Testimony of

Cita M. Furlani
Director
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

United States House of Representatives
Committee on Oversight and Government Reform

"Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"

July 1, 2010

Chairman Towns, Chairwoman Watson, and Members of the Committee, I am Cita Furlani, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce’s National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in the development and deployment of cloud computing technology.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

As one of the major research components within NIST, the ITL accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

NIST works with federal agencies, industry, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to their confidentiality, integrity and availability. NIST researches technologies such as identity management and verification, metrics for complex systems, automation of discovery and maintenance of system security configurations and status, and techniques for specification and automation of access authorization in support of many different kinds of access policies.

In addition to IT-related technology research, ITL is responsible for the development of, publishing, and providing explanatory support for Federal standards, guidelines, and best practices related to cybersecurity.

NIST’s role in cloud computing is to promote the effective and secure use of the technology within government by providing technical guidance and promoting standards. The three cybersecurity objectives, ensuring the confidentiality, integrity, and availability of information technology systems, are particularly relevant as these are the high priority concerns and perceived risks related to cloud computing.

Although the power of modern cloud computing systems is new, the ideas behind cloud computing reach back through decades. In the early 1960s, researchers proposed the idea of computing as a utility, similar to other services such as gas or electricity. Around the same time, techniques to make a single computer appear to be many separate “virtual” computers were developed and implemented on mainframe computers. Some of the building blocks for cloud computing were in place, but performance and costs were barriers, and networking was inadequate. Years of hardware advances were needed to close the gap. By the 1990s, the Internet had made grid computing possible: many computers working together on a single problem over a network. By the 2000s, the term cloud computing was being used to describe computing services delivered over a network, and, in 2010, a substantial and growing number of vendors are developing cloud computing offerings for government, industry, and the general public.

Before discussing ongoing NIST efforts which are directed toward promoting secure and effective use of cloud computing, I refer to the widely-cited NIST definition of cloud computing[1]. Computer scientists at NIST developed this definition in collaboration with industry, academia and government and we expect it to evolve over time as the cloud industry and cloud technology matures:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*.*

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

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

- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

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

[1] The NIST Definition of Cloud Computing, Version 15, Peter Mell and Tim Grance, October 7, 2009.

- *Measured Service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

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

- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

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

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

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

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

  Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

This NIST cloud computing definition, most recently revised in October 2009, has been broadly recognized and helps to clarify a complex emerging information technology paradigm. However, there is still much work to be done.

NIST has initiated focused activities to develop federal cloud computing security guidance as well as to facilitate the development of cloud computing standards. Both are essential and must be considered in parallel in order to effectively support the secure implementation of cloud computing technology. NIST efforts respond not only to high priority security requirements, but to interoperability and portability requirements, which are interrelated with and essential to effectively address cloud computing security.

Following are specific NIST efforts which promote the effective and secure use of cloud computing technology within government by providing technical guidance and promoting the development of standards.

NIST recently held a Cloud Computing Forum and Workshop.   The goal was to engage with stakeholders on ways to accelerate the federal government's secure adoption of cloud computing. Over 500 stakeholders registered for the event – which included representatives from industry, federal government, state governments, academia, and standards development organizations.

NIST is developing a cloud computing Special Publication which will use the definition of cloud computing as a frame of reference to organize and present analysis, recommendations and guidance. The document will provide insight into the technical benefits, risks, and considerations related to the secure and effective uses of cloud computing and guidance in the context of cloud computing: interoperability, portability, and security. The publication will also outline typical terms of use for cloud systems and will identify future research areas in cloud computing as well as recommendations. NIST will develop additional cloud computing Special Publications as research and analysis are completed.

As requested by OMB, NIST serves as the government lead, working with other government agencies, industry, academia, and standards development organizations to leverage appropriate existing standards and to accelerate the development of cloud computing standards where gaps exist. The expectation is that standards will shorten the adoption cycle, support cost savings and the ability to more quickly create and deploy enterprise applications.

Under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU). NIST leads national and international consensus standards activities in cryptography, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing – all essential for secure cloud computing implementation.

NIST has initiated the Standards Acceleration to Jumpstart Cloud Computing (SAJACC) project. The SAJAAC goal is to facilitate the development of cloud computing standards. The analysis and results completed under SAJACC will be used to inform the cloud computing Special Publications described above. SAJACC refers to a strategy, a process, and a portal.

SAJACC was initiated to address a widely acknowledged need in the development and implementation of new complex technologies. Historically, a gap has existed between the time when standards are needed and the time when they become formalized. Complex standards such as the Portable Operating System Interface [for Unix] and current Internet standards have taken years to develop. This has occurred because the development of standards is dependent on the inherently time consuming process of broad participation and consensus building, is driven by technical innovation, and requires due diligence in order to produce a standard of quality and completeness such that it will be effective and broadly adopted.

The SAJAAC strategy is two-fold: 1) to accelerate the development of high-quality standards and 2) to reduce technical uncertainty during the interim adoption period before many cloud computing standards are formalized.

The heart of the SAJACC concept is the process of identifying and validating interim candidate interface specifications by testing against requirements which demonstrate portability, interoperability, and security for users of cloud systems. SAJACC is applying the use case development method to define, refine, and interpret requirements in the form of behavioral scenarios which describe the interaction between people and computer systems. The project is currently formulating an initial set of twenty five use cases, and vetting these with cloud computing stakeholders in academia, government, and industry.   After the use cases have been refined, they will be made available through a public website. In order to verify and demonstrate the test plan and execution process, NIST will conduct an initial set of validation tests against an initial set of legacy interfaces, and publish the results as an example of how future collaborative efforts could be accomplished.

Information exchange and visibility will be accomplished through a SAJACC website. This portal is planned as a public Internet-accessible repository of cloud computing use cases, documented cloud system interfaces (i.e., specifications which have not yet evolved to become formal standards), pointers to cloud system reference implementations (i.e., cloud computing systems where these specifications were incorporated as part of the implementation), and test results which show the extent to which different interfaces can support individual use cases (i.e., satisfy security, portability, and interoperability requirements.)

SAJACC by definition leverages, coordinates, and is heavily dependent on contributions from external stakeholders with an interest in cloud computing standards. The process of identifying new interfaces (with corresponding reference implementations) and new use cases will be ongoing.

NIST has developed standards to support federal agencies' information security requirements for many years, beginning in the early 1970s with enactment of the Brooks Act. Through the Federal Information Security Management Act (FISMA), Congress again reaffirmed NIST's leadership role in developing standards for cyber security. FISMA provides for the development and promulgation of Federal Information Processing Standards (FIPS) that are "compulsory and binding" for Federal computer systems. The responsibility for the development of FIPS rests with NIST, and the authority to promulgate mandatory FIPS is given to the Secretary of Commerce. Section 303 of FISMA states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

These activities include, for systems other than national security systems, standards and guidelines that must include, at a minimum (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

NIST addresses cyber security challenges, which are directly applicable to cloud computing throughout the information and communications infrastructure, through its cross-community engagements. NIST employs collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia to take advantages of technical and operational insights and to leverage the resources of a global community. NIST is responsible for establishing and updating, on a recurring basis, the federal government's risk management framework, cybersecurity controls, and assessment procedures to determine control effectiveness. NIST engages government and industry to harmonize information security requirements to align with industry business models and best practices.

An example is the release of Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* in August 2009 which was developed by the Joint Task Force Transformation Initiative consisting of members from NIST, the Department of Defense, Office of the Director of National Intelligence, and the Committee on National Security Systems. This unified set of security controls provides a standardized method for expressing security at all levels, from system development and acquisition to operational implementation. This allows for an environment of information sharing and interconnections among these communities and significantly reduces costs, time, and resources needed to secure information systems.

In close collaboration with the Department of Defense, the Committee on National Security Systems and the Intelligence Community, NIST revised its Certification and Accreditation (C&A) guideline, Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* to fundamentally change the focus of the information system authorization process from a static (a point in time) approach to a continuous monitoring approach. This continuous monitoring approach, implemented with automated tools whenever possible, will provide authorizing officials and senior leaders within federal agencies with critical and timely information on the ongoing security state of their information systems, thus allowing them to make more informed, risk-based decisions when authorizing federal information systems for operation.

The current version of Special Publication 800-37 was also updated to allow certification and accreditation efforts to be leveraged among federal agencies. This is an important building block needed to support government adoption of cloud computing.

In 2009 and 2010, NIST, in a technical advisory role, supported the interagency Federal Cloud Computing Advisory Council (CCAC) Security Working Group in the development of a concept for a federal approach to coordinate and apply consistent security authorization requirements for cloud computing systems.

The overall approach is being defined under the governance and implementation auspices of the Federal CIO Council. The NIST role is to provide guidance for a technical approach and process which is consistent with NIST security guidance in the context of FISMA. More specifically, NIST is supporting the definition of a technical process in the context of and to be consistent with Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, referenced earlier.

Cybersecurity is a vital, central mission of our laboratory and is a key concern and risk factor related to cloud computing adoption. In a public cloud computing deployment model the customer generally does not have control or knowledge over the exact location of the provided resources such as storage, processing, memory, network bandwidth, and virtual machines.

NIST recognizes that effective cybersecurity guidance is holistic and must be considered in the context of broad and comprehensive information security guidance for federal agencies as well as the interoperability, portability and security technical standards development efforts described previously. The NIST cloud computing security guidance recognizes the need to consider the security requirements of the foundation technologies which are applied to implement cloud computing and to leverage the existing computer security capabilities and knowledge base.

NIST will continue to conduct the research necessary to enable and to provide cloud computing and cybersecurity specifications, standards, assurance processes, guidance and technical expertise needed for effective and secure U.S. government and critical infrastructure information systems.

NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cyber security research, standards development, standards conformance demonstration, and cyber security education and outreach activities.

NIST has initiated a strategic Virtualization Laboratory effort to research and evaluate the security of virtualization techniques and the cloud computing systems that employ them. The lab will serve as a resource for the development of ideas to mitigate security vulnerabilities in virtualized and cloud systems, and to gain hands-on experience that will inform NIST cloud and virtualizations guidelines. The lab plans include two research tasks. The first is to conduct research on the integration of advanced access control mechanisms into virtualized systems. The second task is to conduct research of metrics to evaluate hypervisor security vulnerability and quality. This task will conduct a study of hypervisor architectural principles and will measure the complexity of hypervisor implementations.

NIST has also initiated the Modeling and Analyzing Complex Behaviors in Cloud Computing project. This project seeks to understand and predict behavior in large distributed information systems by using mathematical and statistical techniques applied by scientists to study physical systems. NIST is evaluating various modeling and analysis methods. NIST is conducting its evaluation in the context of communication networks, computational grids and computational clouds. NIST has conducted several studies related to networks and grids. In cloud computing, NIST is initiating a study of the applicability of our modeling and analysis techniques to computational clouds. As a challenge problem, NIST intends to use the model to study various resource allocation algorithms that might be employed to assign virtual machines to clusters and nodes within a cloud.

Thank you for the opportunity to testify today on NIST's role in the development and deployment of cloud computing technology. I would be happy to answer any questions you may have.