CrossTalk would like to thank DHS for sponsoring this issue.

Moving to the cloud is the latest irresistible force to sweep the C-suite and Main Street. The opportunities for flexibility, savings, reduced sustainment, and ubiquity have made cloud solutions compelling for Information Technology (IT) managers around the world.

Those who consider the benefits of cloud computing often cite potential improvements in efficiency, agility, and innovation. These individuals often indicate that existing computing facilities have some degree of duplication, are difficult to manage, and operate at less than optimum capacity. A major benefit of the cloud would be the ability to rapidly meet new demand for capacity and services due to the elastic capacity of cloud providers. Moreover, the cloud also reduces the need for asset management of rapidly evolving technology and enables the use of innovative solutions.

However, there are security challenges unique to cloud architectures, including: dynamic provisioning of platforms of unknown or dubious origin, global access by mobile (and largely insecure) devices, eroded trust boundaries, and the possibility of malevolent neighbors in your public cloud. The acquirer of services must be aware that there are variances in cloud provider security capabilities. Service Level Agreements (SLAs) provide important coverage, including properly articulated security and resiliency expectations, but might not offer a comprehensive solution.

The good news is that the processes, practices, tools, and techniques from traditional IT can be applied to address many cybersecurity concerns. As savvy consumers, we can employ established software and supply chain assurance methods when acquiring cloud-based services, as long as we recognize the new risks and challenges presented by this new technology. Cloud computing has the potential to improve our security capabilities and services. As agencies and departments consider various cloud architectures, more stringent security requirements will encourage cloud service providers to build cloud services with significantly improved security.

To help ensure the U.S. Government adopts best practice methods as we move to the cloud, DHS has coordinated with NIST and other federal agencies in standardizing expectations for IT security for cloud services. Moreover, DHS has provided technical assistance to the Federal Risk and Authorization Management Program (FedRAMP). Housed in the General Services Administration (GSA), the FedRAMP provides a security certification and authorization process that applies consistency and transparency across Federal departments and agencies for cloud implementation and security. This program builds security into the government-wide solicitations from the beginning, while enabling agencies to retain their responsibility and authority to meet their unique network security needs. For providers, the FedRAMP performs oversight of continuous monitoring, and allows vendors to participate in a single risk management process, share compatible requirements, and a consistent assessment process.

As we look to the promise of FedRAMP and other secure services delivering capabilities on which our nation depends, our cybersecurity processes and procedures will continue to evolve, and NIST Special Publications, such as SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations,” will remain in the forefront of security guidance. Although there will always be more to be done to achieve a safe and cyber-secure cloud, we must embrace a shared strategy for cybersecurity and work together to reap the benefits we all envision from this new and dynamic technology.

Roberta “Bobbie” Stempfley
Acting Assistant Secretary
Office of Cybersecurity and Communications
Department of Homeland Security