WRITTEN TESTIMONY OF
NICKLOUS COMBS
CHIEF TECHNOLOGY OFFICER, EMC FEDERAL
ON "CLOUD COMPUTING: BENEFITS AND RISKS MOVING FEDERAL IT INTO THE CLOUD"

BEFORE

THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
AND
THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

JULY 1, 2010

Chairman Towns, Ranking Member Issa, Chairwoman Watson, Ranking Member Bilbray, and Members of the Committee, thank you for the opportunity to address the opportunities and risks associated with moving federal IT into the cloud.

My name is Nick Combs and I am the Chief Technology Officer for EMC Corporation's Federal Division. EMC is a global leader in cloud computing infrastructure and services. We enable the full realization of the inherent power of information by creating complete information environments that are reliable, efficient, and secure. With EMC, users and organizations can bring the power of information to life...information that illuminates what is possible and that moves the world forward. Prior to joining EMC, I served for more than 25 years in the Federal Government as a senior leader in the Army, Senior IT leader in the Defense Intelligence Agency and as an IT Director and CIO with the Director of National Intelligence. During my career in government and the IT industry, I personally experienced many of the IT the challenges facing federal agencies today, particularly as agencies transition to cloud services. In both the public and private sectors, I have worked with different types of cloud computing models, each of which had its own risk management, interoperability, and data portability requirements.

First, let me comment on the term "cloud computing" and its definition. Today, the term is one of the most common yet most misunderstood references to information technology

and services. There are a number of definitions for cloud computing. For purposes of my testimony today, I will adopt the definition of The National Institute of Standards and Technology (NIST), which defines cloud computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

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. Again, NIST has provided definitions of these delivery models that help provide more clarity:

- **Private Cloud** is infrastructure deployed and operated exclusively for an organization or enterprise. It may be managed by the organization or by a third party, either on or off premise.
- **Community Cloud** is infrastructure shared by multiple organizations with similar missions, requirements, security concerns, etc. It also may be managed by the organizations or by a third party on or off premise.
- **Public cloud** is infrastructure made available to the general public. It is owned and operated by an organization selling cloud services.
- **Hybrid cloud** is infrastructure consisting of two or more clouds (private, community, or public) that remain unique entities but that are tied together by standardized or proprietary technology that enables data and application portability.[2]

[1]: "The NIST Definition of Cloud Computing" by Peter Mell and Tim Grance, Version 15, 10/7/2009.
[2] "The NIST Definition of Cloud Computing" by Peter Mell and Tim Grance, Version 15, 10/7/2009.

The organizations represented at today's hearing collectively deploy all of these types of cloud computing models. EMC, for example, deploys solutions and services via private, community and public clouds. As an enterprise, EMC has used its solutions, as well as virtualization technology from VMware – the foundation of cloud infrastructure – as our IT organization leverages private clouds internally, reducing our IT costs and use of power resources. EMC has also been enabling customers to further their virtual datacenters and embrace cloud computing through the solutions and services it offers.

For example, through a public cloud, EMC's Mozy online backup and data recovery service provides peace of mind to over a million consumers and tens of thousands of individuals and businesses. EMC also teamed with Cisco and VMware to start the Virtual Computing Environment coalition, representing 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. Just last month EMC announced the formation of a new Technical Advisory Board to shape the strategic vision of private clouds and beyond. This Board, comprised of recognized industry experts from business and academia, will focus 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, security, application middleware, and technical computing.

The Benefits of Cloud Computing

Cloud computing provides the characteristics that every IT organization needs by enabling IT infrastructures to be flexible, on-demand, efficient, and resilient. Organizations have been building IT systems the same way for the last 40 years and it is time for a change. However, we can no longer afford to have these legacy and stove-piped, monolithic systems in which each requirement has its own IT system. 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 IDC, 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. 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 application software for those internal processes and accounting. We are at a point where government agencies are spending a majority of IT budgets just to maintain our 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 the means through which to address this imbalance.

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 the infrastructure's security posture. Cloud computing brings a level of automation to IT that dramatically reduces costs by sharing resources and frees up more resources to deliver the capabilities that organizations need.

Federal Strategy for Cloud Computing

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 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 us significant amounts of capital and maintenance costs, but enable us to apply and use 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 task of managing today's complicated and antiquated infrastructures. OMB Director Orszag made a similar point last month when he highlighted the fact 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, allowing the federal government to unleash new innovations and improve productivity.

Many federal organizations have already begun to build a bridge to the cloud by adopting some form of virtualization. In fact, virtualization has become the foundation of the cloud and in my 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. Virtualization capabilities are also evolving outside the server realm. In fact, EMC recently announced breakthrough capabilities that enable virtual storage over distance. The industry's first distributed storage federation will provide unprecedented business agility by eliminating the current boundaries of physical storage. This is a key enabler to future cloud architectures.

Cloud Security and Risk Management

Information security is by far the biggest concern of federal CIOs considering implementing cloud infrastructure and services. 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,

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

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.

Admittedly, with cloud computing come sophisticated automation, provisioning and virtualization technologies that have significant security implications, so we must look at security in a whole new way. In March of 2010, RSA the Security Division of EMC, unveiled a shared vision with Intel Corporation and VMware for building a more secure and transparent infrastructure for business-critical cloud services. 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.

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, 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,

[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.

emerging technology practices, such as adaptive authentication and data loss prevention, are both widely used in the commercial world. However, they are only beginning to be adopted in federal government organizations. Such practices must be more broadly deployed. This environment must be transparent to the enterprise and to the user. 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.

For a decade, fraudsters have been crafting malware to steal users' passwords and perform fraudulent actions on their online bank accounts. Cloud computing can increase the risk of exposing corporate assets to fraudsters and cybercriminals. The automaker's next design is worth more on the black market than online bank accounts. The same malware used to steal online banking password is also being used to steal corporate passwords. In the age of cloud computing, solely relying on passwords to protect access to cloud applications is not sufficient. Additional best practices like risk based authentication must be employed and we think that that approach will fit well within the Trusted Identity strategy that is currently being developed by the Obama Administration.

When implemented correctly, cloud environments can be much more secure than today's IT environments, which are often protected by inadequate perimeter security practices. The level of transparency cloud vendors provide is a critical aspect when choosing a cloud partner. While there is a lot of talk about Service Level Agreements (SLA) helping to satisfy federal government information security needs, this alone is inadequate. 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 dash boards

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 the success. That is one of the principle reasons that EMC supports updating the Federal Information Security and Management Act or FISMA, important legislation that will update the law to enable more operational risk management, which is essential in both today's environment and the evolving cloud computing infrastructure.

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. Multi-tenant federated clouds can be deployed where similar security requirements exist. However, placing information on a public cloud today should be limited to public facing information only and then only if the providers can provide the level of auditing and protection procedures needed to deal with breaches of sensitive information.

Conclusion

I again thank the Committee for allowing EMC and I to contribute to this very important effort. IT is on the verge of dramatic change; cloud computing has the potential to have the most significant impact on IT since the development of the microprocessor. 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. Admittedly, security is a top concern, but the technology and best practices exist to address that risk. 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 federal

information technology, and federal departments and agencies should be encouraged to embrace that potential.