Statement of Scott Charney

Corporate Vice President, Trustworthy Computing
Microsoft Corporation

Adapting to the Cloud

Testimony Before the
Committee on Oversight and Government Reform and the
Subcommittee on Government Management, Organization, and Procurement
U.S. House of Representatives

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

July 1, 2010

Chairman Towns, Ranking Member Issa, Chairwoman Watson, Ranking Member Bilbray, Members of the Committee and Subcommittee: Thank you for inviting me here today to discuss the federal government's use of cloud computing.

My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft Corporation. I also serve as one of four Co-Chairs of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States (U.S.) Department of Justice. I was involved in nearly every major hacker prosecution in the U.S. from 1991 to 1999; worked on legislative initiatives, such as the National Information Infrastructure Protection Act that was enacted in 1996; and chaired the G8 Subgroup on High Tech Crime from its inception in 1996 until I left government service in 1999.

I currently lead Microsoft's Trustworthy Computing (TWC) group, which is responsible for ensuring that Microsoft provides a secure, private, and reliable computing experience for every computer user. Among other things, the TWC group oversees the implementation of the Security Development Lifecycle (which also includes privacy standards); investigates vulnerabilities; provides security updates through the Microsoft Security Response Center; and incorporates lessons learned to mitigate future attacks.

Microsoft plays a unique role in the cyber ecosystem by providing the software and services that support hundreds of millions of computer systems worldwide. Windows-based software is the most widely deployed platform in the world, helping consumers, enterprises, and governments to achieve their personal, business, and governance goals. Also, as Steve Ballmer, our Chief Executive Officer, stated, "we're all in" when it comes to the cloud. We already offer a host of consumer and business cloud services, including a wide array of collaboration and communications software.

We operate one of the largest online e-mail systems, with more than 360 million active Hotmail accounts in more than 30 countries/regions around the world. Microsoft's Windows Update Service provides software updates to over 600 million computers globally, and our Malicious Software Removal Tool cleans more than 450 million computers each month on average. We are a global information technology (IT) leader whose scale and experience shapes technology innovations, helps us recognize and respond to ever changing cyber threats, and allows us to describe the unique challenges facing the government as it moves to the cloud.

Cloud computing creates new opportunities for government, enterprises, and citizens, but also presents new security, privacy, and reliability challenges when assigning functional responsibility (*e.g.*, who must maintain controls) and legal accountability (*e.g.*, who is legally accountable if those controls fail). As a general rule, it is important that responsibility and accountability remain aligned; bifurcation creates a moral hazard and a legal risk because a "responsible" party may not bear the consequences for its own actions (or inaction) and the correct behavior will not be incentivized. With the need for alignment in mind, I will, throughout the rest of my testimony, use the word "responsibility" to reflect both responsibility and legal accountability. It must also be remembered that there is another type of accountability:

political accountability. Citizens have certain expectations of governments (much like customers and shareholders have certain expectations of businesses) that may exceed any formally defined legal accountability.

As a cloud provider, Microsoft is responding to security, privacy, and reliability challenges in various ways, including through its software development process, service delivery, operations, and support. In my testimony today, I will (1) characterize the cloud and describe how cloud computing impacts the responsibility of the government and cloud providers; (2) discuss the responsibilities cloud computing providers and government must fulfill individually and together; and (3) examine the importance of trust and identity to cloud computing.

New Computing Models ("The Cloud") Create New Opportunities and Risks

Many people talk about "cloud computing"— what it is, what it does, and why it matters — but it is critically important to have a common understanding of the term before discussing how it changes risk management responsibilities. "Cloud computing" permits all users to leverage Internet-based data storage, processing, and services in new ways, thus complementing the traditional model of running software and storing data on personal devices and servers. There are several key characteristics of the cloud that differ from the traditional client-server model of computing and deliver benefits for customers, including global elasticity, geo-diversity, and co-tenancy.

- Global elasticity means that customers, including governments, enterprises, and consumers, can buy the computing power, storage, and resources they need in a fast and flexible manner without committing to long-term and costly technology investments. Global elasticity provides convenient access to, and creates opportunities for, more efficient delivery of services, and it helps control costs.

- Geo-diversity enables data to be stored in multiple locations, generating efficiency and speed benefits and enhancing reliability.

- Co-tenancy means multiple users share cloud infrastructure, which can create tremendous economies of scale and cost savings.

Service Models and Accountability

The benefits of the cloud can be realized through three different service models described below:

1. Software as a Service (SaaS): The cloud provider makes available to users a single application, such as Hotmail e-mail, or multiple applications, such as Microsoft's Office Suite online.

2. Platform as a Service (PaaS): Users may choose to develop and run their own software applications, while relying on the cloud provider to provide the underlying infrastructure and operating system. Microsoft's Azure is a cloud platform that enables users and developers to write and/or run their own applications.

3. Infrastructure as a Service (IaaS): At its most basic, users rent hardware or virtualized instances of hardware — the infrastructure — to deploy and run their own operating systems and software applications.

Customers need to make informed decisions about adoption of the cloud and its various service models because the model that is embraced will entail different allocations of responsibility between the customer and the cloud provider(s). In the traditional IT model, an organization is responsible for all aspects of its data protection, from its actual use of the data to the protection of that data in its IT environment. A complete data protection program will address the physical security of the data center, the trustworthiness of data center personnel, the configuration and management of hardware and software, and the management of IDs and access controls. Cloud computing changes this. While an organization will still control the use of its data, it will need to set limits on the cloud provider's use of that data. Additionally, it may transfer to the cloud provider the responsibility for certain data center operations. For example, the customer using IaaS may transfer responsibility for data center operations, including the trustworthiness of data center personnel, to the cloud provider.

Once this is understood, it becomes clear that the different cloud service models transfer different amounts of responsibility between the customer and the cloud provider. Figure 1 illustrates these shifts for the different cloud service models.

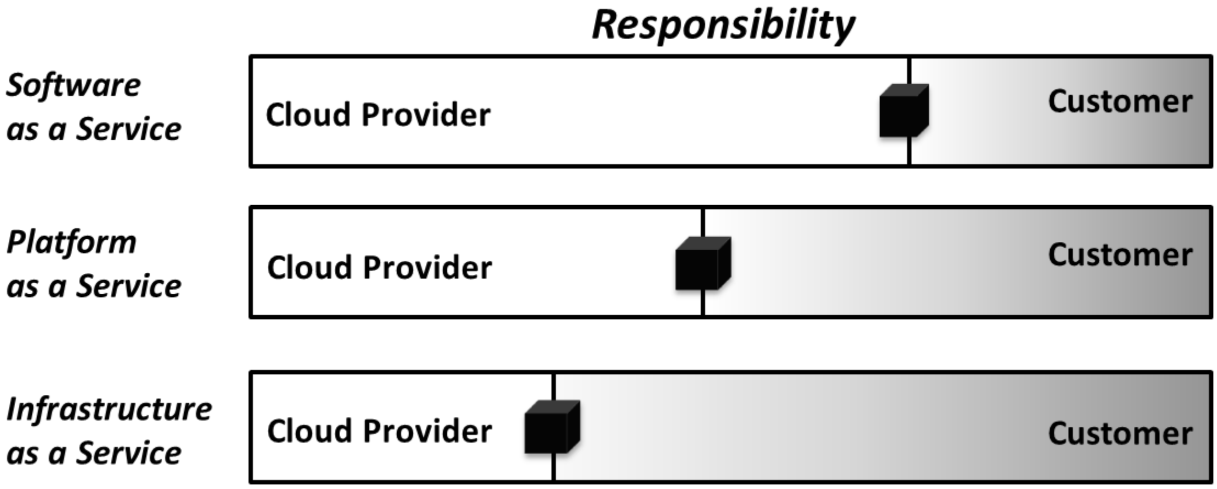

Figure 1: Shifting Responsibility in the Cloud

For example, IaaS customers maintain considerable responsibility for platform, applications, and personnel, but transfer responsibility for the infrastructure (*e.g.*, the physical data center, data center personnel, and hardware) to the cloud provider. At the other end of the spectrum, if customers utilize the entire cloud (from infrastructure to applications), they transfer yet more responsibility to cloud service providers, from physical and personnel security to the secure development and maintenance of applications and the management of identities for access control. Of course, the fact that a customer has transferred these responsibilities to the cloud provider — and may even have transferred legal liability by contract — is not the end of the matter. For example, citizens ultimately may hold a government accountable if data is lost or stolen, or critical data is not available when needed, notwithstanding any cloud provider agreement. Thus, a government may remain "accountable" to its constituents when an incident occurs, notwithstanding any contractual apportionment of responsibility. That said, as the federal government becomes a customer of cloud services, it must be clear about its requirements — and cloud providers must be responsible for meeting those requirements.

Contracts remain, of course, the primary legal documents for aligning responsibilities, but clearly and comprehensively defining requirements for cloud services is an arduous task. As more functions are transferred to cloud providers, requirements become more critical, more challenging, and more complex. The requirements are more critical because of the scale and scope of functions and data being moved to the cloud; they are harder because this is a relatively new domain where reasonable minds may often differ; and they are more complex because specificity is necessary to ensure a common understanding of expectations between customers and providers. While many enterprises have significant experiences with outsourcing services, the integration and adoption of cloud services is an important evolution in technology adoption and integration. Defining how responsibilities for security, privacy, and reliability are allocated — and creating sufficient transparency about this allocation — represent new challenges. Both customers and cloud providers must understand their respective roles and be able to communicate compliance requirements and controls across the spectrum of services available in the cloud.

Types of Clouds

The three basic service models are generally deployed in four different ways: public clouds, private clouds, community clouds, and hybrid clouds.

- In a public cloud, the general public can access the cloud services through a multi-tenant environment.

- In a private cloud, a single organization makes use of a dedicated cloud infrastructure.

- A community cloud is a private cloud shared by a group of organizations or a community with shared concerns, missions, or interests.

- Finally, a hybrid cloud makes use of two or more cloud types, such as a private cloud and a public cloud, where each cloud remains separate, but is linked in a way that can enable data and applications to flow and communicate between the two.

Which cloud model is most appropriate depends on the nature of the IT activity. For highly sensitive information, dedicated on-premises private clouds can provide more control and security, but at a higher cost and with lower scalability, redundancy, and other benefits. In comparison, public clouds offer the greatest cost savings and likely the greatest elasticity, but at the cost of reduced control and increased risk due to co-tenancy. Hybrid clouds may provide the benefits and risks of both types.

Security, Privacy and Reliability Responsibilities in the Cloud

Regardless of the service model and type of cloud deployment selected, security, privacy, and reliability challenges must be addressed. Cloud providers and governments each have distinct responsibilities and, in some cases, shared responsibilities, as they work to help the Nation realize the benefits of cloud computing services.

Cloud providers

The importance of assuring the confidentiality, integrity, and availability of customer data and operations is not new, but cloud computing does have the effect of shifting the responsibility (in whole or in part) for these areas to cloud service providers. Providers must rise to this new reality and provide commensurate levels of assurance for their customers.

Microsoft addresses this challenge through our holistic approach for managing security, privacy, and reliability that is designed to meet or exceed customer requirements. Our approach includes three cross-cutting functions to manage physical, personnel, and IT security: (1) utilizing a risk-based information security program that assesses and prioritizes security and operational threats to the business; (2) maintaining and updating a detailed set of security controls that mitigate risk; and (3) operating a compliance framework that ensures controls are designed appropriately and are operating effectively.

Any analysis of the cloud must start with the technology that powers it. Microsoft has long recognized the importance of building secure and reliable software, and we devote considerable resources to ensuring the quality of our software, including adherence to the Security Development Lifecycle (SDL). The SDL consists of continuously evolving processes and tools designed to reduce the number and severity of vulnerabilities in software products and ensure appropriate and agile response when necessary. Importantly, in the context of discussing providers' responsibilities in the cloud, it should be noted that the SDL considers and accounts for risks related to the environment in which the application will run (*e.g.*, client computers, on-premises services, or the cloud). Thus, the SDL ensures that Microsoft cloud services are developed using secure development practices.

The SDL is not only about improving code quality; it also helps protect people and their personal information. In cases where data from multiple users is stored on the same system, there are implications for managing the transfer, storage, retrieval, and access of that data in a manner that avoids disclosure of the data to unauthorized parties. Users need to know that they can trust the software and hardware to protect their sensitive information and to isolate them from other co-tenants.

Online service providers can use a variety of technologies and procedures to help protect personal information from unauthorized access, use, or disclosure. Microsoft's software development teams apply the "PD3+C" principles, defined in the SDL, throughout the company's development and operational practices. The PD3+C principles are:

- **Privacy by Design** – Microsoft uses this principle in multiple ways during the development, release, and maintenance of applications to ensure that data collected from customers is used for specified purposes and that the customer is given appropriate notice in order to enable informed decision-making. When data to be collected is classified as highly sensitive, additional security measures — such as encrypting while in transit, at rest, or both — may be taken.

- **Privacy by Default** – Microsoft offerings ask customers for permission before collecting or transferring sensitive data. Once authorized, such data is protected using multiple means, such as access control lists (ACLs) and identity authentication mechanisms.

- **Privacy in Deployment** – Microsoft discloses privacy mechanisms to organizational customers as appropriate to allow them to establish appropriate privacy and security policies for their users.

- **Communications** – Microsoft actively engages the public through publication of privacy policies, white papers, and other documentations pertaining to privacy.[1]

Finally, cloud providers have a responsibility to provide reliable and trusted services. Reliability can be achieved through geo-diversity and redundancy in applications, data, and data centers, resiliency in communications, and high availability of services (as guaranteed in Service Level Agreements (SLAs)). Microsoft has multiple data centers located in the U.S., Europe, and Asia that meet internationally recognized standards and third party evaluations (*e.g.*, ISO 27001:2005 and SAS 70 Type I and Type II).[2] We are able to provide robust, geo-diverse services with more than 9,000 Microsoft hosting providers and more than 40% of all hosting providers worldwide using Microsoft products to support their hosting services. We also provide customers the ability to geo-locate their data, for example, ensuring that data resides only in U.S.-based servers. The integrity of cloud providers — including their personnel — is increasingly important, because the scale and scope of their actions can be exponentially increased in the cloud. Microsoft engineers are required to complete state-of-the-art training on many technology topics, including security and privacy, to help them keep pace with an ever-changing industry. By building and managing resilient infrastructure with trustworthy people, we can ensure high availability and commit to 99.9% uptime and 24x7 support in our SLAs.

Government

As cloud providers continue to evolve their operations to meet the responsibilities cloud customers transfer to them, so too must government evolve its approach to integrating the cloud into its operations. The Information Age has arrived and the cloud is ready for the government,

[1] For more information about Microsoft's commitment to privacy, see the Microsoft Trustworthy Computing Privacy page at www.microsoft.com/privacy.

[2] Microsoft's online Information Security Program has been independently certified by British Standards Institute (BSI) Management Systems America as being compliant with ISO/IEC 27001:2005.

but in many respects, the government is not yet ready for cloud computing. For example, according to the Government Accountability Office, federal agencies have serious and widespread information security control deficiencies. In their fiscal year 2009 performance and accountability reports, 21 of 24 major federal agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency. Furthermore, agencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. Agencies' current struggles to identify, manage, or account for security of data and systems are not immediately solved by integrating cloud services. Agencies must still identify and communicate requirements and expectations before transferring the responsibility of these functions to cloud providers. Once this is done, cloud service providers can then enhance agencies' abilities to meet their compliance challenges.

Progress is being made. The Federal Risk and Authorization Management Program (FedRAMP) is an important initial effort to provide joint security authorization for large outsourced systems. This program creates efficiencies for the government by enabling common assessments of cloud service providers, which allows a cloud provider to certify once and have that certification shared among the agencies. The result is a more efficient process than individual agency evaluations. FedRAMP also creates a process for cloud service providers to provide transparency into their operations and empowers agencies to fulfill their responsibilities for systems. Over time, this program could even begin to help reduce the number of federal systems resulting in further savings. In short, FedRAMP is the first government program to help balance responsibility between government agencies and cloud providers.

For security, agencies must approach the cloud thoughtfully, with an unwavering commitment to evaluate threats, assess risks, and define security requirements in order to ensure risks are managed at acceptable levels. Accordingly, agencies must adapt and advance their information security programs and communicate the attendant requirements to their cloud providers so that cloud providers can demonstrate that appropriate security and other operational controls have been implemented.

The government also should require that providers from which it procures cloud computing services meet the government's operational requirements for security, privacy and reliability. As threats continue to evolve, it remains critically important that cloud providers demonstrate secure development practices and transparent response processes for their applications. More broadly, the government should, wherever practicable, ensure that the technologies it procures, acquires, and uses are built and maintained in accordance with industry best practices for secure development. It should also promote (with appropriate incentives) such practices for all application developers. Users — including government users — need to be sure not only that their "boxed" products are secure, but also that their software applications — including those rapidly developed for the cloud — are built and provided on the basis of sound fundamentals.

Despite best efforts to prevent and protect against threats, incidents will inevitably occur. Some of these incidents will require law enforcement investigations, which may be hindered by forensic and jurisdictional issues resulting from cloud architecture and characteristics. Cloud service providers face a number of challenges with respect to forensics. For example, the complexities of the technology and the distributed nature of the data can reduce both access to and the overall quality of forensics data, making audit and attribution of attacks more challenging. Users' data can be commingled on single pieces of hardware, in virtual machines, or distributed across multiple services in the cloud environment.

For investigations, government may not trust cloud providers to investigate an incident, but at the same time, the cloud provider may not be able to grant the government broad access to conduct an investigation into a multi-tenant environment since that might give the government access to confidential data it is not authorized to see. With respect to jurisdiction for law enforcement investigations, the location(s) of data, particularly when crossing national boundaries, may create significant challenges. These legal challenges can be managed, such as through use of geo-located private clouds, but probably cannot be fully resolved for all users in all cases. In some cases, new technologies, techniques, or standards for data forensics and data deletion may need to evolve for use in public, multi-tenant clouds.

In addition to these security requirements, government must identify appropriate controls to protect the vast amounts of sensitive personally identifiable information (PII) that it maintains and uses. Agreements with cloud providers are just one aspect of taking adequate precautions. A cloud provider can protect data as designated by the agency, but the agency itself must maintain policies and procedures for the identification and handling of data in-house, such as on employees' computers. In other words, privacy protections must be maintained seamlessly from the client to the cloud.

Protecting privacy also requires keeping pace with today's technological realities. Congress enacted the Electronic Communications Privacy Act (ECPA) — the primary federal statute regulating government access to subscriber information, stored communications, and real-time communications — almost 25 years ago, at a time when the vast majority of Americans had never heard of the Internet or e-mail. Electronic communications have evolved dramatically over the past 25 years and have become an essential mode of interaction for most Americans. But the law has not kept up with the changes in technology. When applied to the modern computing world, ECPA is complicated and unclear, and needs to be clarified and updated in order to properly account for consumers' reasonable privacy expectations. Microsoft supports the efforts to modernize ECPA that are being led by the Digital Due Process Coalition, and we encourage the government and Congress likewise to take up responsible reform of ECPA.

As with security and privacy, reliability remains a concern of government. In geo-diverse cloud environments, redundancy can help limit situations where data becomes unavailable; yet at the same time, customers must address connectivity to and reliable performance of cloud services. As these services become more integrated into agency operations and mission critical functions, government officials must ensure that they can maintain connectivity to the cloud by having physically diverse communications paths and alternate methods for accessing data centers. In addition, agencies should consider their reliance on cloud services in their business continuity and disaster recovery planning, and establish the necessary SLAs with their cloud providers to ensure continuity of operations.

If requirements are properly defined, cloud computing could ease the compliance challenges facing government. Unfortunately, the federal enterprise struggles today to meet key compliance goals such as those required by the Federal Information Security Management Act (FISMA). With 23,859 government systems across 25 agencies, key compliance metrics continue to lag. For example, 46% of high impact systems and 45% of medium impact systems in the government have not been certified or accredited. That totals 11,548 uncertified systems. Furthermore, just more than half of all federal systems have had security controls tested or business continuity plans tested.[3] Cloud computing could help ensure government data and systems meet expectations for certification, controls testing, and continuity planning. The cloud also provides a platform by which government could reduce the number of duplicative systems — saving costs, ensuring consistent application of Federal security requirements, and improving services to citizens and compliance.

Shared Responsibilities

Protecting the public good in the cloud requires Congress, the Executive Branch, and industry to work together. Our collaborative efforts should focus on promoting transparency around cloud computing providers' security, privacy, and reliability practices and, in turn, helping to ensure that users can make informed choices. Together, government and cloud providers should also address access and consent in privacy practices, including by requiring notice of privacy policies to cloud computing customers and by promoting the harmonization of global data privacy and data retention laws. Finally, we should collaborate to strengthen criminal penalties against hackers of cloud computing, and define penalties for criminal misuse of legitimate cloud services, to provide more effective deterrence and to enhance prosecutors' abilities to investigate and prosecute malicious actors who place cloud computing customers and the broader ecosystem at risk.

Microsoft is committed to securing the ecosystem and works with government through multiple public private partnerships; we also regularly work with our industry peers to address the most challenging issues facing users. Forums such as the Cloud Security Alliance (CSA) bring together subject matter experts to discuss key cloud risks and challenges and share best practices to resolve them. The CSA serves to create a cohesive set of recommendations and provide education around cloud security issues for cloud providers and consumers both domestically and internationally. Industry participation with organizations such as the National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA) helps to define and communicate the security, privacy, and reliability requirements among governments, other cloud users, and cloud providers. Government and industry must continue these international efforts to define and harmonize standards that enable innovation, create opportunity, and power the modern economy.

[3] *See* OMB's Fiscal Year 2009 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, *available online at* http://www.whitehouse.gov/omb/assets/egov_docs/FY09_FISMA.pdf.

These actions will not solve fully the security, privacy, and reliability challenges of integrating cloud computing into the federal enterprise. However, by strengthening the security, privacy, and reliability practices in cloud computing services, and providing greater transparency to users, cloud providers and government will help build confidence in cloud computing services and, in turn, help cloud computing services to reach their potential.

Trust and Identity Imperatives

I have spoken about responsibility with respect to security, privacy, and reliability, but one particular issue is worthy of further note. Today, there are over 1.8 billion Internet users in the world, or more than 26% of the population.[4] Internet users continue to grow at over 19% year over year,[5] yet the mechanisms to provide identity, authentication, and attribution in cyberspace do not yet meet the needs of citizens, enterprises, or governments in traditional computing environments or for the cloud. The lack of trust online stems in part from our inability to manage online identities effectively. The cloud only amplifies the need for more robust identity management to help solve some of the fundamental security and privacy problems inherent in current Internet systems. As people move more and more of their data to the cloud, and share resources across cloud platforms, their credentials are the key to accessing that data. Every day, Microsoft authenticates more than one billion Windows Live ID authentications and processes two to four billion Exchange Hosted Services e-mails. Cloud providers will need to develop technologies that allow us to better manage identities both within their own systems and in settings where identities must be federated across separate networks.

Cyber attacks are facilitated by the anonymity and lack of traceability of the Internet; malicious actors in cyberspace must be convinced that either the cost of their actions is not worth the return on investment or that there is a real chance of attribution and punishment. Mandating robust authentication for some Internet uses — such as accessing critical infrastructures — while ensuring anonymity at other times (*e.g.*, when citizens want to access public information) can help strike the right balance between security and privacy. Modern identity systems increasingly permit users to provide elements of their identity without having to provide more information than is required for a given transaction. Additionally, in appropriate cases, hardware, software and data should be authenticated as well. For example, if someone wants to visit a website with content that is inappropriate for children, that person should be able to present reliable proof of age without having to reveal his or her entire identity. Granular attributes of identity that can be proven or asserted are called “identity claims.”

While the industry and academia are advancing many technological capabilities for strong and robust identity and identity claims, a supporting ecosystem is also required. We must have mechanisms (and associated policies) for the issuance of digital credentials that provide stronger verification and are based upon in-person proofing. We must have interoperable identity systems so those who provide robust credentials and those who wish to consume them can do so easily,

[4] http://www.internetworldstats.com/stats.htm

[5] http://www.internetworldstats.com/pr/edi038.htm

thus enabling better trust decisions. The need for interoperability also demands standards and formats for managing and exchanging identity information.

The draft *National Strategy for Trusted Identities in Cyberspace*,[6] recently released by the White House, represents significant progress to help improve the ability to identify and authenticate the organizations, individuals, and underlying infrastructure involved in an online transaction. Government and industry must continue to work together on this initiative, as well as on advancing standards and formats on both a national as well as a global basis to enable a robust identity ecosystem.

Conclusion

Integrating cloud services into the federal enterprise fundamentally advances government in the Information Age. The characteristics of the cloud can enable a new agility and responsiveness in government to meet the needs of its citizens, but only if government and cloud providers work together in this transformation to embrace the new responsibilities of the cloud.

As part of this transformation, agencies' business models will change and they will transfer responsibilities for security, privacy, and reliability, in varying degrees, to cloud providers. Evaluating and apportioning the risks resulting from this transfer depends largely upon the type of cloud computing service model(s) selected. The adoption of cloud computing in the government is not about the success or failure of any one agency, but about the federal enterprise transitioning functions in a thoughtful and healthy way. The success of this transition depends on two factors: (1) the ability to adapt and advance information security programs and to communicate requirements to agencies' cloud providers; and (2) the ability of cloud providers to meet customers' requirements with sufficient transparency to ensure that requirements for security, privacy, and reliability are met appropriately.

Government is not alone in the adoption and integration of cloud services. Enterprises of all sizes and consumers are dramatically increasing their dependence upon cloud services. As such, it is incumbent upon the government to work with industry to address our shared responsibilities. Addressing these new fundamentals will foster innovative uses of the cloud, cultivate confidence, and advance information technologies for the new economy. The alignment and understanding of responsibility in the cloud requires greater transparency from both cloud providers and cloud customers (including enterprises and governments). The more precise and transparent we are, the greater the trust we will build, and the greater opportunity we create.

[6] http://www.dhs.gov/xlibrary/assets/ns_tic.pdf