Written Testimony of
Nick Combs
"The Next IT Revolution? Assessing the Opportunities and Challenges of Cloud Computing"
Before
Committee on Science, Space, and Technology
Subcommittee on Technology and Innovation
September 21, 2011

Chairman Quayle and other distinguished Members of the Subcommittee, thank you for the invitation to address both the opportunities and challenges associated with cloud computing.

My name is Nick Combs and I am the Chief Technology Officer for EMC Corporation's Federal Division. EMC is one of the world's leading information technology companies and a global leader in enabling businesses and service providers to transform their operations and deliver IT as a service. Fundamental to this transformation is the topic of today's hearing -- cloud computing. Through innovative products and services, EMC and its more than 50,000 employees around the world are accelerating the journey to cloud computing, helping IT departments to store, manage, protect and analyze their most valuable asset — information — in a more agile, trusted and cost-efficient way.

Prior to joining EMC, I served for more than 25 years in the federal government, including senior government positions as the Deputy Chief for Enterprise IT Solutions at the Defense Intelligence Agency, where I was responsible for the engineering and program management of all activities in the Department of Defense Intelligence Information Systems (DoDIIS) environment. I also served as the IT Director and Chief Information Officer of the National Media Exploitation Center (NMEC) under the Office of the Director of National Intelligence. Over the course of my career in government and the IT industry, I have experienced many of the IT challenges facing organizations today, particularly as enterprises transition to cloud services.

As an industry leader on cloud computing, EMC teamed with Cisco (along with investments from VMware and Intel) to start VCE or the Virtual Computing Environment company. VCE represents an unprecedented level of collaboration in development, services, and partner enablement that reduces risk in emerging cloud infrastructures in both the public and private sector. We will all hear more from VCE's Michael Capellas at today's hearing in his role as Co-Chairman of the TechAmerica Foundation Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (Cloud2 Commission).

EMC also has a seasoned Technical Advisory Board to help shape the strategic vision of private and hybrid clouds and beyond. This Board, comprised of recognized industry experts from business and academia, focuses on long-term technology strategy, industry trends, and advanced development opportunities and initiatives. Members were

selected for their expertise and thought leadership in such key areas as server, networking, storage, virtualization, cloud computing, data structures, information security, application middleware, and technical computing.

For today's testimony, I was asked by the Subcommittee to discuss some of the major cyber security challenges facing both cloud service providers and adopters.

During the past couple of years, the frequency, volume and impact of cyber attacks has reached pandemic levels. These attacks are resulting in real economic harm as well as posing very significant national security challenges. Because the Internet is used by everyone, everywhere, and by large, small, government and commercial organizations, there are multiple avenues for exploitation. The targets of more advanced cyber attacks now include organizations as diverse as pharmaceutical and automotive companies to oil and gas firms and the defense industrial base and government agencies; and yes, even information security companies.

As you may know, RSA, the Security Division of EMC, publicly disclosed on March 17, 2011, that it had detected a sophisticated cyber attack on its systems. The attack on RSA was a stark reminder for us – and for the entire information security community – that no one is immune from cyber attacks. The attack also reflects the sophistication of advanced attackers in understanding the interconnections and interdependencies organizations have in our networked world and how to exploit those relationships to achieve their goals.

And this brings us to cloud computing, which is fundamentally changing the way that organizations think about and implement IT. As the Cloud2 Commission pointed out in its recent report, cloud computing is really based on a simple idea: "By allowing [IT] users to tap into servers and storage systems scattered around the country and around the world – and tied together by the Internet – cloud service providers can give users better, more reliable, more affordable, and more flexible access to the IT infrastructure they need to run their businesses, organize their personal lives, or obtain services ranging from entertainment to education, e-government, and healthcare."

We agree and this shift brings new efficiencies, cost savings, and helps organizations gain more productivity from their IT systems. We also believe that the adoption of cloud computing will help improve cyber security over the long-term. While ensuring "trust in the cloud" is critical to spurring cloud adoption, there should be tangible improvements in security that come with the shift to the cloud that is underway.

In the next several years, cloud computing adoption could enable organizations to improve information security by replacing the disparate and legacy IT systems that are so common today. Instead of having our IT and information security organizations protecting stove-piped systems, organizations are able to implement centralized monitoring, management and security solutions. In addition, security is being built into the information infrastructure that makes up the foundation for cloud computing including virtualization and data storage platforms. Cloud computing also holds special

promise for smaller organizations which, left to their own devices, cannot always afford the advanced expertise or technologies necessary for protection against today's threats. Those organizations, by consuming IT services from cloud providers, can gain the benefits of advanced security in affordable ways, with the costs spread over hundreds or even thousands of cloud customers.

I will discuss managing risk and building trust in the cloud in more later in my testimony, but before I do that I would like to provide more information about cloud computing, the benefits of cloud, and our thoughts on the current federal strategy for cloud computing.

First, I would like to comment on the term "cloud computing" and its definition. It is a term that is becoming widely used and is all around us in TV commercials and newspapers and magazines. Cloud has become one of the most common yet most misunderstood references to information technology and services. In fact, I would venture that many of us in the room have family members that are heavy cloud computing users -- without them even knowing it – whether through social media networks, Internet retailing or via the advanced capabilities of smartphones. Cloud computing is increasingly the infrastructure consumer-facing applications are built on.

Given this understanding of cloud computing, I will address the various approaches to implementing the underlying infrastructure that facilitates cloud based solutions. Confusion in the marketplace generally arises from discussion of different approaches to cloud deployment, that is to say discussions of Private, Community, Public, or Hybrid Clouds. The National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce has provided definitions of these delivery models that help provide more clarity:

- ***Private Cloud.*** *The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and exist on premise or off premise.*
- ***Community Cloud.*** *The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or by a third party on premise or off premise.*
- ***Public cloud.*** *The cloud infrastructure is made available to the general public or a large industry group and is owned and operated 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 that are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds.)*[1]

[1] "The NIST Definition of Cloud Computing (Draft)" by Peter Mell and Tim Grance, Special Publication 800-145 (Draft), January 2011.

The customers that we serve on a daily basis collectively deploy all of these types of cloud computing models. EMC and its subsidiary companies deploy solutions and services via private, community, hybrid and public clouds. As an enterprise, EMC has utilized its solutions, as well as virtualization technology from VMware – the foundation of cloud infrastructure – as our IT organization leverages private clouds internally, reducing our own IT costs and energy bills.

In the first phase of EMC's internal shift to a cloud-based infrastructure, our company gained $74 Million in data center equipment savings, $12 Million in power and space savings and a 34 percent increase in energy efficiency. This was just the initial savings for the company; cost savings is one of the reasons why so many organizations in both the public and private sector are moving to cloud computing. And, in both industry and government, we are seeing data center consolidation move forward – with the associated cost savings – in tandem with organizations' transition to cloud infrastructure and services.

On July 20, 2011, the White House announced plans to shut down 373 data centers within the federal government by the end of 2012 as part of the President's goal of closing 800 data centers by 2015, a move that is projected to save more than $3 billion.[2]

EMC has been enabling customers to further their virtual datacenters and embrace cloud computing through the solutions and services it offers. Some examples of the benefits of Cloud computing reflecting various segments of the U.S. economy include:

- Oregon-based Columbia Sportswear, a leading innovator in active outdoor apparel, footwear, accessories and equipment has increased the performance of its IT infrastructure using 25 percent less space after implementing a cloud computing model. At 95 percent virtualized, Columbia has reduced its storage total cost of ownership by 40 percent while enabling 50 percent more virtual machines to be supported in the infrastructure.

- Texas-based Lone Star College System, the fastest-growing community college system in Texas has deployed a private cloud to deliver IT-as-a-Service to over 90,000 faculty, staff and students at more than a dozen locations. In moving to a cloud model, Lone Star has saved more than $600,000 in capital expenditures by utilizing virtualization and consolidating its IT environment. At 90 percent virtualized, Lone Star has reduced its energy consumption by 66 percent while increasing its ability to deliver new IT services in less than a week compared to three to four months before moving to the cloud.

[2] "White House Announces Plans to Shut Down Hundreds of Duplicative Data Centers as Part of Campaign to Cut Waste", White House Press Release, Office of the Press Secretary, July 20, 2011.

- Independent Bank, a Michigan-based bank, has also achieved many benefits from moving to a cloud environment. At 70 percent virtualized, the bank has eliminated 65 servers and avoided additional server expenditures even as its environment expands. All the while, Independent Bank has reduced the time to deploy servers from at least a day to just 1-2 hours. In addition, the bank has seen server-related power consumption dramatically reduced. When it comes to backup, Independent Bank has also reduced its backup storage capacity requirements while decreasing the time to recover data of critical systems from days to just a few hours and even minutes.

The Benefits of Cloud Computing

Cloud computing provides the characteristics that organizations need by enabling IT infrastructures to be flexible, on-demand, efficient, and resilient. In short – it allows them to be more agile. For the most part, IT systems have been built the same way for the last 40 years and it is clearly time for a change – we need more efficiency, agility, productivity, and security from our information infrastructure – with better return on investment than today's more rigid and less efficient approaches. We can no longer afford to maintain legacy and stove-piped, monolithic systems in which each computing requirement has its own dedicated IT system.

To achieve this level of IT transformation and implement technology to make it possible to run IT as a service, organizations have attempted to utilize Service Oriented Architectures (SOA) to bring these disparate IT systems together, but have struggled due to the lack of interoperability standards in designing IT systems. Cloud computing, based on open systems architectures and aligned to evolving cloud standards, can provide the foundation for future interoperable systems.

These new environments can dramatically reduce the largest costs associated with IT systems, particularly those related to operations and maintenance. According to the analyst firm Forrester, more than 70 percent of organizations' IT budgets are dedicated to just keeping the lights on and only 30 percent of budgets are available to bring new capabilities to the organization. Gartner predicts that by 2014, cloud-computing experience will be a listed or demanded skill in most hiring decisions for IT projects and believe that by 2015, 50 percent of Global 1000 enterprises will rely on external cloud-computing services for the top 10 revenue-generating processes.

The federal government has spent billions of dollars for computers to create and process information, internal networks to move that information around, and hardware to store it. And don't forget about the ever-changing application software for those internal processes and accounting. We are at a point where government agencies are spending a majority of their IT budgets just to maintain their current systems and infrastructure. During my service in the federal government, I saw some government organizations with operating and management costs as high as 85 percent of their overall IT budget. Cloud

computing offers a means through which to address this imbalance in how taxpayer funds are spent.

Through the cloud, organizations can centrally manage their IT systems and provide uniform policy implementation. They will reduce their operating and management costs, thus freeing up resources to address other needs. For example, money previously devoted to simply maintaining the infrastructure could be used to increase an organization's security posture.

In short, as the Cloud2 Commission noted in its report: "Cloud technologies are transforming the way computing power is bought, sold, and delivered.

...This new business model brings vast efficiency and cost advantages to government agencies, individuals, and companies of all sizes." We firmly believe that at EMC and that's a fundamental reason why we think U.S. federal agencies should be adopting cloud computing just as aggressively as we are in the private sector.

Federal Strategy for Cloud Computing

EMC supports the Administration's "Cloud First" strategy and along with the ongoing federal data center consolidation efforts, we believe that these policies, if fully implemented, will save the federal government billions of dollars in IT budgets annually. In this area of sky-rocketing budget deficits and new budget caps, now is the time for federal agencies to accelerate their adoption of cloud infrastructure and services. As I mentioned earlier, in addition to the cost savings, the increases in energy efficiency and productivity, moving IT systems to cloud-based infrastructure and services, could also help improve cyber security.

We understand that the transition to cloud computing will not occur overnight; rather it requires a journey to realize all the benefits the cloud has to offer. The federal government has many unique environments, but these diverse organizations can benefit greatly from the successes that commercial organizations have already achieved through the adoption of cloud computing. The economies of scale, flexibility, and efficiencies of these cloud infrastructures will not only save significant amounts of capital and maintenance costs, but enable the application and use of information across our enterprises as never before.

One can only imagine all the ways in which information technology could be applied in the government if federal IT professionals were freed from the burdensome task of managing today's complex and sometimes antiquated infrastructures. Former OMB Director Orszag made a similar point last year when he highlighted the reality that government organizations are unable to match the productivity and innovation of the private sector because of archaic and complicated computing infrastructure. [3] Cloud computing provides a mechanism to address this technology gap, enabling the federal government to unleash new innovations and improve productivity.

[3] Remarks by Peter Orszag, Center for American Progress, June 8, 2010, Washington, DC.

Many federal organizations have already begun to build a bridge to the cloud by adopting some form of virtualization. Virtualization enables the shared use of a physical hardware resource – a simple example is a PC that is able to run multiple operating systems thanks to virtualization software. In fact, virtualization has become the foundation of the cloud and in our view is the great enabler of cloud services across the various deployment models. Cloud computing is virtualization taken to its most logical extreme, creating the ultimate in flexibility and efficiency, and revolutionizing the way we compute, network, store, and manage information

In fact, EMC recently announced breakthrough capabilities that enable virtual storage over distance. The industry's first distributed storage federation provides unprecedented business agility by eliminating the current boundaries of physical storage. For example, the workload and information in an entire data center in the path of an approaching hurricane could be simply shifted to another one hundreds or thousands of miles away with no disruption in service and then shifted back just as easily once the storm passes. This is a key enabler to future cloud architectures.

Trust in the Cloud

Cyber security is clearly one of biggest concerns of federal CIOs who are considering implementing cloud infrastructure and services. When I speak to customers about their journey to the cloud, they consistently bring up cyber security and data privacy issues as possible barriers to adoption. According to an April 2010 Lockheed Martin Cyber Security Alliance survey of U.S. federal government, defense, and intelligence agency decision makers, respondents were most concerned by data security, privacy and integrity in the cloud. [4] In addition, 46 percent of respondents to the Ponemon Institute's November 2009 "Cyber Security Mega Trends" survey of IT leaders in the U.S. federal government indicated that cloud computing increases security risk within their organization.[5] The biggest security concern noted by Ponemon survey respondents (30 percent) was the inability to protect sensitive or confidential information and the second most significant concern (20 percent) was to restrict or limit the use of computing resources or applications.

Technologies and effective best practices exist today to deliver private cloud environments inside federal organizations to gain dramatic improvements in IT efficiency, while also providing the security required to protect sensitive information within the government enterprise.

A hybrid cloud is a result of combining a public cloud with a private cloud. Building a hybrid cloud requires new technology, new processes and trusted partners. One of the biggest benefits for hybrid clouds is the notion of "bursting". Bursting allows IT organizations to build their infrastructure for median capacity and rent additional

[4] "Awareness, Trust and Security to Shape Cloud Adoption," a survey commissioned by the Lockheed Martin Cyber Security Alliance and conducted by Market Connnections, Inc., April 2010

[5] "Cyber Security Mega Trends: Study of IT leaders in the U.S. federal government", Independently conducted by Ponemon Institute LLC; Publication Date: November 18, 2009.

infrastructure from a public cloud when needed. This can dramatically reduce capital expenditures and reduce operational expenditures to a lesser degree.

Even if organizations aren't ready to do this today, they need to be building their private cloud so that this option is available when the organization and process is ready. To do this, you need an infrastructure that allows you to move and entire workload online between clouds. This requires movement of the application and the data across distance.

Second, you need a trusted service provider where you can run your workloads in the public cloud. That service provider must have compatible infrastructure to enable online movement as outlined above. The service provider must also deliver the security and controls you demand along with visibility for you to ensure compliance.

With the adoption of cloud computing infrastructure and services comes sophisticated automation, provisioning and virtualization technologies that have significant security implications, so we must look at security in a whole new way. Establishing trust first requires control and a second level of internal visibility that can be stepped up or expanded for external service providers. However, if control plus visibility is the formula for trust, how do we go about solving for it?

Solving for trust in internal (private) clouds is less challenging than in public clouds because in an internal cloud, the organization controls all IT assets, as well as the geographic location of its data. Control and visibility in internal clouds is about adapting existing processes to the virtual environment while capitalizing on the new advantages of virtualization. This is particularly the case for mission critical functions.

Mission-critical functions require control and visibility into the cloud's performance. They also require additional precautions to ensure that information in the cloud is protected against loss or system unavailability, from external or internal threats, and from data breaches. Only this heightened level of control and visibility can deliver the critical proof that leads to trust:

- Proof that cloud infrastructure meets security specifications and that information is managed in accordance with policies;
- Proof that authorized users are who they say they are; and
- Proof of performance and compliance to satisfy internal management as well as auditors and regulators.

Essential to proof is the ability to inspect and monitor actual conditions first-hand and not just rely on outside attestations, especially for applications handling regulated information or other sensitive workloads. Organizations need transparency into service providers' environments to ensure compliance with policies and Security Level Agreements (SLAs). They need an integrated view of their IT environments, both internal and external, to correlate risks, spot threats, and to coordinate the implementation of countermeasures.

Today, organizations struggle to have control and visibility in their physical IT environments. This challenge need not be exacerbated in the cloud. The good news is that virtualization technology creates the right conditions for organizations to improve control and visibility beyond what's available in today's physical environments.

With virtualization and cloud computing, applications have become completely disassociated from the IT infrastructure on which they run. It provides the flexibility to have the same application run in the datacenter next door on one day, in a centralized datacenter hundreds of miles away the following day, and in a service provider datacenter another day. For that reason, improving information security cannot solely rely on the controls of the IT infrastructure such as the network perimeter. Security must evolve to become much more centered on the users and on the information they are accessing. For that reason, emerging technology practices, such as adaptive authentication and data loss prevention, are both widely used in the commercial world and are increasingly used in federal government agencies.

We believe that in the transformation power of virtualization – so much so that we are focusing our cloud-security strategy and development initiatives on making security and compliance in the cloud 1) logical and information-centric, 2) built-in and automated, and 3) risk-based and adaptive. For years, EMC, RSA and VMware have worked to embed security, management and compliance controls into the virtualization platform.

While perimeter and point security products will still be used by organizations, companies such as EMC and VMware are embedding controls and security management in the virtual layer, creating an environment in the virtual world that is far safer than what exists in the physical. Industry must continue to develop and deliver technology components that support centralized, consistent management of security across the technology stack. Security must be dynamic and intelligent. The static, reactive environment developed in the past simply will not work. Security cannot be an after thought; it must be embedded in the fabric. It must be built into the products and infrastructure by the vendor community.

As I mentioned earlier, stronger security (control) proven through direct monitoring (visibility) is one of the key best practices for trust in the cloud.

RSA, EMC's security division, is working with cloud providers to give them the means to demonstrate security and compliance to their customers, removing this barrier to greater cloud adoption. The RSA Cloud Trust Authority, announced at the RSA Conference in March of this year, gives cloud customers an easy and scalable way to ensure trusted access to multiple cloud provider, while giving the cloud providers themselves a more automated, consistent way to demonstrate compliance with cloud standards for security and confidentiality as they evolve. Over time we expect the Cloud Trust Authority to evolve to offer additional means of security and compliance for digital information and identities.

Best practices such as risk-based authentication should also be implemented in cloud environments and we think that that approach fits well within the President's National Strategy for Trusted Identities in Cyberspace (NSTIC) which was released earlier this year. This important effort, which is being coordinated by the NSTIC Office at NIST in collaboration with the private sector, should be supported by the U.S. Congress.

When implemented correctly, cloud environments can be much more secure than today's IT environments. The level of transparency cloud vendors provide is a critical aspect when choosing a cloud partner. The federal government must take a trust-but-verify approach. Cloud vendors should be required to provide the tools and capabilities to allow customers visibility into their cloud environments to ensure compliance with those SLAs. SLAs should be clearly defined and monitored by government customers to ensure maximum service value is received for budget dollars spent. For instance, SLAs in areas of performance, availability, backup and recovery, archive, continuance of operation, and disaster recovery must be clearly stated, measured, and monitored by the government agencies. Additionally, government risk and compliance capabilities need to be deployed and dashboards provided to the customer to ensure that our information is protected and our policies are being followed.

Security must be risk-based and driven by flexible policy that is aligned to the business or mission need. The need for a common framework to ensure that security policies are consistently applied across the infrastructure is critical to success. That is one of the principle reasons that EMC supports updating the Federal Information Security and Management Act (FISMA). Enacting updated FISMA legislation that will enable continuous monitoring is essential to address today's threat environment as well as provide for an effective operational risk management framework for tomorrow's cloud computing infrastructure.

Conclusion

As I conclude my testimony, I would like to comment on the role of NIST in advancing cloud computing and trust in the cloud. Through its cloud computing workshops, NIST has already played a vital role in bringing together the public and private sector to zero in on the security, interoperability and portability challenges related to the cloud. NIST has also added clarity in its work on coming up with a comprehensive definition of cloud computing.

NIST has also played an instrumental role in the development of the 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 NIST SCAP standard enables the automation of reporting and verifying IT security controls. SCAP provides an effective method to capture, test and continuously monitor these controls.

Both of these initiatives are important steps in the transition of the Federal Government from the old FISMA focus on compliance, to better operational risk management and continuous monitoring under the new FISMA. This process is critical for improving cyber security today as well as positioning the federal government to fully utilize the transition to the cloud to help improve cyber security.

Congress should also allow federal agencies to select the cloud deployment models that best fit their business and security needs, rather than favoring one cloud model over the other.

I again thank the Committee for allowing EMC and me to contribute to the hearing today. Information technology is ushering in dramatic change with the shift to cloud computing and we have to remain focused to ensure we get it right. This will be a journey and we will realize benefits at many points along the way and it will provide organizations with much greater flexibility to meet the demanding needs of our federal government. Security is a legitimate concern, but the technology and best practices exist to address many of those risks and more innovation is happening right now as we sit here together today.

A critical part of the solution lies in engineering security into the cloud, not bolting it on as an afterthought. Ultimately, cloud computing offers great potential for commercial organizations, government agencies and many others and we should do what we can now to embrace the shift to cloud computing that is underway.

Thank you and I look forward to your questions.