websites, like dhs.gov, fema.gov, to public cloud, and we are trying to get experience using the public cloud.

As the FedRAMP process matures we would anticipate over time looking at how that evaluation criteria could change, because I am a real believer, having been in the private sector for a good part of my career, that we always want to foster competition; we always want to have choice. So as we have more and more comfort over time that public cloud services can provide the security levels, okay, and the continuous monitoring capabilities that we need we would look, then, over time to start to relax that criteria or shift

it so that more sensitive data would be able to be moved into the public cloud.

Mr. LUNGREN. Now, what is the interplay between Department of Homeland Security and GSA in terms of assurance of cybersecurity as we move to the cloud? DHS appears to be the point agency for—I don't want to say looking over the shoulder, but looking at other Government agencies and departments to assure that they are taking cybersecurity seriously. I know we have the office in the White House, which is an office that I would suggest is sort of a—my definition, sort of a focal point for policy, but DHS is the operational point.

How do you interface with GSA on something like this, with respect to their responsibilities in the areas that they have authority?

Mr. SPIRES. Let me provide an answer, and I am sure Dr. McClure will then want to weigh in.

First, I should state that I am the CIO for the Department of Homeland Security; there is another part of DHS within what we call our NPPD organization that really has this mission, if you will, to provide—really look at cybersecurity, of course, for the Nation, but in particular, for the civilian government agencies.

Mr. LUNGREN. Hopefully you folks talk to one another.

Mr. SPIRES. We talk to one another all the time. As I like to say, we are the biggest guinea pig for what they want to do next. I think we should be, right? So we work very, very closely with them.

So they have, for instance the US–CERT operation, which gathers——

Mr. LUNGREN. Right.

Mr. SPIRES [continuing]. Incident response information from throughout the Government to be able to share, analyze that information. That organization is working very closely with our organization and with GSA as we look at how we are going to roll out this FedRAMP initiative.

For instance, as FedRAMP rolls out and we look at continuous monitoring for public cloud service providers, those feeds would be provided to the Department of Homeland Security, to US–CERT, for continual analysis, as well as to the agency, so that we can continue to monitor, if you will, public cloud capabilities, if you will, real-time throughout the Government for the use of the public cloud.

Mr. LUNGREN. Dr. McClure.

Mr. MCCLURE. Yes, it is a—excuse me, Mr. Chairman—it is a very complementary relationship. FedRAMP has actually been devised with heavy DHS participation, both from Richard's office, representing the CIO angle, and from Greg Schaffer's office, the NPPD directorate that Richard referred to, which does the operational monitoring and runs a lot of the—a lot of the US–CERT capabilities.

So what we are doing in FedRAMP is designed to actually incorporate the role of DHS into that process. We are not replicating, we are not eliminating anything that is really clearly in DHS space.

In fact, if you look at the recent change made to FISMA that requires agencies to do monthly reporting of continuous monitoring,

FedRAMP is simply building on top of that. It is utilizing that process as we designed our process for FedRAMP.

Mr. LUNGREN. In either your opening statement or an answer to a question you indicated that continuous monitoring was one of the essentials as we move to cloud computing. Is the suggestion that this needs to be increased in intensity? Is it a relatively new concept? Is it one that has been implemented across the board in Government agencies and departments, or is it sporadic?

Given what you said about this being an essential, one would think it would be essential now, and one would also ask whether it is treated as something essential now.

Mr. MCCLURE. Absolutely. The issue with the continuous monitoring controls is the agreement upon the standard for the control and on the data elements that actually would be passed to show compliance.

What we want to do is to make sure that that has been agreed to with industry as well as inside of Government. So that is the process that is underway now, establishing those standards for the controls and the continuous monitoring are and coming up with agreement on the actual data elements that would be shared between entities to show compliance.

Once that is worked out, I think we can begin moving to a near real-time view of what is happening in the provider space, whether it is an internal or external provider that is doing——

Mr. LUNGREN. Mr. Wilshusen, do you have any comments, please?

Mr. WILSHUSEN. Yes, I do. Thank you very much.

As you know, we issued a report just this week on Federal information security. One of the issues we discuss had to do with continuous monitoring.

It is a relatively new phenomenon and requirement within the Federal Government. NIST recently issued some guidance that included it in its risk framework. I believe that came out back in February, perhaps, of 2011, or—I think it was February 2011, if I remember correct.

Right now the experience with Federal agencies in continuous monitoring is still immature, if you will. There is still a great deal that needs to be done. In some respects it is required that agencies have the capability to have automated tools in place in which they can gather this information and feed it on a regular near-real-time basis, and many of the agencies so far don't have those capabilities over all of their assets.

It is also important to know that with continuous monitoring there is that automated aspect of it, but there is still a need for testing and evaluation of the effectiveness of the controls to assure that the information that is being provided through these automated tools is accurate and reliable.

Mr. LUNGREN. One of the key risks the GAO report identifies relating to cloud computing is the dependency on vendor. There was mention by Mr.—by Dr. McClure when we were doing the first round of questions about the scenario in which you terminate a contract or a vendor ceases operations.

Any thoughts on how you protect against the vulnerability there? What do you have to build in to protect the Government's essential needs at that point?

Mr. WILSHUSEN. Well, that certainly is a key risk to Federal agencies. When we did our report last May all 24 of the 24 agencies cited loss of information as a key risk should their cloud service be terminated.

So in terms of being able to help mitigate those risks, it is imperative for agencies to establish comprehensive service-level agreements that specify clearly up front what the roles and responsibilities of the cloud service provider is as well as what the customer is with regard to providing information should they go out of business. It is also—or service is discontinued.

It is also imperative that interoperability and portability standards be developed and implemented so that agencies have the capability to take their information that is being processed by a cloud service provider and use it either internally or to another provider should the need arise.

Mr. LUNGREN. Mr. Spires, is there anything technologically unique about cloud computers that causes more difficulty with this particular concern—that is, termination of services?

Mr. SPIRES. Not on the technical side, sir, but I would echo what Greg said, that one of our big concerns about moving to the public cloud is exactly that, that we want to be able to assure continuity of service to our customers, right, in all events. So we have to work those scenarios as to what happens in the hopefully unlikely event that that cloud service provider can no longer offer that service—so data archiving capabilities, having the standards set—and I know this is something NIST is working on—for cloud interoperability so that we can quickly shift to another cloud service provider if necessary.

Mr. LUNGREN. So cloud interoperability would presume that you have equal security measures available.

Mr. SPIRES. Well, I think that comes back to the FedRAMP initiative and the idea of having these provisional authorizations in place for, hopefully over time, many cloud service providers so that that makes it much easier for us, as CIOs, to have choice and to be able to much more easily move our services. Goes back to my competition point earlier. It also gives us a more competitive playing field, which will drive down costs over time and, of course, provide better service.

Mr. LUNGREN. Before I yield to the gentlelady, the Ranking Member, the Ranking Member of the full committee brought up the question about the contract with the first that is a U.S.-based firm but a wholly-owned subsidiary of a Canadian firm. We are close to Canada, but it is another country, as I recall.

I think Congressman Thompson was bringing up the question of the—I don't know the visuals of that or how we tell the American people, "Yes, we are going to have—the Government is going to use vendors that have cloud computing with all of the assets but also the vulnerabilities we talked about, and it is going to be a company that answers to people who aren't in this country."

You answered it specifically. Do you understand the—at least the question some people might have there?

Mr. SPIRES. Sure. The more general point—certainly at the Department of Homeland Security within my office, we would be—want to always make sure, sir, that our data is protected, that for any sensitive data as we move forward that we would want U.S. citizens to only have access to that data, that it be housed—for sensitive information, that we would only have that data housed in data centers that were on American soil. That would go without—I mean, it is the given, okay?

All I can say, sir, is we followed the regulations. We did an open competition within the providers that were available to us through the GSA vehicle, and based on the evaluation criteria, this firm won that particular task order.

Mr. LUNGREN. Okay. Thank you very much.

The gentlelady, the Ranking Member of the subcommittee, is recognized for 5 minutes.

Ms. CLARKE. Thank you very much, Mr. Chairman.

Let me thank our panelists and thank you for your patience. We need clones around here, that is all I can say.

But let me say that in the brief moments I have had in the hearing I am not as concerned about our capability to secure the cloud, and I say that simply because we were innovative enough to invent it. I believe that our knowledge, our capability, our skills will enable us to protect. So I am going to be affirmative.

Then when I think about young people today and their level of curiosity, their innovativeness, I know that somewhere seated in some classroom today is the person that is going to come forth who will enable us to do what we need to do to move forward with the innovations that we have as a civil society. So I am coming at this not as a scary person but as someone who is ready for the adventure.

Having said that, I would like to ask this question of both Mr. Spires and Mr. Wilshusen: Did you look at the experiences of other Federal agencies in using public clouds before undertaking this effort? If so, what lessons did you learn and how did you apply them? What about State and private sector experiences? Were those also taken into account?

Mr. SPIRES. Ma'am, we certainly have, within our strategy, had numerous discussions, both with other Federal Government agencies—NASA, the Veterans Administration come to mind, both of which have been very aggressive at looking at cloud capabilities. We have also talked to a number of—I have personally talked to a number of CIOs within private sector firms as well as my staff, who have been very involved in reaching out, as well as to advisory services that work in the I.T. industry and serve that industry.

A few of the lessons learned—and I think we are still learning a lot of these lessons, right? I mean, one of our biggest issues, beyond security, because that is probably the biggest issue; we have been talking about that. But the next one is really, this is fundamentally a different business model, and it changes—I mean, we are buying a service-level agreement; we are not, you know, out there purchasing hardware and licensing software and integrating together.

Fundamentally, how we procure this is very, very different. So we have been working across the Federal Government—and as a

matter of fact, in a couple weeks the Federal CIO Council and the Federal Chief Acquisition Officer Council are going to be meeting together to talk about this very issue: How do we work out the procurement issues, the business model issues, so that we put ourselves in the best position to leverage this capability from a business perspective?

I would say that is where a lot of the lessons learned are. I think many of us are still feeling our way, to be honest, as to what is the right business model moving forward.

Mr. WILSHUSEN. Ms. Clarke, when we conducted our review last year over cloud computing security we went to a couple of different agencies and looked at some of the pilot cases that were underway. We went to DOD and looked at the DISA RACE, which is the Rapid Access Computing Environment, and also looked at NASA's Nebula cloud environment.

A couple of lessons learned that they experienced had to do with just the assuring that they are having to reengineer some of their business processes in order to accommodate the use of the cloud computing. They also found that one of the challenges that they had was also clearly specifying and delineating the responsibilities for security of the client personnel, you know, at NASA, as well as the cloud provider.

Now, in both cases each of their implementations were private cloud implementations. They decided in each case to take a kind of a slow, cautious approach before jumping in and maybe going to a public cloud. But in both cases they went to the private cloud implementation, which generally will have a lower threat exposure than public cloud.

Ms. CLARKE. Then I want to ask, are there any agency applications or services that should never move to the cloud, or is everything an agency does open to the move? In either case, why would it be the case?

Mr. WILSHUSEN. Well, I will take an initial stab at that. There is probably implementations and information that is so sensitive, perhaps, you know, classified information that needs to be particularly protected that it should not be placed out into a cloud environment, particularly a public cloud environment, given the current security capabilities present. So certainly classified information probably should not be placed in a public cloud environment.

Ms. CLARKE. So would you say never, or do you foresee in the future that that capability will exist? Because my question was never.

Mr. WILSHUSEN. Right. Well, I was taught from a very early age never to say never, and I think I will keep to that now.

Mr. SPIRES. I think I have essentially the same answer, Ms. Clarke. In the I.T. field I have learned to never say never because things change so much, since, certainly, in the years I have been in this field.

That being said, I would agree wholehearted with Greg. It is going to be quite a while before we would have any comfort in putting any classified information into a public cloud environment, and it may never happen. I think it will quite a few years before we would look to do that.

Mr. MCCLURE. Yes. The only thing I would add, Ms. Clarke, is that it goes back to what the agency sets as its requirements for what it is trying to do with its data and its service delivery. If the data demands protection levels that are beyond the capabilities of either in-house or out-house providers then you have got to address that.

So the term "public cloud" is used pretty loosely. Actually, there are instances, I think, where you will see Federal agencies claiming they do have things in public cloud but it is not the equivalent of what you might find a consumer such as ourselves doing from our own homes.

We have security requirements, records management requirements, 508 requirements. They have all these other requirements that still these providers have to show that they are able to provide that even though they may be called a public cloud solution.

Ms. CLARKE. Thank you very much, Mr. Chairman.

Mr. LUNGREN. Mr. Keating, you are recognized for 5 minutes.

Mr. KEATING. Thank you, Mr. Chairman.

With the new technologies I think there is a possibility of increased risk on infringement of copyright holders' rights because of the nature of this, that it is faster, cheaper, and it is easier to engage with unauthorized reproduction and distribution of public performances of types of copyrighted works. To what extent can the increased reliance on the data storage through cloud computing services contribute to this kind of copyright infringement? Do you see an issue there?

I will throw it open to the whole panel.

Mr. MCCLURE. Sure. I will take a stab at it first.

I think it goes back to in any environment, private or public cloud regardless, you have still basic security and privacy standards that have to be met. Access controls come to mind in this particular case. Who has access to information in these cloud environments is still a huge issue. If you don't define that and put the controls in place then you are subject to losing information no matter what kind of cloud environment you have it in.

Mr. KEATING. Yes.

Anyone else?

Mr. Spires.

Mr. SPIRES. I would just add, sir, that one of the things we are really working on within Homeland Security is strengthening our identity credential and access management capabilities, to pick up on what Dr. McClure said. We foresee in the future having a much stronger authentication model to protect against these very types of things, whether it be copyright infringement, or in our case we are very concerned about privacy and civil liberties, right, and access to the data that we store.

That really transcends whether you are in a cloud environment or whether this is just a more traditional kind of I.T. system and database. But these are the things that we are working on right now that strengthen the safeguarding side yet still enable the right kind of information-sharing to protect the homeland.

Mr. KEATING. Okay.

Mr. WILSHUSEN. I would just like to add that I agree that authorization and identification and verification is going to be key in

this respect. The one additional wrinkle—not to poke a hole or anything—is that the responsibility for sharing that the authorization is correct and the identity of the user is actually verified and claimed may no longer reside with the Federal Government or the Government agency with the cloud service provider. So the effectiveness of the cloud service provider's controls and access controls come into play as well.

Mr. KEATING. Okay. That is interesting.

Thank you very much. I had just one other—might be a bit tangential, but, you know, in terms of the Government security and securing Government data, there is the use of flash drive-type products as well. Is there any advantage or differentiation that is being made when you have that kind of, you know, product, in using a hard drive kind of system versus a software authentication?

Do you get anything more out of—from a secure basis—out of the hardware kind of authentication for that type of product than just the software itself? I mean, is it—where do you see it going? I mean, do you need both? Is it fine just with software, or do you think there is a need for that going forward for secure data?

Mr. WILSHUSEN. Well, I will take the initial stab. Yes, I think, you know, the hardware's authentication and security is something that can definitely help protect information, and particularly with flash drives and thumb drives. It, as you know, is a key risk because those devices can contain——

Mr. KEATING. Right.

Mr. WILSHUSEN [continuing]. Large volumes of information and they are extremely portable, as they are designed to do. Some agencies, like the Department of Defense, has banned their use on their systems because they also are carriers or can be used to carry malicious software and install that on devices on an agency's internal network.

Mr. KEATING. Okay.

I will yield back my time, Mr. Chairman. Thank you.

Mr. LUNGREN. Thank you very much.

I want to thank this first panel for not only testifying but understanding we have votes that interrupt, I understand that this takes a portion of your day, and we appreciate you being here. We thank you for your testimony.

The Members would request the Members of the committee may have some additional questions for you that we might submit in writing. We would ask that you would respond to those in writing.

With that, I am happy to thank you and dismiss you, and we will move on to the second panel.

I am going to ask unanimous consent that Mr. Duncan, who is a Member of the full committee but not a Member of the subcommittee, can sit for this second panel and have the privilege of introducing someone from his State when we get there.

So thank you, to the first panel.

If the second panel would come up, Mr. Sheaffer, Mr. Brown, Mr. Bottum, and Mr. Curran?

Today we have the opportunity to hear from a distinguished second panel on the question of "Cloud Computing: What Are the Security Implications?"

We have Mr. James Sheaffer, the president of Computer Science Corporation's North American Public Sector. Previously, Mr. Sheaffer served as vice president for CSC as well as a general manager of Prime Alliance—that is CSC's partnership with the IRS—to support the business systems modernization program. Prior to joining CSC Mr. Sheaffer spent 27 years in the American Management Systems, Inc. working on telecommunication in North America and Europe.

Mr. Timothy Brown is vice president and the chief architect for security management at CA, Inc. With more than 20 years of information security experience, Mr. Brown has been involved in many areas of security, including threat research, vulnerability management, consumer and enterprise identity, access management, network security in the encryption compliance and managed security services.

John Curran is the president and CEO of American Registry for Internet Numbers. He serves as the chief technology officer and chief operating officer for ServerVault as well as the chief technology officer at XO Communications and BBN/GTE Internetworking. Mr. Curran also has been an active participant in the Internet Engineering Task Force.

It is my privilege to allow Mr. Duncan to introduce the next gentleman, who, as I understand, had something to do with Purdue University. Since I went to Notre Dame I would like you to introduce him.

Mr. DUNCAN. Okay. Thank you.

[Laughter.]

Mr. DUNCAN. Thank you, Mr. Chairman. Thanks for giving me the opportunity, and thanks to the committee for allowing me to sit on the dais with you this morning.

It is my distinct pleasure to introduce one of my constituents, but he is also someone from my alma mater, Clemson University. Jim Bottum is a chief information officer and vice provost for computing and information technology for Clemson University.

Clemson, Mr. Bottum leads efforts focusing on high-performance computing and communication as well as collaborating with State and National government entities. Under his leadership, Clemson University's Palmetto Cluster has appeared at No. 60 in the world's top 500 computing sites alongside Clemson's Computational Center for Mobility Systems, ranked at No. 100.

Mr. Bottum currently serves on the NSF Advisory Committee for Cyber-Infrastructure, NSF Advisory Committee for CRPA Assessment, and the I–2 or Internet 2 Board of Trustees. Prior to coming to Clemson, Mr. Bottum was the first CIP and VP for computing at Purdue, where he was responsible for planning and coordinating all computing and information systems across the university.

He has also served on other NSF committees as well as National laboratory boards and provided consulting services for major universities across the United States. He has worked extensively on issues of cloud computing and should provide an excellent perspective of this issue from his academic research and experience.

I look forward to hearing his testimony and thank you for having him here today. I yield back.

Mr. LUNGREN. I thank the gentleman.

We thank you all for being here. We thank you for your indulgence, in that I know you had to wait as well, as we went over to vote.

We have the procedure here that your written remarks will be made a part of the record in their entirety, and we would ask you to limit your verbal remarks to 5 minutes apiece, and I would ask Mr. Sheaffer to go first.

STATEMENT OF JAMES W. SHEAFFER, PRESIDENT, NORTH AMERICAN PUBLIC SECTOR, COMPUTER SCIENCES CORPORATION

Mr. SHEAFFER. Thank you. Mr. Chairman, Ranking Member Clarke, Mr. Duncan, it is an honor for me to appear before you today.

My name is Jim Sheaffer. I am president of CSC's North American Public Sector, with 29,000 employees who proudly serve and support the missions of Federal agencies.

I also recently served as vice chair for the Public Sector for TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud. In July our commission issued a report called "Cloud First, Cloud Fast" that included 14 specific recommendations for the Federal Government to accelerate the adoption of the cloud, and I respectfully request that that document be entered into the record.*

Let me offer a brief word about CSC. Last year we had revenues of just over $16 billion. We are acknowledged as a leading global provider of I.T. services. We deliver large-scale projects for both public and private sector clients, and we provide cybersecurity to some of the world's largest companies and some of the most sensitive U.S. Government agencies.

By leveraging shared computing resources, higher utilization rates of hardware, and economies of scale, cloud computing is ushering in an I.T. revolution. Users pay only for what they consume. Cloud computing and the as-a-service delivery model enable organizations to cut costs of computing, build capacity for growing volumes of data, and burgeoning requirements for computation.

Cloud is a hot topic, but it is only the latest evolutionary step in the field. I began first with custom-build computers, moved to mainframes, on to personal computers, then to client-servers, and then to the internet.

What is different about the cloud is the rate of adoption. The economics are compelling and the take-up of this technology is much faster than some of the earlier technologies that were adopted. In fact, the global nature of the cloud makes this a different kind of phenomenon.

Today's austere Federal budget climate offers an added incentive for agencies to adopt the cloud, but it also raises questions of trust. Trust is more than just security. U.S. citizens and users must believe in the integrity and reliability of cloud computing in addition to security.

*The information has been retained in committee files.

We acknowledge the challenges. One, the speed of cloud advancement requires new security policies and even new security technologies and procedures.

The internet, which is the foundation for the cloud, was originally designed without a primary focus on security, and since then we have had to play catch-up to make it secure. In the future it will require the design of intrinsically secure architectures to ensure security.

A second risk is that all required security standards for cloud are not yet in place, as we heard from the prior—the previous panel. The National Institute of Standards and Technology and the Cloud Security Alliance, a nonprofit coalition, are developing, with industry support, those standards, and we believe that they need to be global standards, not just standards here in the United States.

Third, cyber threats are serious and dynamic, and becoming more pernicious. Threats are more severe than we experienced in the past, and the capabilities of bad actors are evolving swiftly.

The risks and challenges to cloud computing are substantial but not insurmountable and should not be used as an excuse to shrink from the adoption of the cloud. Fundamentally, cybersecurity must be integral to the architectures and not bolted on after the fact. We at CSC are confident that prudent cloud computing adoption can meet the stringent security requirements.

How should those risks and challenges be addressed? The key is to align the risk profiles of various types of data and their uses with the levels of protection required.

One-size-fits-all approaches provide neither effective security nor the lowest cost. Each application and data set must be evaluated to identify its specific security requirements, and then appropriate cloud solutions can be implemented, choosing from private, public, or hybrid clouds.

As an evolving technology, it is important to gain feedback and lessons learned from the implementation of cloud computing. Lessons will need to be shared across agencies, as one of your previous questions indicated.

The Department of Homeland Security is laudably reaching out to foster a more secure and resilient cyber environment. The Department is leaning forward to show leadership in cloud adoption.

In consolidating infrastructure from the 22 components of the primary data center at Stennis and its backup, DHS is increasing the productivity of its capital investment in computing and it has also implemented a private cloud behind its firewall and security systems. The Department is clearly an early and prudent adopter of cloud computing.

One example of the success of this approach is our systems. With our assistants at DHS we are designing and implementing a private cloud for DHS that will reduce the time to provision new software development and test environments from months to just a couple of days.

In conclusion, cloud computing offers enormous opportunity to improve performance and reduce costs. Security issues can be managed. The United States is a leader worldwide in cloud adoption, and we can and must maintain that position.

I welcome your questions. Thank you.

[The prepared statement of Mr. Sheaffer follows:]

PREPARED STATEMENT OF JAMES W. SHEAFFER

OCTOBER 6, 2011

Mr. Chairman, Ranking Member Clarke, and Members of the subcommittee, it is an honor to appear before you today to discuss security implications of cloud—or shared—computing. The subcommittee laid a good basis for today's discussion in its April 15 hearing on promoting Department of Homeland Security cybersecurity innovation and securing critical infrastructure, and its June 24 hearing on the homeland security impact of the administration's cybersecurity proposal.

I am Jim Sheaffer, President of CSC's North American Public Sector. Recently I served as Vice-Chair for the Public Sector of the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2). The mandate of the Commission was to provide recommendations on how the Federal Government could deploy and accelerate the adoption of cloud technologies, and to address public policies that would enable U.S. innovation in the cloud. In July, the Commission issued a report—*Cloud First, Cloud Fast*—that addresses some of the issues we are discussing today.

Let me begin by offering a brief word about CSC. Last year we had revenues of just over $16 billion. Three-fifths derived from IT services provided to the private sector, and two-fifths from a range of services for the public sector. Acknowledged as a leading global provider of IT services, CSC delivers large-scale IT projects for both public and private sector clients. We provide cybersecurity to some of the world's largest companies, including critical infrastructure providers, and some of the most sensitive U.S. Government agencies.

CLOUD COMPUTING

By leveraging shared computing resources, higher utilization rates of computing hardware, and economies of scale, cloud computing is ushering in an IT revolution which promises far lower costs while greatly improving capacity and performance. Cloud computing combines self-service provisioning of software applications and IT infrastructure with on-demand scaling of computing and storage in which users pay only for what they consume. Cloud computing and "as-a-service" delivery enable organizations to slash unit costs of computing, and build capacity for rapidly growing volumes of data and burgeoning requirements for computation.

Cloud computing is a hot topic. In essence, it is just the latest evolutionary step that has taken us from custom-built computers to mainframes to personal computers to client-servers, and then to the internet. What is different about cloud computing is the accelerating pace of change, rapid adoption rates, and global nature of its use.

Cloud innovation allows entrepreneurs and public sector innovators to create value at little to no capital expense in computing resources, unlike the previous waves. Cloud computing disrupts existing business models and enables wholly new ones. The explosion of mobile computing catalyzes even faster adoption of cloud computing.

Cloud computing hardware can reside on-premise at an organization's facility, or off-premise, such as at an IT provider's facility. The National Institute of Standards and Technology (NIST) defines four types of environments for cloud computing: (1) Private cloud that is operated by an organization and may exist on-premise or off-premise; (2) Community cloud that is shared by multiple organizations related to a specific community and may exist on-premise or off-premise; (3) Public cloud that is available to the general public, owned by a commercial vendor and located off-premise; and (4) Hybrid cloud that is a combination of two or more clouds (private, community, or public).

TRUST

Today's tight Federal budget climate offers an added incentive to agencies to adopt the cloud. But while cloud computing offers substantial benefits, such as cost savings, speed, and responsiveness to mission needs, it also raises questions of trust. Trust encompasses such concepts as security, availability, reliability, transparency to the user, and ability to extract data.

The pace and degree of adoption of cloud delivery services will depend on establishing a basis of trust. This begins with understanding the risks and challenges. Can important data be entrusted to the cloud? Are there new risks and challenges to trust, especially the security of data?

Let us look at the new risks and challenges to trust. One, the speed of cloud technology advancement requires new security policies, and even new technologies and procedures, to keep pace with cloud advancements. Most current knowledge about IT security is based on a world in which most computer resources are under the direct control of a person or organization and in which physical and technical means exist, including software firewalls, to control access. Moreover, the internet was originally designed without a primary focus on security; since then computer security specialists have played catch-up.

Many of those security concepts must be reconsidered for a world in which cloud computing enables a much broader spectrum of solutions and much greater cost savings derived from the sharing of computing, storage, and network resources, bringing new economies of scale. For example, firewall technologies designed for operating inside the virtual fabric of cloud architectures—the design of cloud computing systems—are just now becoming available, and they remain largely untested.

A second risk is that all of the required security standards for cloud computing are not yet in place. Clear, understandable, and verifiable standards are essential for building trust. The National Institute of Standards and Technology and the Cloud Security Alliance—a non-profit coalition of practitioners, companies, and associations—are conducting research and developing new cloud security standards.

Third, while not specific to cloud computing but relevant to it, cyber threats are serious and dynamic—and becoming more pernicious. Business and Government alike face threats much more severe than in the past, and more likely to change and do so swiftly.

Advanced Persistent Threats tend to be state-sponsored and target especially sensitive information, such as military and financial data and intellectual property. Such information lies at the heart of America's security and economic well-being.

The risks and challenges to cloud computing are substantial but not insurmountable. Of fundamental importance, cybersecurity must be integral to cloud computing architectures and not be "bolted-on" after the fact. CSC participates in various forums that develop standards. CSC's rigorous validation and testing programs promote innovation for security solutions.

On balance, we are confident that prudent cloud computing will satisfy stringent security requirements. USCYBERCOM Commander General Keith Alexander said it best to a House Armed Services Subcommittee last March:

"The idea is to reduce vulnerabilities inherent in the current architecture and to exploit the advantages of cloud computing and thin-client networks, moving the programs and the data that users need away from the thousands of desktops we now use—up to a centralized configuration that will give us wider availability of applications and data combined with tighter control over accesses and vulnerabilities and more timely mitigation of the latter."

WAYS TO ENHANCE SECURITY

How should security risks and challenges be addressed? The key is to align risk profiles of varying types of data and uses with levels of protection required.

Understanding the risk profiles of data being considered for the cloud is key to determining the required levels, and hence costs of security. One-size-fits-all approaches provide neither effective security nor the lowest-cost solution. Each software application and data set must be evaluated to identify its specific security requirements. For example, published scientific research may be suitable for less-stringent cloud computing environments than are needed for classified intelligence data on potential terrorists. CSC is assisting Federal agencies to develop roadmaps that outline risk profiles of data sets and identify appropriate cloud solutions.

It will be important to gain feedback and learn lessons from implementations of cloud computing. They can help identify best practices and improve security for future uses.

FEDERAL POLICY

Federal policy on cloud computing and its security has evolved rapidly. In 2002 the Federal Information Security Management Act, or FISMA, came into force. It establishes a "comprehensive framework designed to protect government information, operations and assets against natural and man-made threats," and requires program officials, chief information officers, and inspectors general to conduct annual reviews of information security.

The Federal Risk and Authorization Management Program, or FedRAMP, was initiated in 2010 to provide a standard approach across the Federal Government for

assessing and authorizing cloud computing services and products. A common security risk model enables the Federal Government to "approve once, and use often."

In the *25-Point Implementation Plan to Reform Federal Information Technology Management,* issued on December 9, 2010, the Office of Management and Budget called for reducing the number of Federal data centers by at least 800 by 2015 and creating a Federal-wide marketplace for data center availability. Curiously, not one of OMB's 25 points focused on cybersecurity.

On February 9, 2011, OMB issued a Federal Cloud Computing Strategy, which gives more attention to security. It cautions that cloud security is an exercise in risk management, "identifying and assessing risk, and taking the steps to reduce it to an acceptable level." Risk management based on intelligent risk assessment enhances the protection of the most valuable information and is more cost-effective than compliance-based approaches.

The Federal Strategy points to several potential security benefits of cloud computing. The first is the ability of the cloud provider to focus centralized resources on security services. Second, the greater uniformity and homogeneity of the cloud platform eases security management and improves response times. A third benefit is the improved resource availability of the cloud provider through scalability, redundancy, and disaster recovery capability. Fourth are the improved backup and recovery capabilities and procedures that a cloud provider can offer. A fifth potential benefit of cloud computing is the ability to leverage, as needed, services from other data centers.

At the same time, the Federal Strategy highlights potential vulnerabilities of cloud computing. One is the inherent system complexity of a cloud computing environment. A second vulnerability is dependency on the service provider to maintain secure logical separation in a shared computing resource, or what is called a multi-tenant environment. A third potential vulnerability is the cloud user's need to have sufficient knowledge of potential threats and vulnerabilities to know how to make decisions and set priorities on security and privacy.

Increasing experience in the implementation of cloud computing, with careful attention to security, will help validate and refine our collective understanding of its benefits and risks.

The Department of Homeland Security is laudably reaching out across the Federal Government and the private sector to foster a more secure and resilient cybersecurity environment. The DHS Chief information Officer is leaning forward to show leadership in cloud adoption.

In moving data from 22 separate components into the primary DHS Stennis data center and a secondary backup center, DHS has increased the productivity of its capital investment in computing. While migrating into the two consolidated data centers, DHS has also implemented a private cloud behind a DHS-controlled firewall and security systems. As new security standards are developed and effectively verified, more data will be ready to move to the cloud. In addition to private cloud implementation, DHS is moving certain public-facing websites, such as DHS.gov and FEMA.gov, into a public cloud in order to increase efficiency and productivity. DHS is an early and prudent adopter of cloud computing and its experience may be instructive for others.

CLOUD EXAMPLES

Let me outline three examples of how cloud computing can be implemented in a homeland security context.

First, CSC helps a global chemical company that is part of America's critical infrastructure. Its research unit must allow access to scientists and others from inside and outside the company to foster collaboration for new discoveries. Researchers require high-performance computing and surge IT capacity, and they store highly sensitive intellectual property. The research unit must accommodate projects that start and stop abruptly and then restart.

CSC has installed a private cloud that the chemical company manages to satisfy its own special security requirements. The company has deployed cloud access at each of its laboratories around the world, and CSC federates and orchestrates cloud services across the chemical company's global IT infrastructure.

In a second example, DHS wanted more responsive computing. It opted for cloud computing for the development and testing of new computer application systems. This eliminates costly and time-consuming tasks of procuring, installing, and testing new computer hardware and software every time a software development team starts a new project.

To support DHS, CSC designed and is implementing a private cloud that will reduce the time to provision new development and test environments from months to

just a couple of days. We are also assisting with a strategy and plan for helping DHS encourage management and cultural changes required to take best advantage of the cloud.

A third example is the potential for increased use of unmanned aerial vehicles to help DHS monitor U.S. borders. Evolving technology will allow aerial platforms to collect greatly increasing amounts of ground imagery. As this develops, cloud computing could assist DHS to expand data collection and processing while holding down computing costs.

RECOMMENDATIONS

I wish to call special attention to four important recommendations from the TechAmerica Commission Report, and offer a fifth recommendation.

First, the Federal Government and the private sector should support the creation of international standardized frameworks for securing, assessing, certifying, and accrediting cloud computing.

Second, the public sector and the Federal Government should accelerate the development of an identify management ecosystem to facilitate the adoption of strong authentication technologies, enabling more secure access to cloud services and websites.

Third, a law is needed to clarify responsibilities of companies to notify customers in the event of data breaches, and strengthened criminal laws are required against those who attack computer systems, including cloud services.

Fourth, the Federal Government and the private sector should develop and execute a more robust joint research agenda for cloud computing.

Fifth, verification and continuous monitoring of cloud security ought to be standardized. Independent, professional third-party audit of cloud providers should become standard practice, along with real-time transparency in the security posture of cloud-based systems.

CONCLUSION

In conclusion, as the use of cloud computing accelerates, better security must go hand-in-hand with saving money and improving performance. Cybersecurity must be integrated into cloud computing architectures at the outset, rather than be left to "catch up." This will enhance trust in the information revolution that underlies so much of America's prosperity and homeland security.

I welcome your questions and comments. Thank you.

Mr. LUNGREN. Thank you very much, Mr. Sheaffer.

Now, Mr. Brown.

STATEMENT OF TIMOTHY BROWN, SENIOR VICE PRESIDENT AND CHIEF ARCHITECT FOR SECURITY, CA TECHNOLOGIES

Mr. BROWN. Chairman Lungren and Members of the subcommittee, I want to thank you for the opportunity to talk to you today. CA Technologies is one of the world-leading I.T. management software companies that provides software and services to enterprise, governments, and cloud providers.

The hype and promise to the cloud continue to accelerate, but it is clear that significant confusion remains about exactly what cloud computing is and the risks and benefits associated with it. Security is the concern cited most.

When you consider the loss of direct control involved with the cloud these concerns are expected, but they must be addressed for the cloud to be successful. From a security perspective, any service that is accessed outside of an enterprise's direct control should be considered a cloud service.

Services like ADP, for check processing, and a 401(k) portal are good examples of—that have been around for a long time. Cloud is not new, but the current momentum and explosion of new cloud services gives us opportunity to enhance cybersecurity.

Mr. LUNGREN. I think we lost your mike there.

Mr. BROWN. Am I back?

Mr. LUNGREN. There you are.

Mr. BROWN. All right. We will move up. Here we go.

So CA Technologies believes the responsibility for cloud security lies with both the providers and the consumers. The cloud is neither inherently more secure nor less secure than other I.T. services.

Security fears and arguments that those fears are overblown have muddied the waters about this vital issue. To provide some clarity I will focus on four critical areas affecting cloud security.

First, it is important to note that cloud won't replace all other technologies and service delivery options. As organizations move to the cloud it will be one of many platforms that must be operated and managed together to minimize risk and security vulnerabilities. We should be wary when people say that cloud will replace all technologies.

Second, the responsibility for security rests with both the provider and the consumer of cloud technologies. Different cloud services have different risk profiles.

What is important is transparency. Customers and providers need to agree upon those security expectations and know that the service being deployed meets those requirements.

Customers must have trust in their cloud service providers but also must have the ability to verify their claims and performance. Cloud customers need to be vigilant in their investigation, auditing, and oversight of their providers. Cloud providers must approach securing their customers' data with the same degree of seriousness as the owner of the data.

Third is that a strong trusted identity system that enables the right people to have the right access to the right information at the right time is vital to securing the cloud. Many of the data breaches we read about today find their root cause in weak identity and access management controls.

To be certain the move to the cloud doesn't create new security risks cloud consumers should ask the following: Who has and needs access to what? What can they do with that access? What can they do with the information they obtain? Finally, what did they do with that information?

On-line banking and bill pay services provide an example of how transactions between different cloud services can be accomplished using strong identity management. As most of us know, different on-line banking transactions have different risks, and banks have implemented tiered security requirements based on that risk. Simply accessing your account balances requires one level of authentication, while transferring funds may require a higher degree of security.

If you want to authorize your bank to pay a bill, your bank may need to access a bill payment service in the cloud on your behalf. This type of transaction requires that the bank and the bill pay service have trusted and transparent security practices that are audited and enforced.

Finally, the adoption of standards is critical to the security and operability in the cloud. CA Technologies contributes actively to the

efforts of standards organizations, such as OASIS, and collaborates with NIST.

There are two efforts I would like to highlight. The first is FedRAMP.

FedRAMP offers the promise that solutions can be accredited once and used many times across Federal agencies. While we await the final draft of FedRAMP, several questions about its scope and its implementation remain. We recommend that Congress continue oversight to be sure these important questions are answered.

The second is the National Strategy for Trusted Identities in Cyberspace, or NSTIC. NSTIC is aimed at enhancing trust by strengthening industry-based identity management practices and minimizing the proliferation of username and password combinations we use on-line.

NSTIC has asked for its first budget in fiscal year 2012. We recommend that Congress fund this important effort.

Finally, I would like to offer several additional recommendations for your consideration. First, because we are in the nascent stage of cloud adoption, Congress should look at cloud policy issues through the lens of outcomes, not specific technologies. Static rules and mandated checklists are not adequately flexible and will rapidly become outdated as new technologies emerge.

Second, Congress should avoid adopting policies that create a country-specific—country-specific policy. For U.S. businesses in competing markets all over the world, global harmonization policy will enable industry to build solutions that can be delivered in multiple markets and will enhance our competitiveness.

Finally, the cloud is an opportunity for new business models, enhanced security, and for the United States to drive innovation and technical leadership. We recommend that Congress support the important policy recommendations from the TechAmerica Cloud^2 commission.

I appreciate your opportunity to be here for you today. I would be happy to answer any questions. Thank you.

[The statement of Mr. Brown follows:]

PREPARED STATEMENT OF TIMOTHY BROWN

OCTOBER 6, 2011

Good morning Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee. My name is Tim Brown and I'm honored to be here today to testify on cloud computing security risks and opportunities. I am the senior vice president and chief architect for security at CA Technologies. CA Technologies *(www.ca.com)* is one of the world's largest information technology management software providers. The company has expertise across IT environments—from the mainframe and distributed computing to virtual and cloud technologies. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. The majority of the global Fortune 500 and most major Federal and State government agencies rely extensively on CA Technologies software to manage their constantly evolving technology environments. Founded in 1976, CA Technologies is a global company with headquarters in New York, 150 offices in more than 47 countries, and thousands of developers and researchers worldwide.

CA Technologies was honored to serve on the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2), and was heavily involved in the development of the Commission's recommendations. Since another member of the Commission is participating in the hearing today, I will focus the bulk of my remarks on a number of specific cloud security issues CA Technologies believes are critical to ensure secure adoption of cloud computing.

However, CA Technologies supports the recommendations of the CLOUD² report and I address many of the issues covered in the Commission's report in my testimony today.

CA Technologies believes that cloud computing is neither inherently more nor less secure than other IT platforms, and that securing the cloud is a shared responsibility of both providers and consumers of cloud services. There are a number of policy issues that must be resolved to realize the cloud's potential and we will focus on those issues on our testimony today.

INTRODUCTION

While both the hype and promise surrounding cloud computing continue to accelerate at a feverish rate, it is clear that significant confusion remains in global markets about what exactly cloud computing is and what the risks and benefits are associated with transitioning to this latest technology. Corporate and governmental organizations across the globe are anxious to reap the cost, performance, and agility benefits that the cloud can offer, but at the same time are wary of a range of risks that accompany a different way of buying and consuming technology solutions.

Chief among concerns raised in survey after survey of both current and potential cloud customers is security. Security is often followed by related concerns about data privacy as well as interoperability, availability of cloud services, performance, and transparency of providers. When one considers the loss of direct control that accompanies cloud deployments, concerns about security risks associated with moving to the cloud are not only reasonable, but also expose critical operational risk management issues that must be discussed and addressed when determining if and when to move particular services to the cloud.

It is important to keep in mind that from a security professional's perspective, any service that runs outside of the operationally-controlled environment of an IT organization is considered a cloud service. This is true in the case of commonly-known cloud services like Salesforce.com, Google Docs, and cloud email, but also includes services like ADP, 401(k) programs, corporate travel sites, and health plans. No two applications or systems are alike, and pragmatic implementation of cloud technologies necessitates that risk-based processes be used to determine what services and applications may or may not be feasible to move to the cloud, their level of sensitivity, what platform is most suitable, whether a private or public cloud environment is appropriate, and the specific security and operational controls that are needed.

The use of cloud computing represents an exciting new opportunity for IT organizations and for CIO's in both business and Government to remake the way in which they work together with their customers and the user communities that rely on IT-based services. Because cloud computing enables IT organizations to focus on business services rather than infrastructure, technology organizations will have increased agility to build new solutions to support their customers with minimal investment.

In my testimony today, I would like to focus on the four key areas that CA Technologies feels must be considered in evaluating both the opportunities and risks associated with the transition to cloud:

- The reality of new complexities introduced with the adoption of cloud computing;
- Security considerations for the cloud;
- The critical role that identity management and authentication play in enabling cloud security; and
- The importance of standards development and adoption to ensure interoperability and common implementation of cloud solutions globally.

I will also make some recommendations on the role Congress can play in fostering the secure uptake and adoption of cloud computing solutions.

THE "NEW NORMAL" OF CLOUD COMPUTING

A theme that CA Technologies keeps hearing from our customers is that they want to use cloud computing as a real game-changer. The layers and layers of complexity in IT have made it increasingly more challenging to deliver new services to the business in a rapid manner. The global downturn in markets across the globe has resulted in flat and/or declining IT budgets in both the commercial and public sectors. But the demand for new technology-based services inside large organizations has not slowed, so IT organizations are constantly challenged to provide more business technologies faster with reduced resources.

These factors have all contributed to the perfect storm that has emerged for cloud uptake across the globe.

It is important to note that while many would have you believe that cloud technologies will replace all on-premise IT, in reality the transition to cloud technologies will be gradual and the need to develop and support on-premise solutions will remain for the foreseeable future. The introduction of cloud technologies will create greater complexities for IT organizations to manage and support. With cloud solutions, a single business service may include a combination of physical, virtual, and cloud components that all must work together to deliver the functionality that users expect.

Consumers of cloud technologies will find themselves in a hybrid technology environment for a long time. Existing solutions and technologies will still need to be maintained, and cloud technologies will most often serve as a natural extension of existing IT environments. As such, the cloud introduce a new heterogeneity to IT environments, one that will require coordinated and orchestrated management, transition plans, and risk-based security evaluations.

This can be a real boon to IT organizations that can harness the enthusiasm and momentum of the cloud to drive changes that have been needed in the management process for technology generally. One of the most promising aspects of cloud computing is its ability to fill the gap between technology supply and demand and help organizations focus less on commodity IT services and more on what is unique to their particular business or Government program. Off-loading standard services and functions to the cloud can save money and resources that can be better utilized to drive change and tackle problems that are more foundational and transformative to businesses and governments. At CA Technologies, we call this opportunity the innovation dividend.

To gain this dividend, however, IT organizations must take a very focused and methodical approach to evaluating what should or should not be moved to the cloud. The means that organizations need to evaluate people, processes, technology, and perhaps most importantly, risk involved with each potential opportunity move to the cloud. Organizations may determine that certain services, applications and data are too critical or sensitive to be moved to the cloud, which can be an appropriate risk management decision. The cloud is not a panacea, and may not be appropriate for all workloads. Organizations must take a measured approach that is driven by substantive analysis of the risks and opportunities associated with each opportunity to migrate services to the cloud.

Once decisions have been made to move a particular service or application to the cloud, organizations must evaluate what providers and what services will meet their needs. All of these analyses have impacts on and contribute to the security posture of the organization. Some of the considerations that CA Technologies advises our customers to use in evaluating providers include the following, which have been developed through the Cloud Service Measurement Initiative Consortium (CSMIC) that I provide additional details on later in my testimony:

- *Accountability*.—Can we count on the provider to deliver the promised service?
- *Agility*.—Can the service be changed, and how quickly?
- *Assurance*.—How likely is it that the service will work as expected?
- *Cost*.—How much is it, including both start-up and on-going costs?
- *Performance*.—Does the service do what we need?
- *Usability*.—Is it easy to learn and use?
- *Portability*.—Can I move my data and application from one provider to another?
- *Security and Privacy*.—Is the service safe and privacy-protected?

SECURITY ISSUES IN THE CLOUD

Just like when you buy a car, an appliance, or any other service, the reputation of cloud providers and their ability to deliver on the service promised is a key consideration when making a purchase of cloud solutions. The Cloud Service Provider ecosystem is just as diverse as any other industry. Responsible providers want to do all they can to demonstrate trust and accountability to their customers and that security services are built in and not bolted onto their solutions. These providers will be in the cloud marketplace for the long run and will continue to drive innovation and excellence in the industry. But it is important to keep in mind that new and innovative cloud service providers are emerging daily. We are in the midst of a significant expansion period in the cloud market, and the ever-expanding number of providers who want to move into the cloud market may not have long-term interest or commitment to the technology, which in turn may create risks for customers who want to embrace the cloud. Customers must have assurance their provider of choice will be there when they need service modifications or need to move their data and applications elsewhere, and that they take the responsibility of securing their data as seriously as they do as the owner of that data.

The Cloud Security Alliance (CSA), a major industry consortium focused on cloud security issues, has identified 14 critical focus areas for organizations deploying cloud computing resources.[1] CA Technologies/Ponemon Institute survey of the cloud service provider community made use of these 14 areas in a report released earlier this year. The survey data uncovered a wide range of viewpoints on the role that cloud service providers have in providing security for their solutions. With lower costs and faster deployment being the main drivers for moving to cloud services, some providers feel that security is more the responsibility of cloud customers than it is of providers.

In reality, not all cloud services require the same level of security. It will be appropriate for certain workloads to be deployed in the cloud with different security levels than others. But the goal of cost savings that is so often identified as the main driver for cloud adoption sometimes masks the importance of security risk management. Security must remain at the forefront of all cloud strategy discussions to ensure the right sets of security controls are applied to the right services. What is important is that security, performance, cost, and accountability decisions are clear and transparent to the users of cloud services.

CA Technologies believes that the responsibility for securing the cloud lies with both the providers and the consumers of cloud solutions. The cloud is neither inherently more nor less secure than other IT services and solutions. Generalized concerns over cloud security on the one hand, and arguments that the security risks in the cloud are overblown on the other hand, have muddied the waters to the point that policymakers and practitioners are experiencing security schizophrenia. Should I overlook legitimate security concerns and plunge head-first into the cloud, or should fear and uncertainty of these risks stop me from doing anything that even remotely resembles cloud computing? Like most responsible decisions, the answer lies somewhere in the middle of these two extremes.

Cyber criminals, state and non-state actors, and other cyber adversaries move rapidly and adeptly to exploit weaknesses and vulnerabilities in systems, networks, applications, and practices. They are successful at taking control of machines and stealing data. But done right, the movement to the cloud is an opportunity for organizations to enhance operational security.

As such, potential consumers of cloud solutions must be mindful of the wide range of providers and the security risk management controls they have implemented for the solutions they host or provide in the cloud. A key for cloud customers will be to evaluate both the sensitivities of the services and data they hope to deploy to the cloud, and a long-term viability, references, and the depth of their solutions.

Cloud customers must insist on built-in security and transparency from the providers they select. They need to create compliance plans and closely scrutinize their contracts, Service Level Agreements (SLAs), and the security and disaster recovery plans of their providers to ensure they are making sound choices on who to partner with in moving services to the cloud. A key consideration here is to trust, but verify. CA Technologies recommends that cloud customers meet their responsibility to audit and monitor their providers, including the use of inspection programs, testing and monitoring compliance with SLAs, and assessing the security of critical systems.

IDENTITY AND ACCESS MANAGEMENT AS A FOUNDATION OF CLOUD SECURITY

While there are certainly myriad operational issues to consider when architecting cloud solutions to deliver strong and robust security, CA Technologies believes that identity and access management (IAM) issues deserve particular attention. Our surveys of cloud providers and the views from leading industry analysts and organizations find that identity and access management is the most important issue that companies considering moving to the cloud face today. A strong trusted identity system that enables the right people to have the right access to the right information is critical to the protection and enablement of the cloud.

Cloud service providers and customers generally feel comfortable that they have highly qualified IT personnel and tools which can prevent or curtail viruses from infecting their services, and that they can effectively secure data flowing in and out of cloud services. They are less comfortable with the process of identifying and au-

[1] The 14 focus areas identified by the Cloud Security Alliance are the following: Governance and enterprise risk management; legal and contracting issues; procedures for electronic discovery; compliance and audit; information life-cycle management; portability and interoperability; business continuity and disaster recovery; data center operations; incident response, notification, and remediation; application security; encryption and key management; identity and access management; storage operations; and virtualization operations.

thenticating the users, systems, and devices that need access to their services and managing access to specific information or data when using cloud services.

One of the greatest challenges facing the IT sector today is fostering on-line trust, including the important trust components of security and privacy. The fact is that most on-line threats and successful data breaches of late have been based on and exploit access control and identity management failures in systems. The Government Accountability Office has written to Congress about unauthorized access issues as recently as Monday of this week (October 3, 2011). Identity management and access management controls are central to the secure adoption of cloud services.

Identity and access management practices within the cloud provide the foundation for effective security by ensuring that all users have only the appropriate level of access rights to protected resources, and that those rights are effectively enforced. IT organizations generally as well as cloud service providers, both public and private, struggle to keep up with the explosion in the number of users from multiple systems, applications, and user communities that are consuming their services and the complexity of managing access rights for these users.

With the transition to cloud solutions, employees and applications will continue to move outside the walls of the customer enterprise. This introduces new risks for unauthorized access and the loss of information. Cloud applications are new services that users must have access to, and managing that access without creating new vulnerabilities or new silos of identity are incredibly daunting challenges. Managing the on-boarding and off-boarding of users to cloud services and integrating those access rights with the overall IAM strategy for on-premise solutions requires that cloud providers and customers answer the following questions:

- Who has and needs access to what?
- What can they do with that access?
- What can they do with the information they obtain?
- What did they do with that information?

These questions reinforce that managing access and authorization is but one part of the challenge. To be successful, identity security strategies must also focus on the specific data being accessed and what individual users can do with it. CA Technologies refers to this process and approach as content-aware identity and access management.

Cloud computing creates opportunities for Government agencies and commercial organizations alike to make certain that new silos of identity don't emerge that increase vulnerabilities and complexities for users. For Government programs and systems, we recommend that Federal agencies enhance their IAM capabilities to provide for risk-based authentication, the use of multi-factor authentication solutions, and leverage the investments they have already made in Personal Identity Verification (PIV) cards.

An example of how many of these integrated identity controls are used today can be found in the financial services sector. CA Technologies counts the majority of the world's major financial services organizations as customers, and we have worked closely with these organizations to implement strong and flexible IAM solutions that provide their customers with ease of use in the most secure fashion possible. Financial services firms have taken a security-first approach because of the economic risks of the transactions they conduct. Enhancing the security of those transactions helps meet regulatory requirements, but first and foremost focuses on providing Defense in Depth in ways that enhance security and provide ease of use for consumers that include IAM solutions as a core component. Financial institutions are doing a great job of analyzing not only the risk of individuals and their access rights, but also the unique risks of individual transactions. This is a trend that we believe the overall cloud security market must and will embrace.

Most of us are already comfortable with the concept of signing onto the website of our bank to access our account information. This usually requires that users provide an account number, username, and password. If you want to move money around from one bank account to another at the same financial institution, the bank may require you to provide a secondary identifier, like a PIN, because that transaction involves more risk. If you want to use your bank's bill pay service and authorize the movement of money from your bank to your credit card company or your local utility, the transaction becomes more complicated and introduces additional risk to both parties involved.

In many cases, when you initiate a transaction like this from your bank, the experience to the user will be seamless. But behind the scenes a complex transaction whereby the user is redirected to a bill pay website and has their identity credentials passed to the bill pay provider without needing to sign on or provide their credentials again has taken place securely and transparently. The identity authentication taking place in this scenario is being accomplished via a cloud service. This

type of transaction is an illustration of how user experience and sound security can be implemented across the very diverse technology environments present today. We believe that this represents the direction future secure transactions across public, private, and hybrid cloud environments will progress.

THE ROLE AND NEED FOR STANDARDS IN FOSTERING CLOUD SECURITY

I believe this example also highlights the importance of standards development and the valuable contributions of industry-led, recognized standards development organizations (SDOs) and consortia. The adoption of standards and their integration into the innovative security solutions offered by the vendor community make possible predictable, interoperable, secure implementations in enterprise and cloud-based services. Such standards are vital to the management of cloud security risks. As I noted earlier, existing security technologies implemented in the enterprise are the building blocks of cloud security. And to a huge extent those technologies, and the practices and controls which they support, are standards-based.

Such building block standards are now foundational for cloud computing environments, and where gaps exist, new standards are under development. CA Technologies and other major IT companies contribute actively to these efforts. For example, the Organization for the Advancement of Structured Information Standards (OASIS) has developed important security standards such as Extensible Access Control Markup Language (XACML), Security Assertion Markup Language (SAML), and web services security standards such as WS–Trust. OASIS also has technical committees in place addressing new security challenges applicable to the cloud, such as cloud identity, identity trust elevation, privacy management, and reputation management. Its committees are also working to create profiles which are used to apply existing standards suchas XACML directly in support of cloud computing requirements.

Other standards bodies, including the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), de jure bodies such as the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1), key industry consortia such as the Open Identity Exchange and the Kantara Initiative and other standards organizations are all key contributors to enabling trust in the cloud. In combination with best practices organizations such as the Cloud Security Alliance, the resources contributed by industry, academia, governments, and independent technical experts together represents a huge and on-going investment to support security risk management in the cloud environment. I would like to note the important role that the National Institute for Standards and Technology (NIST) plays by its active participation in industry standards development and as a convener of industry efforts and focus. NIST recently issued a Special Publication 500–291, the Cloud Computing Standards Roadmap, which examines the applicability of standards for the cloud and areas where gaps need to be filled.

The NIST publication looks well beyond security alone, and SDOs and consortia have certainly recognized the importance of standards-based cloud interoperability at the data level, and through the development of relevant application, operational management, license management, audit, virtualization, and other standards that are needed to enable interoperability of applications and services across clouds. CA Technologies is a major participant and leader at many levels of the cloud standardization process. And we believe that all of these categories of standardization, and more, are relevant to the development of interoperable clouds and cloud computing trust.

There are several specific efforts I want to highlight as examples of emerging standards in the cloud security arena. The first and perhaps most important in the Federal space is the Federal Risk and Authorization Management Program (FedRAMP). While still in its draft form, FedRAMP will provide Federal agencies with a baseline, common approach for assessing and authorizing cloud services for use in Federal agencies. This will provide Federal agencies with a common set of controls against which to evaluate cloud services, and will give cloud providers certainty of Federal specifications that must be built into their products. FedRAMP is built on the premise that solutions should be certified once and used many times across Federal agencies. Federal agencies, however, have shown a tendency historically to ignore previous certifications and re-certify technologies for use in their own departments based on special requirements. Reciprocity of authorizations will be a critical gauge of the success of FedRAMP.

FedRAMP will also require the transmittal of more frequent operational security information by providers to the Government, a process that is most-often termed "continuous monitoring." Continuous monitoring offers the potential to dramatically

improve the situational security posture of Federal information systems that rely on the cloud if implemented correctly.

While we await the final draft of the FedRAMP specifications, several questions about its scope and implementation remain, however. Will agencies be required to honor authorizations made by other agencies and avoid re-evaluating solutions that are implemented similarly at another agency? How often and how will the security data envisioned under continuous monitoring be transmitted? How will the Government evaluate this data once received? The answers to these and other questions will be critical to ensuring FedRAMP is both implemented correctly and receives the buy-in needed from Government and the private sector to ensure its success.

A second area I feel is important is the need to develop common service measurement frameworks to help enable data-driven decisions on the relative effectiveness of cloud solutions based on variables like cost, availability, security, and scalability. Right now, there is no standard mechanism to evaluate common services from different providers against one other. The Cloud Service Measurement Initiative Consortium (CSMIC), under the direction of Carnegie Mellon University and with participation from government agencies like the State of Colorado Office of the CIO, and corporations like CA Technologies and Accenture, has begun developing a service measurement index (SMI), which can be used to measure and compare a business service using a common language and evaluation process. A high-level representation of the characteristics and questions the CSMIC seeks to address is included as an attachment to my testimony today. In conjunction with standard recognition of cloud services authorized under the FedRAMP program, the use of a framework like SMI in Government procurements will enhance the analysis of competing cloud services and lead to greater standardization of solutions. As such, CA Technologies encourages the U.S. Government to investigate using the SMI to encourage data-driven decision-making on cloud acquisitions.

Third, in the area of identity and access management, the National Strategy for Trusted Identities in Cyberspace (NSTIC) is a critical initiative that will make it easier for citizens and consumers to securely and confidently navigate cyberspace and will enhance trust among different consumers of identity through the sharing and reciprocation of identity credentials. NSTIC is aimed at enhancing on-line trust by strengthening industry-based identity management practices and minimizing the constant proliferation of username and password combinations that individuals must remember to conduct business on-line. The standards and governance rules that will be developed under NSTIC are a critical component of implementing robust IAM solutions that can enhance trust of and the use of cloud computing services. As the NSTIC program gets up and running at the Department of Commerce, CA Technologies recommends that Congress fully fund this important effort and that Federal agencies become active participants in both the development of the NSTIC standards, and ultimately, accept private sector-issued credentials as a means of authentication for citizens who wish to interact with Government agencies securely.

Standards development, then, is an on-going and vital area of industry and Governmental focus. It is international in scope, and the standards are integral to key Government initiatives such as FedRAMP and NSTIC. It is important that the subcommittee recognize that it is only through support for industry-led, internationally supported standards will we have measurable, interoperable security risk management technologies, innovative technical solutions and practices that can ensure trust in cloud-based services, not only in the United States, but globally.

RECOMMENDATIONS FOR CONGRESS

I was asked to address some of the security risks and opportunities associated with the transition to cloud computing. I hope that my testimony has highlighted that while there certainly are risks, the opportunities are extremely positive if a number of actions are carried out to ensure that the adoption of cloud technologies does not create new silos in IT security and new, unintended risks. We are in the nascent stage of cloud adoption. To ensure the promises of cloud computing can be delivered in concert with effective security risk management, we recommend that Congress:

- Adopt policies that can accommodate future development and flexibility in the cloud market, specifically, and in IT more generally. Too often, Federal policy has imposed static frameworks that must constantly be updated based on new technology developments. We recommend that Congress focus on outcomes and not on specific technologies;
- Avoid policies that create a fragmented, country-specific market for cloud services in the United States. As the cloud market continues to evolve, we see great

risk for market segmentation based on unique policies designed solely to address U.S. or other countries' market demands. For U.S.-based businesses seeking to compete in markets all over the world, globally harmonized policies will enable industry to build solutions that can be delivered in multiple markets, enhances our competitiveness, and makes it easier to deliver innovative solutions around the world. Policies that acknowledge the global nature of cloud markets will enable the United States to maintain its leadership position in cloud computing and encourage innovation to support jobs and exports of U.S.-developed technologies;

- Support standards developed by recognized standards development organizations in the areas of cloud security, interoperability, and transparency. These standards are vital to the management of cloud security risks and should be embraced by Congressional and Executive Branch policy makers;
- Fund and support the continued development and rollout of FedRAMP and the NSTIC. To enhance operational cybersecurity at the Federal level, we recommend that Congress ensure that critical funding to develop and implement these programs be preserved, even in difficult Federal budget environments. We further recommend that Congress keep a watchful eye on FedRAMP implementation to ensure that the efficiencies hoped for are achieved;
- Continue support for NIST and its unique role as both an internationally-respected body of security experts developing standards and practices for the Federal Government as well as for its important function as a contributor to industry-led standards development and as a convener for addressing emerging security issues; and
- Encourage the Federal Government to leverage emerging efforts to develop service measurement indexes in Government cloud procurements. The CSMIC effort I described in my testimony can provide Federal agencies facing budget, performance, and transparency demands with tools that take data-driven approaches to evaluating competing offers of cloud technologies. I believe that frameworks like these can facilitate more robust decision-making about which specific cloud services and providers are right for Federal agencies.

Mr. Chairman, Ranking Member Clarke, and Members of the subcommittee, this concludes my written statement. I appreciate the opportunity to appear before you to share some of our thoughts on cloud security. CA Technologies shares the subcommittee's goal of increasing awareness of the cloud and the particular goal of enhancing cybersecurity, and we would be happy to work with you towards this goal however we can.

I would be happy to answer any questions you may have for me.

Thank you.

Mr. LUNGREN. Thank you very much.

Now, Mr. Bottum, you are recognized for 5 minutes.

STATEMENT OF JAMES R. BOTTUM, VICE PROVOST FOR COMPUTING AND INFORMATION TECHNOLOGY AND CHIEF INFORMATION OFFICER, CLEMSON UNIVERSITY

Mr. BOTTUM. Mr. Chairman, I would like to thank you and the Members of the subcommittee for the opportunity to present this testimony. Located in Clemson, South Carolina, Clemson University is a Nationally-ranked public land grant research university with an enrollment of 19,500 students.

Mr. Chairman, many definitions explain what the cloud represents. A good working definition should reflect the distinctive characteristic of cloud computing, namely on-demand delivery of shared services over the internet.

By allowing users to share resources, cloud computing enables infrastructure to be right-sized, balancing user requirements with the information technology services actually rendered. Cloud computing is both efficient and economical. However, we must ensure that our security tools, practices, and policies grow in proportion to our use of this evolving technology.

Clemson has, in some sense, been in the cloud business for over 30 years, provisioning Medicaid applications and services to the State and citizens of South Carolina. Three years ago, as the recession intensified, we created a South Carolina Cloud experiment to see if several institutions could do things we could not do by ourselves, and/or do them in a more economical fashion.

Today our cloud is operational and involves a collaboration of educational institutions and commercial organizations. Partner institutions include both public and private universities, technical colleges, and historically black colleges and universities. Many of these would not ordinarily have access to the resources as a standalone institution.

Our team is working with a Fortune 500 company to build out a secure and comprehensive cloud computing environment. Considering our diverse set of users and the numerous organizations that connect into the environment, it is important to properly ensure identity and access management and address concerns over data theft or manipulation and vulnerabilities.

Our goal is to apply policies, procedures, and controls that are seamless, transparent, and non-impeding to the end-user. It is my view that the benefits of cloud computing far outweigh the risks.

A thoughtful strategy for prudently broadening adoption of cloud services can facilitate a smooth transition to this dynamic platform. The transition should be complemented with a thoughtful and comprehensive information security initiative to ensure the protection of our data and resources as our environments have evolved.

To increase security within the cloud, R&D is needed in a number of areas. Six important areas are highlighted here.

The first area involves the use of virtual machines. Cloud computing is enabled by virtualization. Further research is needed to better understand virtual machine operation and establish safeguards to effectively protect this evolving environment.

Second is authentication, authorization, and accounting. Current security approaches leverage current best practices. Research is needed to counter the many threats, including eavesdropping and tampering, distributed denial of services, network infrastructure vulnerabilities, and insider threats.

Third, R&D on security applications and tools should focus on the creation of applications that leverage the distributed nature of the cloud to provide a new level of security. This research would result in a more secure environment that is resistant to both infections of individual hosts and the current generation of network-based attacks.

Another area is encryption for programs and data processing. Recent work has produced an encryption system allowing computers to execute encrypted programs.

Research on distributed denial of service detection and control is also needed. A DDOS attack is an attempt to make a computer resource unavailable to its intended users. Currently there is not a good mechanism for DDOS detection and control.

Finally, research on network technologies is also important. Current protocols and tools in place today make it difficult to make networks available dynamically to match the elasticity in clouds.

Adaptive and intelligent networking research is an important area of study.

It is also critical that we have a security-conscious workforce. There is a gap that exists between what universities teach and what industry needs. Universities teach theory and fundamentals, whereas industries desire practical experience.

In addition, Mr. Chairman, I believe attention should be given to legal issues surrounding cloud computing—contractual and service-level agreement issues regarding physical data protection, incident response, confidentiality, privacy and security controls, and other matters, which are important aspects in developing a relationship with a provider.

Mr. Chairman, on behalf of Clemson University, I would again like to thank you for your time.

[The statement of Mr. Bottum follows:]

PREPARED STATEMENT OF JAMES R. BOTTUM

OCTOBER 6, 2011

Mr. Chairman, I would like to thank you and the Members of the subcommittee for this opportunity to present testimony before this committee. I would like to begin by taking a moment to briefly acquaint you with Clemson University.

Located in Clemson, South Carolina, Clemson University [1] is a Nationally-ranked, science and technology-oriented land grant public research university founded in 1889, known for its emphasis on collaboration, focus, and a culture that encourages faculty and students to embrace bold ideas. Clemson's teaching, research, and outreach are driving economic development and improving quality of life in South Carolina and beyond. With an enrollment of 19,500, Clemson is a high-energy, student-centered community dedicated to intellectual leadership, innovation, service, and a determination to excel.

Regarding my own background, I have been the vice provost and chief information officer at Clemson University since July 2006. During my tenure, Clemson has transformed its network, storage, and computational infrastructure, including the data center, into a state-of-the-art set of services benefitting research, education, and public service. We have been recognized for transformative work in publications such as *Network World, Computer World,* and *Storage Magazine.* Before coming to Clemson, I was the first chief information officer at Purdue University beginning in 2001 where I forged a new model for partnering with research (recognized in a publication by the EDUCAUSE Center for Applied Research, July 2005). Prior to that, I was the executive director at the National Science Foundation's National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. I currently or previously have served on a number of National committees including the National Science Foundation's Advisory Committee on Cyberinfrastructure and the Internet2 Board of Trustees.

CLOUD DEFINITION

Mr. Chairman, many definitions exist to explain what "the cloud" actually represents. For purposes of my comments today, a good working definition should reflect what I believe to be the distinctive characteristic that defines cloud computing, namely the elastic, on-demand virtual delivery over the internet of shared services, including infrastructure and software. By allowing users to share access to software applications, computational power, networks, and data storage, cloud computing enables computing infrastructure to be right-sized while balancing user requirements with the information technology services actually rendered. Recognizing this shared component is fundamental to understanding the dynamic effects that are derived from the cloud.

Also inherent in the cloud model is its flexibility. Multiple implementation regimes—private, community, public, and hybrid—permit organizations to select deployment schemes that best meet their needs and missions. Clouds are not one-size-fits-all. As defined in the draft National Institute of Standards and Technology Defi-

[1] Clemson University. <www.clemson.edu>

nition of Cloud Computing.[2] Private clouds are environments where "the cloud infrastructure is operated solely for an organization." Private clouds host and on-demand deliver resources, under the control of the organization, generally within a firewall. Community clouds are where "the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security, requirements, policy, and compliance considerations)." This shared infrastructure enables the community to share in the cost, yet also offers a common set of security and privacy policies and procedures. In Public clouds "the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services." Public clouds may be free or pay-per-use and provide resources that are dynamically provisioned on a self-service basis. Hybrid clouds are environments where "The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability."

CLOUD EVOLUTION

Cloud computing may be characterized as evolutionary over time. Cloud computing should not be viewed as revolutionary, since some of the earliest concepts regarding computer time-sharing and utility computing came out as early as the 1960s, but did not take hold in our society until decades later. Past models of computing focused on utilizing supercomputers, mainframes, and storage devices primarily owned and operated by a single organization. As the internet and broadband capabilities expanded, opportunities arose to connect, share, and leverage these resources by multiple organizations with a common purpose. Referred to as grids, or grid computing, this model provided multiple users and various sites access to a shared heterogeneous computational infrastructure utilized to solve computational problems. During the 2000s, the cloud concept further evolved as major companies such as IBM, Google, and Amazon as well as numerous universities and research organizations began to develop and grow environments.

SOUTH CAROLINA CLOUD EXAMPLE

At Clemson University, our own cloud initiative has coalesced around what we refer to as the South Carolina Cloud[3] or "SC Cloud." SC Cloud represents a collaboration of educational institutions, IT professionals, commercial entities, and others who drive cutting-edge research in the areas of computing and communication infrastructure, data storage and visualization, virtual collaboration, and education workforce training. In pursuing their research, participants access a cluster of ~61,700 PCs as well as other High Performance Computing resources and networks to virtually explore new concepts in a host of critical computing research fields, including: Data modeling, the hyper-growth in connected devices, surge in real-time data streams, on-line and mobile commerce, business use of service-oriented architecture, virtualization, and Web 2.0 applications.

The SC Cloud initially began as a consolidation effort of Clemson's on-campus distributed computing resources to improve computing efficiencies and advance capabilities in research and education. One of the unanticipated results of this effort was the partnerships that developed with other South Carolina universities. SC Cloud partners share a common set of computing and IT services, including networking, high performance computing, server administration, data storage, instructional and classroom technology support, monitoring, and security and privacy. Likewise, higher education also share a common set of issues and challenges related to these services, including the economics of supporting and maintaining a growing set of services during economically challenging times, ensuring an adequate workforce, and continually modifying the service offerings to meet ever-changing demands and expectations. Across South Carolina the value of working together in a shared resource environment was quickly recognized as an evolving "work-in-progress" model that enables institutions to more efficiently and effectively address computing and information technology collectively.

---

[2] Mell, Peter and Timothy Grance. National Institute of Standards and Technology. "The NIST Definition of Cloud Computing (Draft)." National Institute of Standards and Technology Special Publication 800–145. January 2011. <http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf>

[3] South Carolina Cloud. <http://www.clemson.edu/ccit/rsch_computing/CUCI/sc_cloud.html>

CLOUD BENEFITS

Our SC Cloud experience resonates and echoes many of the benefits found in cloud computing across the Nation, regardless of the cloud deployment model. Costs are reduced by sharing the overhead capacity required for peak loads. Large numbers of standardized hardware enables next-day parts replacement contacts in lieu of expensive rapid response time, on-site maintenance contracts. Advantageous hardware and software pricing is negotiated. Economies of scale allow investment in redundant cooling, backup power, and other facility infrastructure. Virtualization and infrastructure management solutions make it possible to rapidly deploy or remove resources incrementally based on demand. Researchers focus on research instead of administering systems. Reliability is improved by locating away from high-risk areas. Energy use is reduced by eliminating the need for powering and cooling unused capacity, and energy costs are reduced by locating where power is cheaper.

There are numerous examples of both public and private entities that have realized sizable benefits from the adoption of cloud computing initiatives. GlaxoSmithKline, a leading pharmaceuticals company, recently deployed a Microsoft cloud solution through a Deskless Worker Suite to 15,000 of its employees, reducing IT operational costs by 30 percent while enhancing productivity and expanding external collaboration.[4] The U.S. Air Force saved an estimated $4 million annually on its Personnel Services Delivery Transformation (PSDT) system by implementing a cloud solution from RightNow and customers can now find answers from over 15,000 documents within 2 minutes, a drastic improvement from previous wait times of 20 minutes.[5] The Department of Energy estimates it will save $1.5 million over the next 5 years in hardware, software, and other labor costs from implementing a cloud solution at the Lawrence Berkeley National Lab for its e-mail accounts and from utilizing Google Sites and Google Docs for its scientific research teams.*

Another benefit of cloud computing adoption is a company's ability to better manage its power resources for its IT infrastructure. By deploying an IBM cloud-based endpoint management solution, Fiberlink—an innovator in voice, data, and IP networking solutions—achieved a 25% annual growth rate over the last 5 years and has saved an estimated $500,000 a year from improved power management alone.[6] A study concluded this year by Verdantix and sponsored by AT&T estimates that cloud computing could enable companies to save $12.3 billion off their energy bills and results in a carbon emissions savings of 85.7 million metric tons by 2020.[7] Another study from Microsoft and Accenture revealed that moving business applications to the cloud could cut per-user carbon footprints by 30 percent for large, already efficient companies and as much as 90 percent for the smaller and less efficient businesses.[8] Cloud computing is not only beneficial to the companies themselves that use the technology, but its benefits can extend to the environment at large because of its decreased dependency on independent hardware sites distributed across a company.

Our experience with SC Cloud has been that it is a collaborative mechanism for research, as well as the high-quality, innovative R&D it is delivering to advance our understanding about virtual environments in ways that are beneficial to both the public and private sectors. It is this type of environment that is instructive for framing some of the key considerations in cloud migration. I would like to share some of that experience with the committee today, particularly in the areas of security, scalability, and identity management.

SECURITY—CLEMSON UNIVERSITY EXAMPLE

Concerns over data theft or manipulation and vulnerabilities to critical applications are real when contemplating the network security architecture of the cloud

---

[4] Microsoft Corporation—Case Studies. 2009. <http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000005460>

[5] Kundra, Vivek, Federal Chief Information Officer. State of Public Sector Cloud Computing. 2009. <http://www.info.apps.gov/sites/default/files/StateOfCloudComputingReport-FINALv3_508.pdf>

* [sic]

[6] IBM Corporation—Success Stories. 2011. <http://www-01.ibm.com/software/success/cssdb.nsf/CS/LWIS-8KZPUW?OpenDocument&Site=corp&cty=en_us>

[7] Verdantix Research. "Verdantix Cloud Computing Report For Carbon Disclosure Project Forecasts $12.3 Billion Financial Savings For US Firms." 2011. <http://www.verdantix.com/index.cfm/papers/Press.Details/press_id/58/verdantix-cloudcomputing-report-for-carbon-disclosure-project-forecasts-12-3-billion-financial-savings-for-usfirms/->

[8] Accenture Corporation. "Microsoft, Accenture and WSP Environment & Energy Study Shows Significant Energy and Carbon Emissions Reduction Potential from Cloud Computing." 2010 <http://newsroom.accenture.com/article_display.cfm?article_id=5089>.

platform. Clemson's Information Security and Privacy organization mission is to protect the confidentiality, integrity, and availability of information and informational resources. The goal is to apply policies, procedures, and controls that are seamless, transparent, and non-impeding to the organization. Controls match the risks that exist and ensure the protection of data, provide redundancy, and include the ability to monitor Clemson's environment. Security and privacy at Clemson are a shared responsibility, meaning efforts have been made to educate and raise awareness among faculty, staff, students, alumni, etc. so that security and privacy become a natural part of the culture.

The security challenges that Clemson faces are typical of other higher education institutions and similar to those mentioned in Cloud Security Alliance's Top Threats to Cloud Computing".[9] CSA is a "member-driven organization chartered with promoting the use of best practices for providing security assurance within cloud computing." CSA's research shows that the top security threats include such areas as insecure interfaces, malicious insiders, shared technology issues, account or service hijacking, and unknown risk profiles. We have implemented a series of policies, best practices, and controls that provide for increased protection, but know that nothing is 100% "bullet-proof." Staying ahead of the curve of threats and vulnerabilities is a continual challenge, which Clemson addresses through a variety of best practices that should be part of any organization's security strategy.

First among these best practices are human resource procedures. A criminal background and E-verify check is conducted on all university personnel prior to their hire and employees are bound by confidentiality in their work. In addition, establishing a series of policies and procedures provides a foundation by which Clemson's security strategy has been developed and lays the framework under which security operations function. Included topics among the policies are Acceptable Use, Userid and Password, Network Security, Server Administration, and Data Center access. Regarding security clearances, employees needing access either physically or virtually, must be requested and authorized by supervising personnel based on the employee's job function requirement. Restricted or secure areas are protected by monitored and recorded video surveillance and key-card access. Additionally, the main data center facility has staff on-site 24/7/365. Technical controls are put in place based on the evaluated risk, a variety and matrix of controls would be deployed that might include physical or logical network segmentation, Firewall and Access Control List use, increased and elevated levels of monitoring, separated Virtual Private Network use, limited availability of access, and more stringent levels of credential use.

SCALABILITY—SC CLOUD AND HEALTH SCIENCES SOUTH CAROLINA EXAMPLES

For most organizations, economics is the force multiplier driving them into cloud computing to realize enterprise efficiencies both in terms of IT spending and asset utilization. Clemson has been in the "cloud business" for over 30 years provisioning Medicaid applications services to the State and citizens of South Carolina. As previously mentioned, the SC Cloud evolved into a State-wide consortium of institutions who either could not afford to address the infrastructure needs on their own or did not have the expertise to deploy in-house resources. What once started as a Clemson private cloud need, evolved into a community cloud where the volume of computing and cloud services increased, but yet did not result in any service degradation at Clemson. These institutions realized the economic benefit of fully participating in the SC Cloud, especially in the context of high-performance computing, as it enables them access to a set of resources that are flexible, scalable, and reliable to meet current and future needs. Institutions participating in the SC Cloud include both public and private universities, including technical colleges and Historically Black Colleges and Universities,[10] or HBCUs.

Likewise, the SC Cloud further evolved and scaled to provide flexibility for the Health Sciences South Carolina referred to as HSSC.[11] HSSC is composed of six of South Carolina's largest health systems and the State's largest research-intensive universities. This State-wide biomedical research collaborative has a vision of transforming the State's public health and economic well-being through research as well as education and training of the health-care workforce. Given Clemson's security strategies previously described as well as our experience being the primary provider of operational support to South Carolina's Department of Health and Human Services for Medicaid transactional processing and eligibility determination, HSSC de-

[9] Cloud Security Alliance. "Top Threats to Cloud Computing V1.0." March 2010. <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

[10] United States Department of Education—Historically Black Colleges and Universities <http://www2.ed.gov/about/inits/list/whhbcu/edlite-index.html>

[11] Health Sciences South Carolina. <http://www.healthsciencessc.org>

termined that the SC Cloud would be a natural fit not only for infrastructure, platform, and software cloud services, but also for security as a service. Clemson essentially serves as the Information Security Office for HSSC by providing the same suite of services afforded to Clemson, but also applying the same confidentiality, integrity, and availability philosophies, strategies, controls, policies, and procedures within a HSSC context. This environment shares much of the infrastructure utilized by Clemson, yet is segmented in such a way so as to provide a hybrid cloud that addresses both Clemson's and HSSC's needs.

Building upon the previously-mentioned security best practices, Clemson's experiences with scalability has demonstrated four additional areas of consideration when forging a cloud computing security strategy. First among these is ensuring a trust relationship is established between client and provider. Current cloud models are widely used because they provide economies of scale. They also, however, outsource data and resource management to third parties. Clients must rely on the ability of the provider to assure privacy, accuracy, and availability of information. Developing a trust relationship, as in the case of HSSC with Clemson, is an important consideration in ensuring the safety of data. Clemson's experience with Medicaid data as well as the policies, procedures, and controls that are put in place enable an increased level of trust. Continual interaction and engagement has resulted in Clemson being at the table when HSSC is in the early stages of application development and the subsequent change management. This has resulted in security and privacy being an integrated, proactive part of HSSC's planning and operations.

Clemson University's relationship with HSSC members has been strengthened with their deployment of previous investments in authentication research and development. Clemson University is a participating member of Internet2's InCommon federated identity management supporting Shibboleth authentication. HSSC systems has utilized Shibboleth authentication to allow for multiple trusted participating members to leverage their own identity management vetting process and procedures for access to HSSC systems. This is a great example of how R&D has produced a viable, productive application and methodology to achieve greater efficiencies and ease of use without compromising the security of the system.

Second, the level of cloud integration should be considered. Depending upon an organization's mission and requirements, an organization may only take advantage of cloud infrastructure services. Some may pursue software as a service. Yet others may outsource the entire suite of cloud services, including security as a service. In the case of HSSC, the SC Cloud provides infrastructure, platform, and security. In other words, one size does not fit all and a cloud provider should be flexible.

Third, natural disasters such as Hurricane Katrina, the recent earthquake in Japan, and the Midwest floods show the importance of disaster recovery and business continuity. Documenting a plan and implementing redundancy technologies are obvious components of this planning. Conducting test failovers and actual physical disaster drills on a periodic basis should also be included in any DR/BC strategy. Many lessons are learned when physically conducting a disaster exercise that enable an organization to be better prepared.

Fourth, one of the reasons HSSC chose Clemson is because of its Medicaid provisioning experience with medical data, compliance, and audit response. Clemson has a proven track record of being able to address internal and external audit requests and quickly address any findings. A cloud service provider should be able to address their experience and capabilities in dealing with Federal compliance and audit needs.

IDENTITY AND ACCESS MANAGEMENT

Considering the diverse set of users that the SC Cloud has and the numerous organizations that connect into the environment, it is important to properly ensure identity and access management (IaAM). Identity and access management concerns the need to permit access to enterprise resources only to authenticated users, with access to only the data they have permission to view or change. Without appropriate procedures in place to verify access, concerns over identity theft and the insider threat can arise.

Authentication is performed when a computing session starts. In existing systems, a user is authenticated in one of three ways: Knowledge, which is something the user knows such as a password; possession, which is something the user has such as a smart card; or identity, which refers to biometrical aspects, such as a fingerprint.

Clemson's experience has been that identity and access each can be problematic. Passwords can be forgotten, sent over the network in clear-text, so that they are readable in transit or revealed inadvertently. Simple passwords are easy to guess.

Complex passwords are easily forgotten, or need to be written down. Taking IaAM issues a step further, smart cards, dongles, or other authentication tokens can be stolen. Voiceprints may have false negatives if the user has a cold. People are hesitant to use retina scans, since they seem invasive. Biometrics can also be spoofed. Clemson limits these challenges by requiring complex passwords, providing training to faculty, staff, and students, and using a single-sign-on service that forces password encryption in transit over the network.

On a local machine, authentication is straightforward. If authentication uses knowledge, for example a password, the user is prompted directly for the information. If possession is used, the token (ex. smart card) can be interfaced directly to the computer. Some authentication systems give the user a device that displays a code value to enter into the system. For biometrics, a physical device has to interact with both the user and the computer system. Two-factor authentication uses more than one authentication technique. This helps minimize the damage caused by keyloggers and related tools.

All these approaches assume the device used to access the internet is trustworthy. If the local hardware or software is not trustworthy (for example compromised by malicious software) this will compromise both knowledge and biometric authentication.

Access control is at least as challenging as authentication. When all data and users were locally created and managed, it was relatively easy to provide controlled access. However, in the cloud, it is more difficult to provide controlled access. It is possible for there to be different levels of security for systems and different levels of assurances for users. The basic infrastructure security level within a public cloud should match the level of the highest security need, not be a mixed bag of approaches. Understanding the access control security practices as well as the results of the provider's risk assessment efforts are essential considerations. As discussed later in my testimony, further study is needed in the area of identity and access management technologies and policy.

CONSIDERATIONS

Mr. Chairman, the power of cloud computing offers tremendous advantages to both the commercial and public sectors. For our Government agencies in particular, cloud migration represents an achievable strategy for deriving the tangible cost savings that the current economic and fiscal environment demand. Furthermore, it enables both the smart, streamlined organizational construct that Government employees need to better perform their mission, and the more efficient services delivery model that taxpayers deserve. And, while I have enumerated some of the challenges that exist, it is my view that the benefits of cloud far outweigh the risks, and that a thoughtful strategy for prudently broadening adoption of cloud services can facilitate a smooth transition to this dynamic platform. Many of the security-oriented policies, procedures, controls, and best practices previously mentioned are key elements of any security strategy. Additional components that such a strategy might consider include current areas of research and development, education and workforce priorities, and economic implications.

AREAS OF RESEARCH AND DEVELOPMENT

Many areas of research and development exist in the cyber-security field. It is my opinion as well as the opinion of other researchers in the field that Cybersecurity R&D is best conducted in an operational environment as opposed to a simulated environment. The SC Cloud was set up in an operational environment with this principle in mind. IT staff provisioners work side-by-side with researchers from academia and industry across the spectrum. Cybersecurity is critical to all communities. An exemplary Federal program that includes this program is the NSF funded Global Environment for Network Innovation or GENI.[12] Core premises of GENI are that the internet architecture is over 25 years old and in need of strengthening and updating. A second premise is that network R&D should be conducted on the internet itself and the GENI approach is to use "slices". Analogous to the use of virtual machines to allow isolated computing on a shared computer, emerging technologies now allow virtual network slices to be created on shared network infrastructure to allowed isolated network operation. Network virtualization not only allows cyber R&D occur on production internet in protected ways, it also enables isolated and secure enterprise operations to take place on a shared network.

My comments will highlight some research, which in my opinion are of importance and worthy of investment.

[12] Global Environment for Network Innovations (GENI). <http://www.geni.net>

The first area of R&D involves the use of virtual machines (VMs) in clouds. Cloud computing is enabled by virtualization. This has enabled servers to migrate from one host to another dynamically for load balancing as well as made easier dynamic recovery from hardware failures. Security can be enforced by executing programs on different virtual machines. Virtual machines, however, are subject to various vulnerabilities. Researchers at Clemson have shown how power and timing data can be used to extract information, including cryptographic keys, from running systems. Further research is needed to establish what hardware safeguards are required to effectively protect virtual machine environments.

The second area of R&D is authentication, authorization, and accounting. Current security approaches leverage current best practices for authentication, authorization, and accounting relying on Public Key Infrastructure (PKI) and a certificate authority (CA) hierarchy to establish a chain of trust. Traditional approaches are designed to secure monolithic computing entities, but the distributed nature of the cloud could be leveraged to provide additional security.[13] As cloud computing leverages distributed resources at different sites and potentially of different ownership—for example, an enterprise might dynamically purchase computing resources from multiple cloud providers for resilience, load balancing, and cost optimization, the cloud user needs ways to identify itself in consistent, unified, secure, and portable means to all resources.

R&D on security applications and tools is another area of research that focuses on the creation of applications that leverage the distributed nature of the cloud to provide a new level of security that neutralizes security vulnerabilities and the various classes of attacks. This research would result in a cloud environment that is resistant to both infections of individual hosts and the current generation of network-based attacks.

Another R&D area is encryption for programs and data for processing. Recent work[14] has produced a true homomorphic encryption system that allows computers to execute encrypted programs. In theory this should be free of side-channels, but the newness of this approach means that vulnerabilities may still be found.

Research on Distributed Denial of Service (DDoS) detection and control is also needed. A Distributed Denial of Service attack is an attempt to make a computer resource unavailable to its intended users. A DDoS attack can shut down cloud service site or constantly affect cloud performance, thus increasing the costs. Currently there is not a good mechanism for DDoS detection and control. It is not possible to detect the source of the DDoS or control the traffic. DDoS is currently an intensive area of research. For example, the National Science Foundation's GENI project funds researchers at Clemson to leverage OpenFlow, a software-defined networking technique, to flexibly analyze network traffic for DDoS threats and control different categorized traffic to ameliorate detected threats.[15] Some suggestions have been made for ways to create DDoS-resilient clouds.[16]

Finally, research on network technologies is also important. Current protocols and tools in place today make it difficult to make networks available dynamically to match the elasticity in clouds. Networks tend to be static and specialized with data passing through hundreds of thousands of separate network devices that operate individually instead of as a unified system. A paradigm shift is needed to instill more dynamic control plane flexibility to match the growth of diverse applications and devices utilizing cloud services, including mobile, across entire networks in a cloud environment.

Such a paradigm shift can be seen today through the implementation and use of Software Defined Networking (SDN) technology such as OpenFlow,[17] which has been developed as the network layer of the GENI model. SDN moves the control plane from the individual network device to external controllers that can view and manage a network as a system instead of a vast network of individually-configured

---

[13] R.R. Brooks, "Mobile code paradigms and security issues," *IEEE Internet Computing,* vol. 8, no. 3, pp. 54–59, May/June 2004. R.R. Brooks, *Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks,* CRC Press, Boca Raton, FL, 2005.

[14] C. Gentry, *A Fully Homomorphic Encryption Scheme,* Ph.D. Dissertation, Dept. of Computer Science, Stanford University, 2009. T. Rabin (ed.) *Advances in Cryptology—Crypto 2010.* LNCS vol. 6223, Springer Verlag, Berlin 2010.

[15] Brooks, Richard and Kuang-Ching, Wang. EAGER-GENI Experiments on Network Security and Traffic Analysis. National Science Foundation Award No. 1049765. <http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1049765>

[16] Dingankar, C. (MS) "Enterprise Security Analysis Including Denial of Service Countermeasures," ECE Dept. Clemson University (August 2007). C. Dingankar, S. Karandikar, C. Griffin, and R.R. Brooks, "On Bandwidth Limited Sum of Games Problems," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,* 41(2) 341–349, March 2011.

[17] OpenFlow. <www.openflow.org>

devices. Additionally, SDN makes it easy for new network protocols to be rapidly prototyped into production networks.

In addition, adaptive and intelligent networking that does not rely only on the end-host or individuals for correct protocol application is an important area of study. One cannot rely on all providers having firewalls, consistent security standards, intrusion detection, etc. Distributed tools are needed to enable automated security through improved network monitoring to analyze traffic patterns and detect/isolate vulnerabilities as well as securing internet traffic in distributed and seamless ways.

EDUCATION/WORKFORCE PRIORITIES

Mr. Chairman, in addition to R&D, it is also critical that we have a security-conscious workforce. There is a gap that exists between what universities teach and industry needs. Universities teach theories and fundamentals whereas industries desire practical experience from university graduates. This is difficult to incorporate into the curriculum. Programs are needed to facilitate bridging this gap and partnerships between universities and 2-year technical and community colleges should be encouraged. In addition programs that encourage students to major in science, technology, engineering, and mathematics (STEM), including an emphasis on cybersecurity, are needed.

NSF GENI is an example of program that is filling this gap by creating an environment linking industry with university research thus providing experiences for students to receive training and education on core technologies that are applicable in the workforce. In addition, GENI also extends these opportunities to multiple disciplines ranging from computer software, computer system, networking, to hardware engineering thus giving a student a broader experience of conducting research and having regular interaction on a large scale with other fields of study. Federal facilitation of similar programs in cross-cutting areas may begin to close this gap over time.

ECONOMIC IMPLICATIONS

There is a growing body of research involving interactions between information security and economics.[18] Current market incentives reward behaviors that do not safeguard the well-being of the public. This is in direct conflict with the Institute of Electrical and Electronics Engineers (IEEE)[19] and Association for Computing Machinery (ACM) codes of ethics.[20]

Hardware and software markets have network externalities: The value of an investment depends in large part on whether or not other parties make the same purchase decision.[21] These markets are "tippy," i.e. miniscule differences in quality or perception result in major differences in profitability. In our industry, network externalities often result in markets where one product dominates the market. This explains the historically dominant market positions of the IBM PC, Microsoft Windows, and Intel processor architecture.[22] The need to be the dominant player induces pressure to be "first to market" with new applications. Arriving early usually tips the market enough to dominate it. In this "winner take all"[23] context, actions that improve product quality and security, but delayed delivery can be fatal to an enterprise.

This is exacerbated by software being a "lemon market"[24] with information asymmetry between buyer and seller. The buyer cannot reliably distinguish between quality goods and shoddy products. Under these conditions, buyers choose the lower-priced product. Shoddy products are produced more cheaply, driving quality products from the market.

These factors encourage the industry to quickly produce large quantities of poorly analyzed programs. There is little financial incentive to do otherwise and much to

---

[18] Anderson, R. and T. Moore, 2008: Information security economics—and beyond. *Lecture Notes in Artificial Intelligence,* 5076, 49.

[19] Institute of Electrical and Electronics Engineers Code of Ethics <http://www.ieee.org/about/corporate/governance/p7-8.html>

[20] Association for Computing Machinery Code of Ethics and Professional Conduct <http://www.acm.org/about/code-of-ethics>

[21] Katz, M.L. and C. Shapiro, 1985: Network externalities, competition, and compatibility. *The American Economic Review,* 75, 424–440.

[22] Besen, S.M. and J. Farrell, 1994: Choosing how to compete: Strategies and tactics in standardization. *Journal of Economic Perspectives,* 8, 117–131.

[23] Dekel, E. and S. Scotchmer, 1999: On the evolution of attitudes towards risk in winner-take-all games. *Journal of Economic Theory,* 87, 125–143.

[24] Akerlof, G.A., 1970: The market for "lemons": quality uncertainty and the market mechanism. *The Quarterly Journal of Economics,* 84, 488–500.

gain. The consequences of poor software quality for consumers and the economy as a whole are immense. Dr. David Rice cites NIST studies showing the annual cost of insecure software to the United States as conservatively $180 billion.[25] He also cites a market research survey, which finds 75 percent of computers connected to the internet have been infected and used to distribute spam. Computer and network security is likely to remain a difficult problem for the foreseeable future. Research and development of secure systems will be costly, but that cost is expected to be much less than current losses due to on-line system misuse.

OTHER CONSIDERATIONS

In addition, Mr. Chairman, there is one other priority that I believe will receive attention as cloud services grow, namely the many legal issues surrounding cloud computing. Contractual and service-level agreement issues regarding physical data protection, incident response, confidentiality, access, availability, privacy, security controls, and other such critical matters are important aspects in developing a relationship with a provider. Likewise, intellectual property issues and export controls, meaning where is the data being stored, should also be discussed in a cloud computing strategy. It is conceivable that some cloud service providers could store data outside the United States for backup or archival purposes. Also, consideration should also be given to the portability of data and what happens to the data once a provider contract is terminated. Safeguards and assurances are important to ensure all data packaged for migration to a new provider and that all data is cleaned and removed from any provider asset. Finally, considering the level of hardware manufacturing that occurs overseas, assurances that personal computers, tablets, etc. do not contain viruses or other security compromising elements is needed.

Mr. Chairman, on behalf of Clemson University I would again like to thank you for the opportunity to testify before the subcommittee and I look forward to your questions.

Mr. LUNGREN. Thank you much, Mr. Bottum. I was just thinking that cloud computing is the only thing I have not heard being argued for the breakup of the Big East or ACC, and I suspect that maybe we will be hearing about that——

Mr. DUNCAN. Will the gentleman yield?

Mr. LUNGREN. Sure.

Mr. DUNCAN. Go Tigers against Boston College——

[Laughter.]

Mr. LUNGREN. Well, I have got a neighbor who is a freshman at Clemson, so I will say okay.

Mr. Curran.

STATEMENT OF JOHN CURRAN, CHIEF EXECUTIVE OFFICER, AMERICAN REGISTRY OF INTERNET NUMBERS

Mr. CURRAN. Thank you, Chairman Lungren, Ranking Member Clarke, Members of the subcommittee, for having me here today. You have my written testimony so I will keep my verbal comment brief.

I am going to focus on areas related to using the cloud over the public internet, because that is truly what is new in what we are discussing. Dr. McClure, earlier today, indicated that the use of public clouds poses new areas of risk, and I would like to highlight four of those that this committee should consider when looking at this issue.

First is, the relationship of public clouds to other initiatives within the Federal Government for cybersecurity needs to be carefully considered, because public clouds are using vendors outside the Federal Government, yet the Federal Government has several Government-wide security initiatives. These include HSPD–12 for vali-

[25] Rice, D., 2008: *Geekonomics.* Addison-Wesley, Upper Saddle River, NJ, 2nd ed.

dation and authorization; this includes the Trusted Internet Connections program.

When you make use of a public cloud and a public vendor they may not be familiar with how to actually use those initiatives, which are Government-wide cybersecurity initiatives. So the documentation and the approach to vendors so that they have everything they need when they design their public cloud to make use of Government-wide cybersecurity initiatives is essential. Otherwise, our public clouds won't be participating in our Government-wide initiatives. This is very important.

Second is the issue of the physical location of the actual data and systems. The FISMA framework and the FISMA security control profile always had an assumption within it of Federal control of the facilities or systems. It is true about 10 percent of our Federal inventory is outsourced to contractors, but even then, it is outsourced in a way that puts it directly under agency control to the vast majority of cases.

When we make use of public clouds we suddenly have the idea of using a FISMA profile that is 10 years old to secure public clouds that may actually be worldwide in nature. The problem, of course, is that the questions to be asked—where is the data, where is the systems—simply don't exist in the original FISMA profile.

Now, the proposed FedRAMP security profile does have enhancements, and one of the enhancements it includes is talking about the personnel that are making use of managing this data. In the current public drafts it does not include, however, controls for where is the data and the systems themselves? So we know, in many cases, that the systems are managed by U.S. citizens, but we don't know necessarily that they are located within the United States.

A given agency can implement SLAs to cover that if they know to do so. What might be a better approach is making that inherently part of the profile, so as GSA accredits organizations they say where there systems are, so a Federal agency CIO has the ability to say: Is that acceptable to me or not?

The third matter is on migration, and I guess this is more important. The FISMA profile is very good about talking about recovering of systems; it has a whole contingency planning section which handles the failure of a given server or data center. That was perfect for when we were talking about Federal agencies.

But the recovery now that is provided by the FISMA profile now works within the cloud. It is whether a cloud provider provides fail over one of their data centers to another one of their data centers.

The problem is, we now need contingency planning at one level higher up. In fact, you need to worry about the case where the cloud provider themselves is no longer able to provide service securely and you need to move not to another one of their data centers but to an entirely different cloud provider. You might need to do that on very rapid notice to accommodate a cloud provider who is compromised in an irrecoverable manner.

So the migration is not a question just of cost or being able—agencies being able to get their own data back. It is actually a security control. It is an inherent function that needs to be provided so that if a cloud provider is compromised the ability to migrate

isn't a question that we are all asking; it is inherent and it is known to be able to quickly move up in a short number of days or hours and move to another provider.

Finally, the internet itself: The internet itself is not static. It is changing rapidly, and there are several security protocols, such as DNSSEC, to secure the Domain Name System, and I.P. version 6, the new internet protocol that is coming out, that need to be considered. We need to make sure these are part of the profile for FedRAMP so we don't build on the internet while the internet is changing out from under us.

I would like to thank the committee for having me. I look forward to your questions.

[The statement of Mr. Curran follows:]

PREPARED STATEMENT OF JOHN CURRAN

OCTOBER 6, 2011

I. INTRODUCTION

Good morning Chairman Lungren, Ranking Member Clarke, Ranking Member Thompson, and Members of the committee, and thank you for inviting me to testify before the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee.

I am the president and chief executive officer of the American Registry for Internet Numbers, Ltd. ("ARIN"), which issues Internet Protocol (IP) number resources for the United States, Canada, and Caribbean, but I am speaking here today in my personal capacity based on a long history of building and securing FISMA-compliant Federal Information Technology (IT) systems.

I have first-hand knowledge of these matters from my experience in the internet industry since 1990, including serving as the chief technology officer for several Government contractors and Internet Service Providers (ISPs) including BBN, GTE Internetworking, and XO Communications, as well as internet standards work in the Internet Engineering Task Force (IETF). Most recently, I served for 5 years as executive vice president and chief technology officer for ServerVault, providing secure managed IT services for sensitive Federal Government applications. My duties included direct responsibility for securing and preparing the certification of FISMA Moderate impact level Federal information systems over shared internet-based infrastructure. I have prepared my remarks today out of a desire to see the advancement of responsible Cloud-based computing for the Federal Government.

I would like to start by offering congratulations to the GSA for the development of its Federal Risk and Authorization Management Program (FedRAMP) program, as well as the recent Infrastructure as a Service (IaaS) Blanket Purchase Agreement (BPA) awards. By developing this program in cooperation with the Federal CIO council, the GSA has enabled agencies to leverage cloud-based storage, virtual machines, and web hosting services in a manner that should improve the cost and timeliness of Federal IT system deployments.

II. MANAGING EMERGING RISKS FROM CLOUD COMPUTING

As a result of my experiences deploying Federal IT systems over the public internet, I was asked to present at cloud interoperability workshop in 2009, and to identify the most critical challenges that Federal CIO's faced in making use of cloud computing under the existing FISMA security framework. Back then, the major difficulties that I identified were:

- Agency pressure for deployment of timely, cost-effective IT systems;
- Administration expectations for leveraging new IT technologies;
- Compliance with IT policy mandates (Federal and agency-specific);
- Lack of common IT infrastructure services between systems & Potential vendor lock-in with any sizable deployment;
- Preparation of extensive FISMA control documentation for each system.

It is remarkable to see the progress that has occurred since that time. As a result of the FedRAMP program (with its common security control baseline), agencies now have a clear roadmap that should address many of these challenges in making use of cloud computing for Federal IT applications.

I must note, however, that cloud computing does not eliminate all of the challenges, and in particular, cloud computing may actually heighten the difficulties that Federal CIO's face in some areas if not carefully managed. The areas that are most likely to pose increased risks as a result of the introduction of cloud computing are:

1. Interaction of cloud computing services with Federal cybersecurity initiatives;
2. Physical location of cloud computing facilities and data;
3. Migration between vendors of cloud computing services;
4. Evolution of cloud computing services with internet technologies.

None of these risks precludes the use of cloud computing services by the Federal Government, but each does pose new challenges for Federal CIO's to consider and may warrant consideration by the Federal CIO Council and its partners to determine if additional standards or coordination activities would help minimize these risks. I will outline each of these risk areas with recommendations for further consideration.

III. INTERACTION OF CLOUD COMPUTING SERVICES WITH FEDERAL CYBERSECURITY INITIATIVES

There are several Government-wide IT security initiatives that require consideration with respect to cloud computing because of their service nature: Specifically, there is the distributed issuance and recognition of user authentication credentials via the HSPD–12 initiative, as well as the provision of secure and monitored internet connectivity via the Trusted Internet Connections (TIC) initiative. These programs provide certain security-related services to Federal IT environments which result in increasing cybersecurity protection on a Government-wide basis as more agencies make use of the services.

While specified in the FedRAMP security profile for Moderate risk environments, the actual mechanism and ability to participate in these Government-wide cybersecurity initiatives by private cloud computing vendors remains unclear, and any deployment of Federal IT systems via cloud computing services that do not leverage these common capabilities dilutes the value of these initiatives in supporting the overall cybersecurity stance of the Federal Government.

The goal must be to have unequivocal documentation for cloud computing companies on how to appropriately secure their offerings, including how to make use of Government-wide cybersecurity initiatives, and thus encourage significant industry-wide vendor participation in offering FedRAMP cloud services. The resulting competition will both drive down costs and improve service quality for all FedRAMP participants.

IV. PHYSICAL LOCATION OF CLOUD COMPUTING FACILITIES AND DATA

One of the more unusual consequences that results from the use of the cloud computing is the potential loss of the ability to know at any given time the specific physical location for the systems and data which support a given Federal IT system. While it may be possible to know the set of data centers which support the service (and the FISMA-based FedRAMP security control profile does specify certain physical controls at such facilities for facility access, power redundancy, etc.), the question of actual physical location of the Federal IT system is highlighted when the cloud service provider has facilities which are outside of the United States.

As a practical matter, there may not be a concern with incident services being provided for out of non-U.S. locations, and it may be desirable in some circumstances with Federal applications that must be accessed globally. However, the present FedRAMP profile does not directly address the question of location and it is not assured that use of facilities and storage of data outside the United States is universally desirable, particularly if the use of cloud computer for Federal IT applications is undertaken on a large scale.

The FedRAMP program should include controls that address the physical location of cloud computing facilities and data storage used by the application, and allow (as is done with the corresponding personnel controls) for the consideration of exceptions once fully documented and reviewed.

V. MIGRATION BETWEEN VENDORS OF CLOUD COMPUTING SERVICES

The ability to extract agency data in standard formats from cloud computing services (whether that be application data such as mail messages and mailing lists, or system data such as the virtual server, storage, and network configurations) is essential to be able to migrate between cloud vendors. Lack of this capability means vendor lock, eroding the financial benefits of cloud computing and preventing timely response if a vendor's security is irrevocably compromised.

There are on-going efforts in the area of standards for cloud computing data, and this work should continue and be prioritized by the agencies supporting the FedRAMP program. Unlike an internal agency information system, cloud solutions are inherently subject to change by the cloud service provider, and this creates a new requirement (specifically, the ability to quickly and reliably migrate to another service provider) where it previously was not needed for agency systems. FedRAMP must facilitate migration capabilities to protect against any cloud computer vendors that fail to continuously deliver the necessary quality or security in their offerings.

The FedRAMP security control profile includes standard FISMA contingency planning and recovery security controls, but these fundamentally only address recovery within a given service provider cloud. Specific mechanisms should be put in place to insure that Federal agencies can extract their data and configuration in generally accepted formats and that these mechanisms suffice for service migration to other cloud computing vendors.

VI. EVOLUTION OF CLOUD COMPUTING SERVICES WITH INTERNET TECHNOLOGIES

The internet is constantly evolving with the introduction of new standards and technology, and in making use of the internet as a platform for cloud computing, FedRAMP must be equally prepared as these changes occur. This is particularly true when it comes to internet technology improvements in the area of cybersecurity.

In many cases, the Federal Government has taken an active interest in the technologies and standards that could improve the overall security of the internet, and this includes DNSSEC initiative in securing the Domain Name System (DNS), the next version of the underlying network protocol for the internet—Internet Protocol version 6 (IPv6) and on-going work in internet routing security. These technologies are now being deployed in the public internet, and are also covered by specific directives in the FISMA security control baseline and/or guidance from OMB.

These new standards are quite important in protecting the global internet from cybercrime, in that they insure that internet users reach the actual website that they intended to, and that their communication is protected in the process. When it comes to agency use of cloud computing services, these protections are equally important, since these services are reached over the public internet.

It is crucial that the FedRAMP program clearly and unambiguously incorporates DNSSEC and IPv6 into the FedRAMP baseline, and that on-going developments in internet-wide security technologies are promptly incorporated as they reach maturity.

Furthermore, the on-going need to adopt and maintain state-of-the-art security technologies and practices for cloud computing services does not appear to be given sufficient priority in the FedRAMP approach. While traditional Federal IT systems have been built and certified one at a time in predominantly closed environments, the rapid pace of evolution of internet threats requires equally dynamic and responsive security responses. Vendors should be given the flexibility to propose additional or alternative security mechanisms, as there are security lessons learned from running large-scale internet services that are not readily available to the Federal IT community, and the benefits of such experience should not be lost in the process of structuring cloud services into the FISMA framework.

VII. CONCLUSION

The FedRAMP program is a remarkable achievement; by providing agencies with ready access to additional computing resources that have already undergone a joint authorization process, the program offers the potential to significantly improve cost and timeliness of Federal IT deployments.

While not detracting from the importance of this achievement, the use of public and shared cloud computing services does introduce new areas of risk to be considered, and this is particularly true with respect to the interaction of cloud computing services with Federal cybersecurity initiatives, the geographic location of Federal data, the migration between vendors of cloud computing services, and the evolution of cloud computing services with the internet.

The risks should not preclude use of cloud computing services by the Federal Government, but the model should be closely examined, and appropriate efforts inserted into the FedRAMP program so that it can deliver its full benefits in an efficient and secure manner.

Mr. Chairman, Ranking Member Thompson and Members of the subcommittee, this concludes my written statement.

Thank you again for this opportunity to speak before you today on this important topic, and I would be happy to answer your questions.

Mr. LUNGREN. I thank you, Mr. Curran.

I thank all of you for your testimony, and I will yield myself 5 minutes for first questions.

Mr. Sheaffer, one of the things that struck me as you spoke was the idea that in the past, with the internet and so forth, we didn't build in security at the outset and we have had to play catch-up. Mr. Curran has just outlined a number of things that deal with building security into our advances in computer technology, including the cloud. Could you comment on the comments that he made?

Mr. SHEAFFER. Certainly, sir. I agree that we are in a position where we are using a technology and infrastructure that was not originally intended to be with the security issues in mind, and I agree that there are a number of initiatives underway to address a number of those vulnerabilities and issues.

I think there has been a—there is good examples that exist in—within our intelligence community and in the secure side of Government operations that point the direction that we are able to build architectures that can secure data and applications adequately in a private cloud environment. I think some of the comments were addressed to how are we going to do that in the public environment, and I would go back, I think, to some comments in the earlier panel that suggest that until we can do that we have to be careful about what we put out into the public domain.

But the interest of the commercial sector is to, as quickly as possible, get to a point where they can provide those adequate protections and the innovation that is going on in the commercial world, I think, will solve those problems in time.

I think in the mean time I would agree, we have to be aware of what they are, do what we can from a standards perspective to build in standards and approaches that will guarantee to the maximum extent possible that those vulnerabilities can—and risks can be managed. But we will, as a—from a technological perspective, solve those problems.

Mr. LUNGREN. Mr. Brown, it appears one of the messages from this panel is that the dynamism of the I.T. world——

Mr. BROWN. Yes.

Mr. LUNGREN [continuing]. That we make a mistake when we take a static view of things and that cloud computing is one evolutionary point in this utilization of advanced information systems. So therefore, we have got to try and, from our standpoint, make decisions that reflect that.

At the same time, there is this sort of fundamental issue or concern that reflected in both constituencies and Members of Congress that there is something about possessing a system, there is something about possessing your own information, there is something about fencing off your information from everything else, which is perversely at odds with using the internet.

Mr. BROWN. Right.

Mr. LUNGREN. Yet, people seek both the ease of access and the multiplication of recipients of their information that the internet offers with a heightened sense of privacy. So I think one of the great concerns we have to deal with—both legitimate aspects of it and, let's say, hyped aspects of it—are that as you surrender your possession of the system and move more to a cloud system, which,

as I get your various definitions, essentially means you are cooperating with other systems in a way that your information is not totally under your control, how do we both overcome the fear that people have a loss of security because of a loss of possession, but at the same time assure them that we do have technology fixes so long as we understand that that requires a sufficiency of information that the users have and a persistence in the use of what I will just call generally good cyber hygiene?

Mr. BROWN. So, one of the things that we have to understand is that from an economic standpoint, cloud is coming, okay? The reason why is that in cloud computing we can do many more releases, put together more software that is better more quickly, we can test it in one environment, we can get higher quality software out of the, you know, out of our building and into the hands of the consumers quicker.

If we don't, as vendors, embrace cloud we will be out of business, okay?

Mr. LUNGREN. That is a pretty strong imperative.

Mr. BROWN. Yes. So it is a very strong imperative. If we don't embrace cloud we will be out of business.

So I think the same goes for governments in the same way, that if you want to keep up, if you want to move quickly, embracing the cloud for the same efficiency reasons needs to occur. Now, anytime we have these types of changes, right, we have opportunities to become better or become worse, right? We believe that cloud gives us an opportunity to become more secure.

Now, the things that need to happen there is you need to have trust in the providers, like as what we said, but you need to be able to verify, right? So you need to be able to have things like FedRAMP that allow you to monitor those providers to make sure they are not only doing what the contract says, but actually doing what they say, right?

You need to be able to be cautious as you go in—enter into these environments to make sure that—you know, in some cases we are going to see huge expansions of cloud providers and only a certain portion of them will survive, so you need to have contingency plans set up to be able to move from one cloud provider to another.

So it is not a question of if it is going to happen. It is going to happen; we are going to move there.

So it is a question of how we get enough trust in that environment that we can effectively move forward. Trust ends up being transparency; it ends up being, you know, acceptance of this is what a—this is what a cloud provider is going to do; and the ability to consistently monitor what they are doing to ensure that, you know, what they—they are doing what they say they need to do.

Mr. LUNGREN. I have got a whole bunch of other questions, but I am going to yield to Ms. Clarke now for 5 minutes.

Ms. CLARKE. Thank you very much, Mr. Chairman.

I want to thank the panelists for lending their expertise to this discussion today.

My first question is, many potential agency users of the cloud believe it is not yet secure enough for their needs. From your perspectives, are they right?

Mr. BOTTUM. Well—excuse me—I am a provisioner, and so I say amen to everything Mr. Brown just said, and it is a question of building up trust. I think with the relationships we have, you know, that is essentially how we got there, was through building the trust of the end-user and the community that we are provisioning for.

The first thing I did 5 years ago when I went to Clemson was consolidate 43 I.T. departments into one, and that is essentially building a cloud for 43 people who used to do their own—departments that used to do their own computing. So over time you have to, you know, build that trust and that true performance.

I think, you know, directly answering your question is it secure enough, we get tested in a number of ways. I think the end-user has to figure out how they, you know, trust but verify, I think.

I mentioned that we run the Medicaid system for the State of South Carolina. We get both planned visits, audits, and we get unplanned visits and audits. So you have to be ready at all times.

It is a matter of communication, policies, people working together. I think, you know, the—to me, you know, the cloud is—you know, we just call it something different every decade. It was timesharing in the 1980s; it was the grid in the 1990s. We did a project with Notre Dame, the Northwest Indiana Computation Grid.

But basically it is, you know, that is essentially what it is, is a matter of people working together and creating a trusted environment, so——

Mr. CURRAN. Let me address this a little bit, and I will pick up on the comments of the earlier panel from DHS CIO Spires. At the end of the day, the question of whether or not secure enough is the agency CIO's determination. That is truly his job.

What we need to do is make sure that the mechanisms we have put in place give that agency CIO enough information to make that determination. The FedRAMP program is a start at a profile of controls that would make public clouds useful to CIOs.

However, right now there are a number of pieces that a CIO has to fill in on their own. If you want your data within the United States that is not in the profile; that is your SLA. If you are worried about migration, that is not in the profile; that is something you are going to worry about.

So the answer is: Is it suitable today? For an ambitious, high-energy agency that decides it is going to take this on, yes, where they fill in those pieces. So the question is whether or not we can make a FedRAMP program where those functions are already provided for, already clearly documented.

That doesn't mean all the data, for example, needs to be in the United States. An agency whose workers are around the globe doing aid might want data centers that are close to where those people are for performance reasons. Someone else doing sensitive work might want to know that the cloud that he is using has said all of its servers are located in the continental United States.

It is making sure that information is in the profile and in the documentation so the agency CIO has the work he has, has the information he needs to do the job of answering that question. I think it is possible to use it today; I think it could be much easier to use with work.

Mr. BROWN. One of the other important points here is that there will be specialized cloud services that are developed for specialized purposes, okay? So, you know, if there is enough money available for someone to produce a cloud service that is ultra-secure, you know, ultra—you know, ultra-secure and ultra-resilient, right, somebody will produce that cloud service from—as long as the economic model fits.

You are going to see other economic models that take less security, and less security less resilience. All of those types of models are okay as long as they transparently tell you what their models are and what they can provide.

Ms. CLARKE. Let me thank you all for your answers. So many questions come to mind once you raise that question and then you get the answers, right? So it is a totally new space. That is a lot of pressure on a CIO.

Then you start thinking about, well, does this become an issue for litigation as, you know, we begin to build those areas of trust, all right? So does that become a whole 'nother practice within the legal field and an understanding of that world that we have created?

So, my time is elapsed and I want to just thank you once again for raising the consciousness here in the Congress of what we need to do. Thank you.

Mr. LUNGREN. There are so many questions, but you have been very good about—let me just ask one general question. When we look at all the positives of cloud computing, however we want to define it, and as the new evolutionary point, is it a canard to suggest, though, that with cloud computing you do create some more target-rich environments? That is, if I could go after a larger bit of information or a larger universe of data points that involve a number of different players it might be worth my while to put more capital investment and time to go after it, or is that just——

Mr. BROWN. Same idea as Fort Knox, right? So can we protect the gold, right? That is the question, right, is: Can we have appropriate safeguards to protect that information?

If you look at what some systems have done, you know, your data actually isn't stored in one central location; little pieces of your data are stored all over, in many different servers all over the, you know, world, therefore they can't be reconstituted into one piece. So, you know, because the data just happens to be stored in the cloud it takes advantage of technology that makes it harder to compromise one data center. It won't help you. You have to compromise the whole system.

So there are technology advantages to, you know, moving to the cloud. But you are right about a target, right? As you have more data in one place it is more of a target, but it is also one of the things that you can centrally protect.

Mr. LUNGREN. Well, I want to thank all four of you for testifying, and the previous panel. This is an issue that we are just scratching the surface on here. I think there is a lot of confusion about it, I guess even, I would say, fear, just because this is a new notion to the larger public, computer—cloud computing.

I think one of our obligations is not only to help clear up that confusion as best we can, but understand the reality as best we can.

I think what you suggest, Mr. Curran, is make sure that all the moving parts are related, that if we do something on the Government side where we think we have certain protections that that is not only communicated with but is operational with public clouds as we work with them, and that we sort of anticipate these things instead of doing patchwork approaches later on.

So I want to thank you. I thank you for your valuable testimony.

Members of the committee may have some additional questions for you and, we would ask you if you would please respond to those in writing upon your receipt. The hearing record for Members will be held open for 10 days, and the subcommittee stands adjourned.

[Whereupon, at 12:56 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE WILLIAM KEATING FOR RICHARD SPIRES

Question 1a. I'm concerned about maintaining the security of Government data maintained and transmitted through mobile data storage devices, particularly USB flash drive products. While I appreciate the obvious day-to-day benefits of flash-drive technology, flash drives infected with malware, as well as lost and stolen drives, present a clear threat to our Government's information systems. I understand that some flash drives use hardware—instead of software—authentication, which protects the devide from malware and hacking.

Are you familiar with hardware-authenticated drives?

Answer. Response was not received at the time of publication.

Question 1b. If so, to what extent have you tested and evaluated them?

Answer. Response was not received at the time of publication.