Written Testimony of
Jim Bottum, Chief Information Officer
Clemson University

Before the
U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, & Security Technologies
The Honorable Dan Lungren, Chairman

Cloud Computing: What Are the Security Implications?

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[i] 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 Definition of Cloud Computing[ii]. ***Private cloud*****s** 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**[iii] 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 ~1700 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, online 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.

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[iv]. The US 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 two minutes, a drastic improvement from previous wait times of 20 minutes[v]. The Department of Energy estimates it will save $1.5 million over the next five years in hardware, software and other labor costs from implementing a cloud solution at the

Lawrence Berkeley National Lab for its email accounts and from utilizing Google Sites and Google Docs for its scientific research teams[v].

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[vi]. 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[vii]. 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[viii]. 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 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"[ix]. 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 employees 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 statewide 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,[x] or HBCUs.

Likewise, the SC Cloud further evolved and scaled to provide flexibility for the Health Sciences South Carolina referred to as HSSC[xi]. HSSC is composed of six of South Carolina's largest health systems and the state's largest research-intensive universities. This statewide biomedical research collaborative has a vision of transforming the state's public health and economic wellbeing through research as well as education and training of the healthcare 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 determined 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 key-loggers 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[xii]. 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.

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[xiii]. 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[xiv] 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[xv]. Some suggestions have been made for ways to create DDoS resilient clouds[xvi].

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[xvii], 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 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 two-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 cyber-security, 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[xviii]. Current market incentives reward behaviors that do not safeguard the wellbeing of the public. This is in direct conflict with the Institute of Electrical and Electronics Engineers (IEEE)[xix] and Association for Computing Machinery (ACM) codes of ethics[xx].

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[xxi]. 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[xxii]. 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”[xxiii] 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"[xxiv] 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 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[xxv]. 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 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.

References

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

[ii] 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>

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

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

[v] 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>

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

[vii] 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-cloud-computing-report-for-carbon-disclosure-project-forecasts-12-3-billion-financial-savings-for-us-firms/->

[viii] 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>.

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

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

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

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

[xiii] 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.

[xiv] 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.

[xv] Brooks, Richard and Kuang-Ching, Wang. EAGER-GENI Experiments on Network Security and Traffic Analysis. National Science Foundation Award # 1049765.
< http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1049765>

[xvi] 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

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

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

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

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

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

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

[xxiii] 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

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

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