Ranking Member Yvette D. Clarke (D-NY), Opening Statement as prepared

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

"Cloud Computing: What are the Security Implications?"

October 6, 2011

Thank you for having this hearing on the 'Cloud' today, it is particularly timely in that the Department has just let a contract on moving some of its public websites to the 'Cloud'.

Cloud computing can and does mean different things to different people. The common characteristics most share are; on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and dislocation of data from inside to outside the organization.

The National Institute of Standards and Technology is developing a synopsis of cloud models and of their strengths and weaknesses, and as policy makers, it will be important that we know clearly how and when cloud computing is an appropriate tool for government agencies.

Cloud computing has been identified as a tool for bringing greater efficiency, functionality and flexibility to government computing, but the variety of models for service delivery and customer needs complicates any discussion of the technology.

Cloud computing is a developing area and its ultimate strengths and weakness are not yet fully researched, documented and tested. Assessing and managing risk in cloud computing systems can be a challenge. Things I am hoping to hear about today include deployment models, service models, economic considerations, operational characteristics, service-level agreements and security.

Inherently, the move to cloud computing is a business decision. Relevant factors to be considered include the readiness of existing applications for cloud deployment, transition and life-cycle costs, maturity of service orientation in the existing infrastructure, and security and privacy requirements.

The short definition of cloud computing used by NIST is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Complex computing systems are prone to failure and security compromise and it is important to understand that cloud systems, like all complex computing systems, will contain flaws, experience failures, and experience security compromises. In general, most would agree that agencies should have security controls in place for cloud-based applications that are the same as or surpass those used if the applications were deployed in-house.

Assessing and managing risk in government cloud computing systems will be a huge challenge, and our risk analysis for agencies information will be complicated. We must find the path to available safeguards that can reduce risk to an acceptable level.

What we want to achieve is a federal government IT that enables better service delivery, increased security, and dramatically lower costs. There are inefficiencies in our IT systems, and outdated technologies and information systems undermine our efficiency and threaten our security.

What we don't want are federal IT projects that last multiple years without delivering meaningful functionality or security. A government powered by modern information technology is a faster, smarter, and a more efficient government.