Testimony of

John Curran, President & CEO
American Registry for Internet Numbers

before the
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Homeland Security Committee U.S. House of Representatives

Hearing on
Cloud Computing: What are the Security Implications?

October 6, 2011

I. INTRODUCTION

Good morning Chairman Lungren, Ranking Member Clarke, Ranking Member Thompson, and Members of the Committee, and thank you for inviting me to testify before the Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee.

I am the President and Chief Executive Officer of the American Registry for Internet Numbers, Ltd. ("ARIN"), which issues Internet Protocol (IP) number resources for the US, Canada and Caribbean, but I am speaking here today in my personal capacity based on a long history of building and securing FISMA-compliant federal Information Technology (IT) systems.

I have first-hand knowledge of these matters from my experience in the Internet industry since 1990, including serving as the Chief Technology Officer for several government contractors and Internet Service Providers (ISPs) including BBN, GTE Internetworking and XO Communications, as well as Internet standards work in the Internet Engineering Task Force (IETF). Most recently, I served for 5 years as Executive Vice President and Chief Technology Officer for ServerVault, providing secure managed IT services for sensitive federal government applications. My duties included direct responsibility for securing and preparing the certification of FISMA Moderate impact level federal information systems over shared Internet-based infrastructure. I have prepared my remarks today out of a desire to see the advancement of responsible Cloud-based computing for the federal government.

I would like to start by offering congratulations to the GSA for the development of its Federal Risk and Authorization Management Program (FedRAMP) program, as well as the recent Infrastructure as a Service (IaaS) Blanket Purchase Agreement (BPA) awards. By developing this program in cooperation with the Federal CIO council, the GSA has enabled agencies to leverage cloud-based storage, virtual machines, and web hosting

services in a manner that should improve the cost and timeliness of federal IT system deployments.

II. MANAGING EMERGING RISKS FROM CLOUD COMPUTING

As a result of my experiences deploying federal IT systems over the public Internet, I was asked to present at cloud interoperability workshop in 2009, and to identify the most critical challenges that Federal CIO's faced in making use of cloud computing under the existing FISMA security framework. Back then, the major difficulties that I identified were:

- Agency pressure for deployment of timely, cost-effective IT systems
- Administration expectations for leveraging new IT technologies
- Compliance with IT policy mandates (federal and agency-specific)
- Lack of common IT infrastructure services between systems & Potential vendor lock-in with any sizable deployment
- Preparation of extensive FISMA control documentation for each system

It is remarkable to see the progress that has occurred since that time. As a result of the FedRAMP program (with its common security control baseline), agencies now have a clear roadmap that should address many of these challenges in making use of cloud computing for federal IT applications.

I must note, however, that cloud computing does not eliminate all of the challenges, and in particular, cloud computing may actually heighten the difficulties that Federal CIO's face in some areas if not carefully managed. The areas that are most likely to pose increased risks as a result of the introduction of cloud computing are:

1. Interaction of cloud computing services with federal cybersecurity initiatives
2. Physical location of cloud computing facilities and data
3. Migration between vendors of cloud computing services
4. Evolution of cloud computing services with Internet technologies

None of these risks precludes the use of cloud computing services by the federal government, but each does pose new challenges for Federal CIO's to consider and may warrant consideration by the Federal CIO Council and its partners to determine if additional standards or coordination activities would help minimize these risks. I will outline each of these risk areas with recommendations for further consideration.

III. INTERACTION OF CLOUD COMPUTING SERVICES WITH FEDERAL CYBERSECURITY INITIATIVES

There are several government-wide IT security initiatives that require consideration with respect to cloud computing because of their service nature: specifically, there is the

distributed issuance and recognition of user authentication credentials via the HSPD-12 initiative, as well as the provision of secure and monitored Internet connectivity via the Trusted Internet Connections (TIC) initiative. These programs provide certain security – related services to federal IT environments which result in increasing cybersecurity protection on a government-wide basis as more agencies make use of the services.

While specified in the FedRAMP security profile for Moderate risk environments, the actual mechanism and ability to participate in these government-wide cybersecurity initiatives by private cloud computing vendors remains unclear, and any deployment of federal IT systems via cloud computing services that do not leverage these common capabilities dilutes the value of these initiatives in supporting the overall cybersecurity stance of the federal government.

The goal must be to have unequivocal documentation for cloud computing companies on how to appropriately secure their offerings, including how to make use of government-wide cybersecurity initiatives, and thus encourage significant industry-wide vendor participation in offering FedRAMP cloud services. The resulting competition will both drive down costs and improve service quality for all FedRAMP participants.

IV. PHYSICAL LOCATION OF CLOUD COMPUTING FACILITIES AND DATA

One of the more unusual consequences that results from the use of the cloud computing is the potential loss of the ability to know at any given time the specific physical location for the systems and data which support a given federal IT system. While it may be possible to know the set of data centers which support the service (and the FISMA-based FedRAMP security control profile does specify certain physical controls at such facilities for facility access, power redundancy, etc.), the question of actual physical location of the federal IT system is highlighted when the cloud service provider has facilities which are outside of the United States.

As a practical matter, there may not be a concern with incident services being provided for out of non-US locations, and it may be desirable in some circumstances with federal applications that must be accessed globally. However, the present FedRAMP profile does not directly address the question of location and it is not assured that use of facilities and storage of data outside the United States is universally desirable, particularly if the use of cloud computer for federal IT applications is undertaken on a large scale.

The FedRAMP program should include controls that address the physical location of cloud computing facilities and data storage used by the application, and allow (as is done with the corresponding personnel controls) for the consideration of exceptions once fully documented and reviewed.

V. MIGRATION BETWEEN VENDORS OF CLOUD COMPUTING SERVICES

The ability to extract agency data in standard formats from cloud computing services (whether that be application data such as mail messages and mailing lists, or system data such as the virtual server, storage, and network configurations) is essential to be able to migrate between cloud vendors. Lack of this capability means vendor lock, eroding the financial benefits of cloud computing and preventing timely response if a vendor's security is irrevocably compromised.

There are ongoing efforts in the area of standards for cloud computing data, and this work should continue and be prioritized by the agencies supporting the FedRAMP program. Unlike an internal agency information system, cloud solutions are inherently subject to change by the cloud service provider, and this creates a new requirement (specifically, the ability to quickly and reliably migrate to another service provider) where it previously was not needed for agency systems. FedRAMP must facilitate migration capabilities to protect against any cloud computer vendors that fail to continuously deliver the necessary quality or security in their offerings.

The FedRAMP security control profile includes standard FISMA contingency planning and recovery security controls, but these fundamentally only address recovery within a given service provider cloud. Specific mechanisms should be put in place to insure that federal agencies can extract their data and configuration in generally accepted formats and that these mechanisms suffice for service migration to other cloud computing vendors.

VI. EVOLUTION OF CLOUD COMPUTING SERVICES WITH INTERNET TECHNOLOGIES

The Internet is constantly evolving with the introduction of new standards and technology, and in making use of the Internet as a platform for cloud computing, FedRAMP must be equally prepared as these changes occur. This is particularly true when it comes to Internet technology improvements in the area of cybersecurity.

In many cases, the Federal government has taken an active interest in the technologies and standards that could improve the overall security of the Internet, and this includes DNSSEC initiative in securing the Domain Name System (DNS), the next version of the underlying network protocol for the Internet – Internet Protocol version 6 (IPv6) and ongoing work in Internet routing security. These technologies are now being deployed in the public Internet, and are also covered by specific directives in the FISMA security control baseline and/or guidance from OMB.

These new standards are quite important in protecting the global Internet from cybercrime, in that they insure that Internet users reach the actual web site that they intended to, and that their communication is protected in the process. When it comes to

agency use of cloud computing services, these protections are equally important, since these services are reached over the public Internet.

It is crucial that the FedRAMP program clearly and unambiguously incorporates DNSSEC and IPv6 into the FedRAMP baseline, and that ongoing developments in Internet-wide security technologies are promptly incorporated as they reach maturity.

Furthermore, the ongoing need to adopt and maintain state-of-the-art security technologies and practices for cloud computing services does not appear to be given sufficient priority in the FedRAMP approach. While traditional federal IT systems have been built and certified one at a time in predominantly closed environments, the rapid pace of evolution of Internet threats requires equally dynamic and responsive security responses. Vendors should be given the flexibility to propose additional or alternative security mechanisms, as there are security lessons learned from running large-scale Internet services that are not readily available to the federal IT community, and the benefits of such experience should not be lost in the process of structuring cloud services into the FISMA framework.

VII. CONCLUSION

The FedRAMP program is a remarkable achievement; by providing agencies with ready access to additional computing resources that have already undergone a joint authorization process, the program offers the potential to significantly improve cost and timeliness of federal IT deployments.

While not detracting from the importance of this achievement, the use of public and shared cloud computing services does introduce new areas of risk to be considered, and this is particularly true with respect to the interaction of cloud computing services with federal cybersecurity initiatives, the geographic location of federal data, the migration between vendors of cloud computing services, and the evolution of cloud computing services with the Internet.

The risks should not preclude use of cloud computing services by the federal government, but the model should be closely examined, and appropriate efforts inserted into the FedRAMP program so that it can deliver its full benefits in an efficient and secure manner.

*****

Mr. Chairman, Ranking Member Thompson and Members of the subcommittee, this concludes my written statement.

Thank you again for this opportunity to speak before you today on this important topic, and I would be happy to answer your questions.