TechAmerica
FOUNDATION

Statement of

Michael Capellas
Co-Chair
Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2)

The Next IT Revolution? Cloud Computing Opportunities and Challenges.

Before the

Subcommittee on Technology & Innovation

House Science, Space, and Technology Committee

September 21, 2011

Michael D. Capellas, Chairman, VCE.

Good morning, Chairman Quayle, and Members of the Subcommittee. My name is Michael Capellas and I am Co-Chair of the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud. I am honored to be invited to testify on a subject of critical national importance. Cloud computing has far ranging economic implications of utmost relevance to U.S. jobs creation, productivity and technology leadership.

As many on the subcommittee have no doubt observed, cloud computing has taken on many meanings and there is widespread confusion in the market about what cloud means, how to get it, what it's good for and what potential drawbacks to cloud might exist. But the cloud business opportunity is significant, with analysts projecting cloud revenues to top $50B within three years.

Those that follow the technology industry know that cloud computing has been around for many years. It is only recently that revenue projections have sharply increased, so it is important to understand why many experts think cloud computing is poised to grow rapidly over the next decade and why all the cloud hype exists in the marketplace.

The application of IT has been the single most important driver of U.S. productivity over the past two decades. My objective today is to convey the Commission's findings around why the cloud is so important in terms of U.S. competitiveness, including jobs creation and productivity.

But first I want to suggest that most of these predictions about strong cloud market growth are wrong. I think they are wrong because they understate cloud growth and they understate the impact cloud will have in reshaping the IT landscape. Cloud will be like nothing we've seen before. Why is this important to the U.S. government? Information Technology has been synonymous with economic prosperity since the middle of the last century. IT has experienced numerous waves of changes since that time. Previous IT waves include the world wide web, the proliferation of handheld mobile and tablet internet devices, and virtualization technologies that together can provide anytime, anywhere, any-manner connection to data, applications and people. Cloud computing represents the culmination of many waves, and as such it promises to spur the most significant transformation we've seen to date.

Cloud computing will bring unprecedented opportunity to both users and those engaged in the business of IT infrastructure, solutions and services. But what is at stake is significantly larger than the tens of billions of dollars that analysts are describing. I believe cloud computing has the potential to both reshape the IT landscape and shift wealth between nations. Trillions of dollars of global economic wealth will be based upon competiveness in our 24x7 world. Cloud computing as a foundational element to IT can make companies, agencies and organizations more nimble and competitive by boosting productivity and increasing the speed of business. Moving to cloud faster will thus become a key consideration as organizations seek to become more competitive.

As requested, let me take a moment to address the essence of cloud computing. Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Central to cloud computing are concepts of on-demand, self-service to an elastic pool of flexibly provisioned resources with measured service. In contrast to a traditional IT environment where different teams of specialists independently manage servers, networking and storage, in cloud computing these components are pre-assembled in a highly standardized and automated converged infrastructure, and the users do not have to know or care about how the components are put together.

As an analogy, computers used to connect together over proprietary local networks, and it was difficult and expensive for different networks to talk to each other. Information was compartmentalized and generally only available to a few users. IP – the Internet Protocol - was created as a network that could span great distances, and after a few years of solid but not remarkable growth, the entire market rapidly shifted to IP because it had evolved to solve both the problem of distance and the problem of communicating with other networks. IP thus became the de facto standard and users no longer needed to know or care about the underlying network. As a participant in the IP technology wave, I'll note that IP technology development was largely led by U.S. companies and has contributed to U.S. technology leadership, job growth and productivity. Standardizing on IP simplified IT operations, reduced cost, and spurred advances like unified communications and high definition video over IP that we enjoy in our homes today.

Cloud computing also promises to simplify IT operations, reduce costs, and increase the speed and effectiveness with which organizations can do business and accomplish missions. Most Americans already use cloud computing in one form or another. Most social networking sites and thousands of e-commerce sites are "running in the cloud."

But misconceptions and concerns with cloud may impact success for companies and agencies, and I believe continued U.S. leadership in IT is dependent upon U.S. leadership in cloud computing.

The CLOUD^2 commission, comprised of 71 commissioners from leading U.S. companies and academia, delivered detailed recommendations to federal officials on how to best allow the U.S. government to capitalize on the advantages of cloud, while spurring U.S. job growth and enhancing overall U.S. competitiveness in the world market. I was privileged to co-chair the Commission, working with industry leading experts from many U.S. companies, meeting with key customers and government agencies, and leading meetings between the Commission and numerous U.S. government officials. The Commission included some of the technology industry's brightest minds, who put our nation's best interests above individual company interests for the duration of our work effort, displaying focused and intense collaboration over a multi-month period resulting in a highly successful and influential outcome.

The Commission identified a set of common barriers spanning institutional inertial, restrictive policies, and technology concerns such as security and privacy that are currently inhibiting cloud awareness and adoption. Through comprehensive analysis and collaboration, a set of fourteen actionable recommendations along with a prescriptive Cloud Buyer's Guide was delivered to government IT officials and the commercial market as a whole. The Commission recognized the need to enable many paths to cloud computing, and determined that interim steps could be instrumental in accelerating many customers' journey to cloud.

The first step in accelerating the adoption of the cloud and driving U.S. leadership in cloud innovation is earning the trust of current and potential cloud users. Trust in the cloud is a result of a combination of factors that enable individuals and organizations consuming cloud services to be confident that the services are meeting their computing needs. These needs include security, privacy, performance and availability; the factors that contribute include transparency of practices, accountability, resiliency and redundancy, access and connectivity, supply chain provenance, life cycle integrity, and governance.

In response to industry concerns about cloud trust, the Commission created recommendations to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. Specific recommendations are associated with robust identity management, federal data breach laws, the promotion of privacy frameworks, cloud service level transparency, transnational data flows, and re-examining mechanisms for lawful access by law enforcement or government to data stored in the cloud via reform of the Electronic Communications Privacy Act. The Commission encouraged the government to lead by example by increasing adoption of cloud computing and pursuing interim paths to cloud such as converged infrastructure deployments and virtualized data centers. Finally, the Commission made recommendations on policies mandating public disclosure of information about relevant operational aspects of public cloud services, including portability, interoperability, security, certifications, performance and reliability.

Members of Congress are encouraged to absorb the entire set of recommendations and act on them where possible. Excerpts from the Commission recommendations follow below, and the benefits of acting swiftly are clear. Cloud computing will enable companies (and governments) to move faster and be more responsive and flexible. Companies will be able to try several prototypes at once, test their limits, and then build and deploy new, better prototypes—all within a few weeks. This may be the most important benefit of the cloud—it enables companies of all sizes and in all sectors, as well as governments, non-profits, and individuals, to more quickly build new applications and services by reducing the cost and complexity of deploying and managing IT resources. Most companies and organizations spend the vast majority of their IT budget just maintaining their current infrastructures and the applications that run on them. The cloud will enable them to devote more resources and talent to creating new products and services and improving productivity. This democratization of innovation is a huge opportunity for people, organizations, and countries around the world. To maintain its competitive position, the United States must focus on quickly and effectively harnessing the full power of cloud computing, leading in both the deployment of cloud and the development of new cloud services. This will help American companies generate high-paying jobs and compete in the global marketplace.

Recommendation 1 (Trust in the Cloud) In recent months, senior U.S. officials have described threats such as cyber crime and state-sponsored industrial espionage as outpacing many enterprise defenses. In this evolving cyber threat environment, the commission believes that cloud security services and solutions, if done correctly, may provide improved security relative to non-cloud environments.

In order to implement applicable best practices and standards around security and information assurance, the Commission supports the efforts underway on programs such as the Federal Risk and

Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP). FedRAMP is a voluntary, General Services Administration (GSA) led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The Commission believes that a well-defined FedRAMP framework will help accelerate the adoption of cloud in the Federal government. The NIST SCAP is a standard that enables the automation of reporting and verifying IT security control parameters. SCAP provides a ready method to capture, test and continuously monitor the controls and integrity settings required to achieve the respective standard and/or compliance requirements. Security metrics efforts should build upon industry and academia initiatives already chartered to address standard cloud performance measurement frameworks. As the cloud is deployed by federal agencies and businesses in multiple sectors, cloud-related security issues will become an important element of the overall security discussion for those communities. The Commission therefore recommends that cloud expertise be integrated into existing information-sharing structures, such as the Information Sharing and Analysis Centers (ISACs) and the Sector Coordinating Councils.

Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites. Mechanisms to provide identity, authentication, and attribution in cyberspace are essential to accelerating adoption of cloud computing services and improving trust in the cloud. (For example, identity management facilitates access verification, billing, law enforcement access, and other features and capabilities.) Two characteristics of a robust identity management ecosystem are (1) enabling higher level transactions to occur electronically and (2) enabling credentials to be utilized across multiple services and websites. In addition to supporting the development of a private sector-led identity management ecosystem, the commission also suggests specific steps that the federal government could take as a user of cloud services that would contribute to advancing robust identity management: Deploy, as appropriate, multi-factor authentication for federal cloud applications as used by federal personnel and government contractors doing government contract work. And accelerate the adoption of strong authentication, including multi-factor authentication and one time passwords, to enable mobile access to secure federal cloud services and websites.

Recommendation 3: The Commission recommends a national data breach law to streamline notifications and make it simple for customers to understand their rights with regard to notification. Such a law should include preemption of state laws to provide for harmonization. In addition, the law should take into account the various types of entities that are involved in processing the covered data cloud service providers, industry, government, nonprofit organizations, academic organizations, etc., and specifically provide that notice should be given by the entity that has a direct relationship with the parties whose information was subject to the breach. Finally, the law should have notification requirements based on risk of harm. Note that the motivation for such legislation is not limited to cloud computing, but adoption of cloud computing would benefit from this action. Specifically, by clarifying responsibilities and commitments around notification, the law will enable cloud providers to prepare to take expected steps in case of a breach and enable customers to trust the providers to do so. As a complement to the above recommendations, the U.S. government should update and strengthen criminal laws against those who attack our cyber infrastructure, including cloud computing services. In addition to clarifying cyber criminal offenses and defining penalties, the Federal government must commit adequate resources and personnel to investigating and tracking down cyber criminals. As much of cyber crime is transnational, the federal government should promote further international cooperation around cross-border prosecutions and identifying countries affording safe havens to such criminals.

Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda. The Commission recommends that government, industry, and academia take responsibility for developing and carrying out a research agenda that will promote U.S. leadership in the cloud by enabling innovation that benefits customers and service providers. Relevant cloud-oriented research areas include, but are not limited to, usability, privacy, availability, integrity, confidentiality, security, cryptography, identity management, energy efficiency, resource allocation, portability, and dependability. Government research agencies, like the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA), should fund universities and other organizations to conduct long range research activities, including those that build educational and research capacity and high risk, high-reward projects. Cooperative cloud test beds will also be a critical element in advancing the overall evolution of cloud technologies.

Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks. The Commission recommends that the U.S. build upon the work of existing, accepted privacy and data protection principles-based frameworks such as the Organization for economic Cooperation and Development (OECD) and/or Asia-Pacific Economic Cooperation (APEC) to develop and promote a comprehensive, technology-neutral privacy framework. The existing U.S. laws are sector specific and state specific, and this approach is different than those in other regions (e.g., Europe). In some quarters, there is a concern that this may impede the transnational flow of data with other countries, especially those in Europe. These actions would help provide the certainty and flexibility required for continued cloud innovation and would be a step toward fostering a global market for cloud services. Industry should embrace such frameworks and utilize them to the fullest extent practicable.

Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud. The Commission recommends that the U.S. modernize legislation governing law enforcement access to digital information in light of advances in IT in general and the cloud in particular. Reform of the Electronic Communications Privacy Act (ECPA) is critical to clarifying the legal conditions under which U.S. cloud providers and their customers will operate, as technology changes have overtaken many aspects of ECPA as originally written. Various groups such as the Digital Due Process Coalition have proposed making government access to data stored in the cloud consistent with government access to data stored in in-house IT systems. The U.S. Department of Commerce should conduct a study to assess the impact of the USA PATRIOT Act and similar national security laws in other countries on a company’s ability to deploy cloud in a global marketplace. This action may provide insights into how best to address the uncertainty and confusion caused by national security statutes (e.g., PATRIOT Act) and similar laws of other nations) that are perceived as impediments to a global market place for cloud services.

Recommendation 7: Critical to improving trust in the cloud and accelerating adoption is the need for best practices in collecting forensic data and information in ways that do not result in significant, adverse impacts on individuals and/or organizations using the cloud-based information. To address this, the Commission recommends that the Federal CIO work with applicable agencies such as the U.S. Department of Justice and other relevant organizations to establish best practices specifically addressing acceptable methods for collecting forensic evidence from organizations using cloud-based information systems. In addition, cloud providers should assist their customers (e.g., individuals, commercial entities, government) with technologies to facilitate ediscovery and information retrieval requirements, whether in support of regulatory compliance or litigation activities.

Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads. This recommendation highlights the role of the U.S. government both as a customer of cloud services and as a leader in enabling trustworthy use of the cloud. Government agencies, in evaluating potential models for using the cloud, should not assume or default to the notion that no government workload and/or task is suitable for cloud computing environments in other countries. Instead, they should carefully consider the types of data and tasks within their information and communications technology portfolios to match suitable workloads to the cloud computing models that achieve the required level of confidentiality, integrity, and availability at the appropriate levels of efficiency, cost, and redundancy.

Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use. The Commission recognizes the need for information and tools that provide users with meaningful ways to evaluate the characteristics and performance of various cloud implementations, whether they are contemplating deployment or evaluating performance of their current services. Development of metrics around key cloud attributes should be driven by user needs and provider capabilities. The government and commercial sector should collaborate on lessons learned, and each should be careful to avoid dominating the development of these metrics. Different government and business sectors will likely demand different measures and tools.

Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices. One benefit of the cloud is its ability to store and process large quantities of data. For customers making the transition to cloud, this often raises questions about how they access or move that data, especially in cases where they are switching between cloud providers. Data portability can be achieved in a variety of ways, and cloud providers should be transparent about their conformance with industry standards and best practices as well as the documents, tools, and relevant third-party solutions they make available to their customers. Customers should recognize that early consideration of data portability in selecting and implementing cloud services can reduce the risk of vendor lock-in. A collection of data portability standards, formats, and practices is vital to encouraging widespread cloud adoption. Government and industry should collaborate on facilitating the rapid development and dissemination of these standards and other relevant tools. The collaboration between NIST and the private sector in preparing the NIST standards roadmap under the Federal Cloud Computing Strategy is an excellent example of these types of efforts.

Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions. In interviews with senior government officials, the Commission found that the current Federal Acquisition Regulation (FAR) does not need alteration for agencies to acquire cloud services. The FAR is already flexible enough to allow agencies to acquire IT as a service. However, agencies should demonstrate flexibility in adapting current procurement models and existing contracts to take advantage of new cloud offerings. One of the biggest challenges agencies may face in budgeting is predicting the costs of cloud computing over the course of a fiscal year. Cloud computing is designed to scale quickly to a customer's needs, providing maximum flexibility to the user. If the cloud service is based on a predictable subscription model (such as a standard monthly fee per user), these budget projections can be easily accommodated. If the cloud service is based on pay-as-you-go usage, however, it can be difficult to predict costs unless the user can precisely forecast future computing needs. To address this challenge, the Commission recommends that the current efforts to update and streamline the OMB 300 exhibit form and associated budget scoring include tools that facilitate and encourage the new business models associated with cloud. OMB and Congress should communicate to agencies that it recognizes budgeting for cloud is not like budgeting for traditional IT services and should assure agencies it will provide support and flexibility during and after the transition to the cloud. To help agencies acquire cloud services, the Commission also recommends Congress and OMB demonstrate flexibility in changing budget models. Government must find ways to provide more flexibility for agencies to reduce and transition funds in the capital expenditure accounts to the operations and maintenance expenditure accounts as part of implementing innovative cloud solutions and achieving savings. In making decisions about budgeting and acquisition, federal agencies, through the CIO Council, would benefit from sharing best practices, tools for objective analysis of cloud performance, and ways to predict and document different contributors to the budgetary impact of switching to the cloud.

Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments. Adopting a new technology can be difficult, and the transition of agencies to the cloud will require investment of time, resources, and political will by the federal government. In recognition of this, the Commission recommends that OMB establish incentives and provide support for agencies beginning cloud adoption.

One possible incentive is to allow agencies to retain and redirect a portion of the overall budget savings realized from cloud adoption. Another approach is to provide seed money to agencies that help with the initial investments required in moving to the cloud.

Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services. The Commission recommends that the federal government and industry continue to expand deployment of high bandwidth networking, enhance network resilience, and advance IPv6 adoption to ensure ample broadband connections. Efforts such as those advocated in the Federal Communications Commission's National Broadband Plan, including making additional spectrum available and expanding opportunities for opportunistic and unlicensed spectrum use, are necessary to allow cloud computing to function effectively and for businesses and citizens to realize the benefits of innovative new cloud technologies. With rapidly rising demands for connectivity, the last batch of IPv4 addresses, assigned earlier this year, is unlikely to meet demand beyond the end of 2011. Since cloud computing depends on the connection of many individuals, devices, and locations, a quick transition to IPv6 is vital to ensuring the successful adoption and operation of cloud computing in the future.

Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services. The Commission commends GSA's outreach efforts to federal agencies to provide materials, expertise, and support around investigating, procuring, and deploying cloud solutions. GSA could build on this work by creating a cloud educational portal to help agency buyers, architects, administrators, and end users in understanding all aspects of cloud computing. Government, using existing programs in technology education and workforce training,4 can facilitate and encourage academic institutions and educational organizations to develop and offer courses relevant to cloud, in partnership with industry.

In a time when the government is seeking to do more with less and the commercial sector is being called upon to create jobs and grow the economy, now is the time to act on the cloud. Cloud computing has ushered in vast improvements in the cost, agility and efficiency of computing. These benefits alone drive a strong business case; however, the more compelling return is the opportunity to leap forward; to discover new markets and improve how we interact with, serve, and support U.S. citizens, users and other nations. The cloud holds the potential to unlock widespread entrepreneurism of all shapes and sizes, and expand the scope to do entirely new things — innovations such as social networking, which we could not fully imagine just a decade ago, would not exist without IT's continued evolution to the cloud.

It is the hope of the Commission that the federal government, industry and academia will implement these recommendations and be leaders in shaping how the future unfolds through the adoption of the cloud across the United States and around the world. Furthermore, these recommendations should demonstrate that cloud computing is not a new technology that needs further validation or analysis before it can be safely adopted; it is a natural evolution in computing. Those who recognize this and take early advantage of the benefits it offers will, in the coming decades, be the leaders not in only IT but in driving the cloud's evolution, and therefore, in driving business and mission results.