



Cloud First, Cloud Fast: Recommendations for Innovation, Leadership and Job Creation

A Report from the Commission on the Leadership
Opportunity in U.S. Deployment of the Cloud (CLOUD²)*

*Pre-publication copy – subject to minor technical corrections. Final printed version available Aug 2, 2011 at www.techamericafoundation.org/cloud2.

CLOUD² COMMISSION REPORT

FOREWORD

Cloud technologies are transforming the way computing power is bought, sold and delivered. Rather than purchasing licenses or hardware, users may now obtain computing power as a service, buying only as much as they need, and only when they need it. This new business model brings vast efficiency and cost advantages to government agencies, individuals, and companies of all sizes. The numerous benefits of cloud computing have already won over many adopters and are generating significant cost savings, efficiencies, flexibility, innovation, and new market opportunities.

This report reflects the growing imperative to fully embrace and capitalize upon the power of cloud computing. The Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD²) developed the report at the encouragement of the Federal Chief Information Officer and the U.S. Department of Commerce. The Commission's mandate was to generate recommendations for accelerating adoption of cloud technologies in the U.S. government and in the commercial space and to identify public policies that will help foster U.S. innovation and leadership in cloud computing.

The Commission was composed of representatives from 71 companies and organizations, including cloud providers, cloud users, and other businesses that are involved in enabling cloud deployment. To build on this diverse set of expertise and perspectives, the Commissioners interviewed numerous government representatives, heard presentations from a variety of organizations, and analyzed relevant past reports.

Actionable Recommendations — Trust, Transnational Data Flows, Transparency and Transformation

Moving to cloud computing is a change that involves people, policies, processes, and technology. The Commission identified barriers that have kept some government agencies from moving to the cloud and recommended actionable solutions to overcome these. In addition, the Commission identified barriers to commercial deployment of cloud services and recommended actions to eliminate them. Since government, industry and academia share the responsibility to accelerate adoption and drive U.S. innovation and leadership, the recommendations reflect actions for all three key stakeholders. Industry, as represented by the Commission members, is committed to enabling the transition to the cloud by companies and government agencies and accepts the responsibility for taking actions that enable cloud adoption.

In this report, the Commission has focused on 14 specific recommendations, categorized into four thematic areas: Trust, Transnational Data Flows, Transparency, and Transformation. For each recommendation, the report identifies why the action is needed, how it should be

implemented, who should implement it, and what benefits should be expected from implementation. The Commission intentionally made these recommendations direct and prescriptive.

The four areas are briefly discussed below.

Trust

Users of cloud computing want assurance that when using cloud services, their workloads and data will be treated with the highest integrity and their security, privacy, and availability needs will be met. To enable trust and confidence in cloud services, the Commission recommends that government and industry develop common frameworks, best practices and metrics around security and information assurance to assist users in choosing and deploying the security level most appropriate for their workloads. The Commission also recommends strengthening the identity management ecosystem and data breach laws, as well as supporting increased research on cloud computing as an investment in future cloud innovation.

Transnational Data Flows

In a global economy, it is common for businesses to operate in multiple countries and for cloud providers and users to work and transfer information across national borders. This adds complexity to cloud adoption because of the data, processes, and people residing on multiple continents with different laws and cultures. In this context, the Commission recommends that industry and the U.S. government promote privacy frameworks, that the U.S. government identify and implement mechanisms to clarify processes and mechanisms around lawful government access to data, and that the U.S. continue international discussions in these areas. We also recommend that the U.S. government lead by example by demonstrating its willingness to trust cloud computing environments in other countries for appropriate government workloads.

Transparency

Users want an abundance of information about the cloud services they buy and unfettered access to the data and processes they entrust to the service provider. To meet these needs, cloud providers must be open and transparent regarding the characteristics and operations of the services they provide. Government and industry should collaboratively develop metrics that facilitate this information sharing and customers' ability to compare cloud offerings. Additionally, to ensure that data is available to customers should they wish to change cloud services, cloud providers should enable portability through industry standards and best practices.

Transformation

The transition to cloud computing is placing new requirements on purchasing processes, infrastructure, and people's skills. For government agencies, the fact that buying cloud computing services can be fundamentally different from buying in-house IT systems poses a

challenge. Therefore, agencies, the Office of Management and Budget (OMB), and Congress must demonstrate more flexibility around budgeting and acquisition processes. Such flexibility, in combination with OMB incentives for moving to the cloud, will increase the rate of adoption by government agencies. Additionally, to accommodate the bandwidth and reliable connectivity necessary for the growth of cloud computing, the nation's currently stretched and aging IT broadband infrastructure should be updated, in conjunction with embracing IPv6. To help acquisition and IT personnel understand and carry out the transition to cloud, government agencies, companies, and academia should develop and disseminate appropriate educational resources.

In addition to the recommendations in the body of the report, the Commission also produced a *Cloud Buyer's Guide*. The guide walks potential government buyers through questions to ask and steps to take prior to purchasing a cloud computing solution. Designed to be a living document, the guide is available online at <http://www.cloudbuyersguide.org/>. As cloud technology evolves, this online resource can be easily updated with new frequently asked questions (FAQs) and guidance.

By providing clear, actionable recommendations, the Commission hopes to help accelerate the deployment of cloud computing at companies and government agencies. Cloud's widespread adoption will drive increased efficiencies and job growth and continue to position the United States as a technology leader in a global marketplace.

Introduction/Purpose of Report

For more than 50 years, the United States has taken advantage of new developments in Information Technology (IT). U.S. companies and government agencies were early adopters of the mainframe computer, the minicomputer, the personal computer, and the World Wide Web. We are now entering a new phase in the history of computing that will be at least as transformative as the mainframe or the Web and provide at least as much benefit to all Americans. Cloud computing represents a powerful new way to provide computing power and storage—and it will unleash huge new opportunities for companies and citizens able to harness it.

Cloud computing¹ is based on a simple idea. By allowing computer users to tap into servers and storage systems scattered around the country and around the world—and tied together by the Internet—cloud service providers can give users better, more reliable, more affordable, and more flexible access to the IT infrastructure they need to run their businesses, organize their personal lives, or obtain services ranging from entertainment to education, e-government, and healthcare. Most Americans already use cloud computing in one form or another to do email or back up the files on their laptop or smartphone. Most social networking sites and thousands of e-commerce sites (large and small) are running in the cloud. Cloud computing is not a technology of the future; it is already being used for business and government applications worldwide.

On the other hand, cloud computing does represent a fundamental shift in how computing is accomplished. The cloud is not only a new way to more easily and cheaply get the computing power needed to do what companies and individuals are doing today; the cloud, like the Web, will also generate new business models and drive companies to reorganize and change the way they go to market, team with partners, and serve their customers. It will enable companies (and governments) to move faster and be more responsive and flexible.

Companies will be able to try several prototypes at once, test their limits, and then build and deploy new, better prototypes—all within a few weeks. This may be the most important benefit of the cloud—it enables companies of all sizes and in all sectors, as well as governments, non-profits, and individuals, to more quickly build new applications and services by reducing the cost and complexity of deploying and managing IT resources. However, that requires cloud providers to make services simple and easy to use and deploy, and it requires that cloud customers make the effort to understand the new capabilities clouds can provide.

¹ The National Institute of Standards and Technology, in consultation with industry and government, has drafted a definition of cloud, including descriptions of the essential characteristics, service models, and deployment models. See http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

Most companies and organizations spend the vast majority of their IT budget just maintaining their current infrastructures and the applications that run on them. The cloud will enable them to devote more resources and talent to creating new products and services and improving productivity.

This democratization of innovation is a huge opportunity for people, organizations, and countries around the world. To maintain its competitive position, the United States must focus on quickly and effectively harnessing the full power of cloud computing, leading in both the deployment of cloud and the development of new cloud services. This will help American companies generate high-paying jobs and compete in the global marketplace.

Whether the United States will benefit as much from this new phase in the evolution of computing as it did from the mainframe and the Web depends upon many factors. Will the iconic U.S. companies that have pioneered and promoted the cloud continue to lead in the development of cloud services? Will companies embrace cloud computing and take advantage of the capabilities it provides? Will the public sector be able to move to the cloud? Will individuals be comfortable with their data and software located in the cloud rather than on a device in their hand? Will government policies—both in the United States and abroad—facilitate deployment of and innovation in cloud services? We firmly believe that the answer to all these questions can and should be an unequivocal YES.

We are convinced that cloud computing is developing extremely rapidly, much like the Web did in the 1990s, and will have a major impact on computing and the economy. How cloud computing develops will be shaped by key choices and policy decisions that will be made over the next two or three years. It is critical that industry and government work together to make the right choices.

In some cases, the U.S. government may choose NOT to take action and allow market forces to guide the evolution of the digital economy. U.S. national policies that conflict with those of other countries, even if designed to achieve worthy goals like security or consumer protection, could end up constraining how the cloud develops or discouraging investment in new cloud services and applications.

The most effective way for governments to shape the evolution of the cloud is not through law and regulation but by being smart users of the technology. This is particularly true in the area of security, where some government agencies have especially challenging requirements. As agencies work with industry to ensure that the cloud services deployed are at least as secure and trusted as the IT systems in use today, the agencies can provide a model that cloud customers in governments and corporations around the world can emulate.

This report provides recommendations for government, including the White House and key Federal agencies, on how they, in cooperation with industry, academia, and other nations, can (1) adopt policies that will foster development and growth of the cloud and (2) deploy the cloud

effectively, making government work better, cheaper, and smarter. These recommendations cover a lot of territory but focus on four areas: Trust, Transnational Data Flows, Transparency, and Transformation. Responsibility for success also lies with cloud providers, and the Commission makes specific recommendations to providers throughout the report. The report also includes a “Buyer’s Guide” that advises Federal agencies on how to accelerate adoption of cloud services.

TRUST

The first step in accelerating the adoption of the cloud and driving U.S. leadership in cloud innovation is earning the trust of current and potential cloud users. Trust in the cloud is a result of a combination of factors that enable individuals and organizations consuming cloud services to be confident that the services are meeting their computing needs. These needs include security, privacy, and availability; the factors that contribute include transparency of practices, accountability, resiliency and redundancy, access and connectivity, supply chain provenance, life cycle integrity, and governance.

Cloud computing is the natural evolution of IT, and it will continue to evolve. Similarly, enabling trust in the cloud is an evolution—trust is not a static state, and cloud services are not static deployments. As cloud computing evolves, one element that will enable trust is the monitoring of characteristics that impact the quality of cloud service delivery and continuity. Monitoring can expose what is happening in a cloud deployment, and, coupled with systems for analysis, improvement, and accountability, can help enable trust in the functioning and security of the cloud.

Risk management is an important element of enabling trust because it is integral to the process of monitoring and accelerating cloud adoption and implementation in the short term. Risk management capabilities need improvement for enterprises adopting cloud services, for communications providers connecting cloud services to people, for cloud service providers, and for application providers. Areas relevant to the cloud include review of current and emerging standards, industry best practices, understanding risk simultaneously at a system level and asset level, risk transfer in cyberspace, methods for assessing and meeting security needs of data whose sensitivity varies over time, and mitigation of abuse of cloud assets.

This Commission believes that trust is a ubiquitous concept, central to cloud adoption and U.S. leadership. Enabling trust, as with all of the recommendations, is an incremental process and should not become a reason to resist moving to the cloud. The Commission recognizes that enabling trust is a pillar of cloud adoption and notes that recommendations in subsequent sections of this report also support enabling trust in the cloud.

In recent months, senior U.S. officials have described threats such as cyber crime and state-sponsored industrial espionage as outpacing many enterprise defenses. In this evolving cyber threat environment, the commission believes that cloud security services and solutions, if done correctly, may provide improved security relative to non-cloud environments.

Recommendation 1 (Security & Assurance Frameworks): Government and industry should support and participate in the development and implementation of international, standardized frameworks for securing, assessing, certifying and accrediting cloud solutions.

The Commission recommends that cloud-computing service providers collaborate with the National Institute of Standards and Technology (NIST), relevant associations and standards bodies to assess and evolve current best practices and standards, to strengthen cloud security metrics, and to facilitate information sharing.

Best Practices and Standards: Collaboration on best practices and standards should focus on identifying and addressing gaps in relevant domestic and international best practices and existing standards related to security, privacy, transparency, and accountability with respect to delivering trusted cloud computing services. The best practices and standards should be assessed in the context of the industry segments served by their respective provider types.²

In order to implement applicable best practices and standards around security and information assurance, the Commission supports the efforts underway on programs such as the Federal Risk and Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP).

FedRAMP is a voluntary, General Services Administration (GSA) led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The Commission believes that a well-defined FedRAMP framework will help accelerate the adoption of cloud in the Federal Government. The NIST SCAP is a standard that enables the automation of reporting and verifying IT security control parameters. SCAP provides a ready method to capture, test and continuously monitor the controls and integrity settings required to achieve the respective standard and/or compliance requirements.

Metrics: The Commission believes that cloud-related security metrics are critical for establishing a basis for trust in the cloud and recommends that industry collaborative efforts also address security measurement frameworks. Security measurement frameworks should include relevant security metrics that will allow potential customers to compare and select appropriate security levels for their cloud services. For example, a standard set of risk-based performance measures weighted and tailored for relevance to needs and matters of importance to each customer would enable potential customers to determine the appropriate security levels for their workload and data.

² Examples include the International Standards Organization (ISO 27001/27002), NIST (SP-800-53), and the Payment Card Industry Security Standards Council (PCI DSS)

Security metrics efforts should build upon industry and academia initiatives already chartered to address standard cloud performance measurement frameworks. Examples of such initiatives include the Carnegie Mellon University Cloud Service Measurement Initiative Consortium (CSMIC), the Distributed Management Task Force's (DMTF) Cloud Management Working Group, and the Cloud Security Alliance (CSA). This is also an opportunity to build on similar efforts of government agencies to develop standards, best practices, and key performance indicators (KPIs), such as in the work underway at NIST, the National Security Agency (NSA), GSA, and the Federal CIO Council.

To foster the development of measures and metrics, these collaborative efforts should also promote educational and research programs around cloud security. These types of frameworks and tailored criteria will allow public sector organizations to develop specifications pertinent to government and help formulate procurement guidance for cloud services.

By establishing and adopting standardized frameworks for securing, assessing, certifying, and accrediting cloud systems, cloud providers can deliver a higher level of transparency and trust to consumers. Transparency of real-time status and performance metrics associated with the confidentiality, integrity, and availability of cloud systems will further contribute to enhanced trust and confidence in secure cloud services.

Information Sharing: As the cloud is deployed by federal agencies and businesses in multiple sectors, cloud-related security issues will become an important element of the overall security discussion for those communities. The Commission therefore recommends that cloud expertise be integrated into existing information-sharing structures, such as the Information Sharing and Analysis Centers (ISACs) and the Sector Coordinating Councils.

Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites.

Mechanisms to provide identity, authentication, and attribution in cyberspace are essential to accelerating adoption of cloud computing services and improving trust in the cloud. (For example, identity management facilitates access verification, billing, law enforcement access, and other features and capabilities.) Two characteristics of a robust identity management ecosystem are (1) enabling higher level transactions to occur electronically and (2) enabling credentials to be utilized across multiple services and websites. For the cloud, these have two benefits. First, a more robust authentication system would facilitate the transition of a wider variety of workloads and interactions to cloud services. Second, multi-use credentials would facilitate interoperability and allow customers to assemble the systems most appropriate for their workloads. In this case, a community of identity management systems will enable

seamless transitions when data, processing tasks, and other applications reside on different platforms at different service providers with different access control requirements, or when cloud services have to integrate with traditional IT systems.

The need for identity management capabilities is not new or unique to the cloud, and there is an opportunity to build on existing initiatives and innovation underway in this area. The National Strategy for Trusted Identities in Cyberspace (NSTIC, <http://www.nstic.us/>), released in April 2011, is aimed at developing a broad, private-sector led, identity management ecosystem that enables the identification and authentication of the individuals, organizations, and underlying infrastructure involved in an online transaction. The Commission endorses NSTIC's goal of facilitating creation and broad deployment of identity capabilities, and the adoption of cloud services by business and government will provide additional opportunities and motivation for development of this identity ecosystem.

In addition to supporting the development of a private-sector led identity management ecosystem, the Commission also suggests specific steps that the Federal Government could take as a user of cloud services that would contribute to advancing robust identity management:

- Deploy, as appropriate, multi-factor authentication for Federal cloud applications as used by Federal personnel and government contractors doing government contract work
- Accelerate the adoption of strong authentication, including multi-factor authentication and one time passwords, to enable mobile access to secure Federal cloud services and websites

These actions are important because implementation of strong authentication will increase resilience of the cloud ecosystems. The Commission notes that the adoption of cloud technologies in the Federal Government continue in parallel with the coordinated development of these recommended systems rather than wait for a particular identity management solution.

The two preceding recommendations address some aspects of security and trust in the cloud; while security is certainly a critical element of trust in the cloud, it is not the only element. Good security is a continuous effort. This is true for all IT systems, not just the cloud.

A hypothetical target of perfect or near perfect security should not be used as an excuse for failing to use the cloud. Instead, the focus should be on whether the cloud provides security as good as or better than in-house IT deployments. The Government should, of course, always seek to enable continuous improvement of security and the human and technical systems that connect to the cloud. This point is consistent with the discussions and recommendations throughout this report, such as those on monitoring, measuring, and information sharing; on risk assessment and management; on the importance of policies, people, and practices; and on research.

Recommendation 3 (Responses to Data Breaches): Government should enact a national data breach law to clarify breach notification responsibilities and commitments of companies to their customers, and also update and strengthen criminal laws against those who attack computer systems and networks, including cloud computing services.

Cloud services, like existing IT systems, will be the target of malicious actors. In addition to defending against attacks, the Commission notes that clarity around what should happen in the event of a data breach will serve both cloud consumers and providers. Timely notification and transparency to customers (individuals, organizations and governments) enables rapid response and the opportunity to minimize damage. Also, cloud service providers and law enforcement should have the tools needed to take action against criminal activity against clouds, such as breaching of data.

Specifically, the Commission recommends a national data breach law to streamline notifications and make it simple for customers to understand their rights with regard to notification. Such a law should include preemption of state laws to provide for harmonization. In addition, the law should take into account the various types of entities that are involved in processing the covered data cloud service providers, industry, government, nonprofit organizations, academic organizations, etc., and specifically provide that notice should be given by the entity that has a direct relationship with the parties whose information was subject to the breach. Finally, the law should have notification requirements based on risk of harm.

Note that the motivation for such legislation is not limited to cloud computing, but adoption of cloud computing would benefit from this action. Specifically, by clarifying responsibilities and commitments around notification, the law will enable cloud providers to prepare to take expected steps in case of a breach and enable customers to trust the providers to do so.

As a complement to the above recommendations, the U.S. government should update and strengthen criminal laws against those who attack our cyber infrastructure, including cloud computing services. In addition to clarifying cyber criminal offenses and defining penalties, the Federal government must commit adequate resources and personnel to investigating and tracking down cyber criminals. As much of cyber crime is transnational, the Federal government should promote further international cooperation around cross-border prosecutions and identifying countries affording safe havens to such criminals.

Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda.

The Commission recommends that government, industry, and academia take responsibility for developing and carrying out a research agenda that will promote U.S. leadership in the cloud by enabling innovation that benefits customers and service providers. Relevant cloud-oriented

research areas include, but are not limited to, usability, privacy, availability, integrity, confidentiality, security, cryptography, identity management, energy efficiency, resource allocation, portability, and dependability.

In conducting research on the cloud, industry should undertake short- and medium-term research where practical impacts are clear and investment risk is lower. Government research agencies, like the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA), should fund universities and other organizations to conduct long-range research activities, including those that build educational and research capacity and high-risk, high-reward projects. Cooperative cloud test beds will also be a critical element in advancing the overall evolution of cloud technologies.

Cloud technology has matured rapidly and will continue to develop. This recommendation should not be perceived as concern about cloud's current capabilities but rather as an investment in ensuring that the U.S. maintains a leadership role in the development, commercialization, and deployment of new cloud technologies and the expansion of cloud to new workloads, sectors, and activities. Basic research investments a decade ago yielded the ideas, technologies and capabilities that are fueling today's cloud developments. Continued innovation in the cloud will benefit directly from a sustained research agenda.

TRANSNATIONAL DATA FLOWS

The development and use of latest-generation information and communication technologies has allowed organizations and individuals to operate cloud-based services in any location around the world. The expansion of trade and business operations on a global level has also brought new challenges for operating in the global market. The globalization of business and trade through technology has resulted in multi-directional data flows and an exploding volume of data sources and stakeholders. This adds complexity to cloud adoption because of the data, process, and people residing on multiple continents with different laws and cultures. Despite these challenges, transferring data is an integral part of the cloud and must be addressed.

The recommendations classified within Transnational Data Flows address the need for collaboration across national borders and the need for international frameworks to standardize the process. The Commission believes that recommendations to promote privacy frameworks, utilize performance-based criteria over proxy criteria that do not reflect specific and measurable attributes, and actions that overcome real and perceived challenges of transnational data flows are critical for the U.S. to adopt and lead in cloud computing. These actions are important because the United States must act as both a consumer of the cloud and as a leader in cloud innovation and markets. If the United States does not take a proactive position in both of these roles, the potential of a powerful global cloud market that enables individuals, industries and governments to innovate rapidly may not be fully realized.

Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks.

The Commission recommends that the U.S. build upon the work of existing, accepted privacy and data protection principles-based frameworks such as the Organization for Economic Cooperation and Development (OECD) and/or Asia-Pacific Economic Cooperation (APEC) to develop and promote a comprehensive, technology-neutral privacy framework. The existing U.S. laws are sector specific and state specific, and this approach is different than those in other regions (e.g., Europe). In some quarters, there is a concern that this may impede the transnational flow of data with other countries, especially those in Europe. These actions would help provide the certainty and flexibility required for continued cloud innovation and would be a step toward fostering a global market for cloud services. Industry should embrace such frameworks and utilize them to the fullest extent practicable.

Concepts of privacy are evolving in the Internet age, when information seldom has a single physical location, and duplication and sharing can occur quickly and easily. In addition, expectations around the norms and goals associated with privacy differ by culture, generation, and other factors. In this environment, the above recommendation is designed to demonstrate that the U.S. and U.S. companies take privacy seriously and to provide a basis for international discussions around mechanisms to resolve conflicting privacy policies. Such actions will also help overcome misunderstandings and confusion around the U.S. position on privacy; where uncertainty may be causing multinational and foreign organizations to avoid U.S.-based clouds or cloud computing altogether.

Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud.

The Commission recommends that the U.S. modernize legislation governing law enforcement access to digital information in light of advances in IT in general and the cloud in particular. Reform of the Electronic Communications Privacy Act (ECPA) is critical to clarifying the legal conditions under which U.S. cloud providers and their customers will operate, as technology changes have overtaken many aspects of ECPA as originally written. Various groups such as the Digital Due Process Coalition have proposed making government access to data stored in the cloud consistent with government access to data stored in in-house IT systems.

The U.S. Department of Commerce should conduct a study to assess the impact of the USA PATRIOT Act and similar national security laws in other countries on a company's ability to

deploy cloud in a global marketplace. This action may provide insights into how best to address the uncertainty and confusion caused by national security statutes (e.g., PATRIOT Act³ and similar laws of other nations) that are perceived as impediments to a global market place for cloud services.

In addition, the U.S. government should take the lead on entering into active dialogues with other nations on processes for legitimate government access to data stored in the cloud and processes for resolving conflicting laws regarding data. These discussions should build on existing agreements and arrangements with other nations (e.g., expedited Mutual Legal Assistance Treaties and bilateral and multilateral agreements).

These three steps all will contribute to increasing clarity around the rules and processes cloud users and providers should follow in an international environment. Without U.S. leadership and cooperative international efforts, the world will face a far more complex legal environment, one that is not conducive to fully leveraging the cloud.

Recommendation 7 (E-Discovery and Forensics): Government and industry should enable effective practices for collecting information from the cloud to meet forensic or e-discovery needs in ways that fully support legal due process while minimizing impact on cloud provider operations.

Critical to improving trust in the cloud and accelerating adoption is the need for best practices in collecting forensic data and information in ways that do not result in significant, adverse impacts on individuals and/or organizations using the cloud-based information. To address this, the Commission recommends that the Federal CIO work with applicable agencies such as U.S. Department of Justice and other relevant organizations to establish best practices specifically addressing acceptable methods for collecting forensic evidence from organizations using cloud-based information systems. In addition, cloud providers should assist their customers (e.g., individuals, commercial entities, government) with technologies to facilitate e-discovery and information retrieval requirements, whether in support of regulatory compliance or litigation activities.

Specific issues that will need to be addressed include methods to facilitate cooperation among service providers, how best to maintain a verifiable chain of custody, how best to collect data from proprietary technologies, and how best to minimize service availability impacts resulting from seizures of data and equipment. Improving the processes and practices around evidence collection and forensics will improve cloud customers' confidence in continuity of service and

³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

their ability to meet legal requirements. It will also provide tools to support the tracking and prosecution of cybercriminals (as discussed in Trust Recommendation 3).

Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads.

This recommendation highlights the role of the U.S. Government both as a customer of cloud services and as a leader in enabling trustworthy use of the cloud.

Government agencies, in evaluating potential models for using the cloud, should not assume or default to the notion that no government workload and/or task is suitable for cloud computing environments in other countries. Instead, they should carefully consider the types of data and tasks within their information and communications technology portfolios to match suitable workloads to the cloud computing models that achieve the required level of confidentiality, integrity, and availability at the appropriate levels of efficiency, cost, and redundancy. Evaluation of the specific workload and/or task needs is necessary to determine suitable potential cloud computing environments and models.

By evaluating cloud services based on the performance needs of specific workloads, the U.S. Government can show leadership in the adoption of approaches that recognize the multiple factors that contribute to ensuring trust in the cloud (see discussion around Trust Recommendation 1). The development of the frameworks, best practices, metrics, and standards to enable this approach should help businesses and other governments take a similarly comprehensive approach to trusted cloud deployment.

While the Commission is not declaring that no circumstances exist in which certain types of Federal data could be limited to U.S. storage, it is critical to understand that location is but one factor in the security of information, and location should not be viewed as a proxy for security in the cloud. For example, effective use of security technologies, including technologies to make data unreadable and unusable, is as important, if not more important than location in enhancing the security of data in the cloud.

Cloud providers typically locate data centers based on a variety of factors, including technical issues like network topology, economic issues like the price of electricity, and business issues like proximity to markets. Once data centers have been built, however, the storage and processing of data can occur in multiple data centers and across geographic boundaries and legal jurisdictions. For some customers and workloads, the preference might be to allocate storage and processing locations based on technical and economic factors (perhaps to maximize speed, or minimize cost). For other customers and workloads, there may be concerns about data touching certain legal jurisdictions that impose data handling requirements around privacy, retention or other legal or regulatory burdens.

To service customers with such concerns, cloud providers could enable the setting of policies around specific data and workloads to control what legal jurisdictions those data or workloads may enter and enable tags to carry provenance attesting to those locations. (The discussion above about the need to conduct international dialogues on methods for resolving inconsistent rules between countries is also a critical step toward dealing with these concerns.)

The Commission encourages adoption of approaches that give cloud providers the flexibility to develop and deploy services for a diversity of workloads in innovative ways, rather than constrain cloud services by geography. This will allow users, when appropriate, to take advantage of the potential benefits in access, reliability, resiliency, efficiency, and costs that can result from geographical distribution of workloads.

TRANSPARENCY

U.S. leadership in the cloud will be facilitated if cloud providers make a firm commitment to transparency. Transparency in the context of cloud computing requires vendors to share relevant information about their capabilities, offerings, and service levels.

Transparency by cloud vendors will encourage the shift to the cloud by addressing some of the primary reasons Federal agencies and commercial companies do not move to the cloud: uncertainty about how systems outside of their control will perform and fear of being unable to access or move their data. We offer two recommendations specifically designed to allay these concerns by ensuring customers maintain control over the performance of their systems and access to their data while still realizing the cost, efficiency, and scalability advantages of cloud computing.

Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and Government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use.

The Commission recognizes the need for information and tools that provide users with meaningful ways to evaluate the characteristics and performance of various cloud implementations, whether they are contemplating deployment or evaluating performance of their current services. Development of metrics around key cloud attributes should be driven by user needs and provider capabilities. The Government and commercial sector should collaborate on lessons learned, and each should be careful to avoid dominating the development of these metrics. Different Government and business sectors will likely demand different measures and tools.

Currently, the lack of transparency and standard metrics make it difficult for customers to compare the cloud offerings of different providers. Unsure about what they are being offered and unclear on the differences among the cloud options available, many customers hesitate before moving to the cloud or decide to delay moving to the cloud until there is agreement on common metrics that facilitate easy comparison of cloud providers. The Commission encourages industry to work with the appropriate government agencies to create customer tools that make “apples-to-apples” comparisons possible among different cloud providers and the services that they provide. This will increase the confidence commercial and government customers have in moving to the cloud and will accelerate cloud adoption.

Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices.

One benefit of the cloud is its ability to store and process large quantities of data. For customers making the transition to cloud, this often raises questions about how they access or move that data, especially in cases where they are switching between cloud providers. Data portability can be achieved in a variety of ways, and cloud providers should be transparent about their conformance with industry standards and best practices as well as the documents, tools, and relevant third-party solutions they make available to their customers. Customers should recognize that early consideration of data portability in selecting and implementing cloud services can reduce the risk of vendor lock-in.

A collection of data portability standards, formats, and practices is vital to encouraging widespread cloud adoption. Government and industry should collaborate on facilitating the rapid development and dissemination of these standards and other relevant tools. The collaboration between NIST and the private sector in preparing the NIST standards roadmap

under the Federal Cloud Computing Strategy is an excellent example of these types of efforts. This work should serve as a model for future efforts around data portability and could be extended to other facets of cloud including workload and application portability. Both Government and industry should continue to emphasize open, multi-vendor, unencumbered standards and best practices.

TRANSFORMATION

Cloud computing is a disruptive technology that has significantly changed the IT landscape. Although cloud computing offers many benefits to adopters, it also poses challenges to Federal agencies and commercial organizations that are trying to adapt to the technological changes ushered in by the cloud. To achieve the benefits offered by cloud computing, Government and industry need to be open to re-envisioning the role of IT and willing to make the investments necessary to harness the power of the cloud.

The first two recommendations in this section focus specifically on actions that the Federal government can take to facilitate the transition to cloud. By stepping forward as a leader in the adoption of cloud computing, the Federal Government can play a key role in driving innovation and economic growth in the IT industry and demonstrate that it considers the cloud an important, effective, safe and secure environment. The second two recommendations focus on the transformation in infrastructure and workforce that are necessary for widespread cloud adoption.

Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions.

In interviews with senior Government officials, the Commission found that the current Federal Acquisition Regulations (FAR) do not need alteration for agencies to acquire cloud services. The FAR is already flexible enough to allow agencies to acquire IT as a service. However, agencies should demonstrate flexibility in adapting current procurement models and existing contracts to take advantage of new cloud offerings.

One of the biggest challenges agencies may face in budgeting is predicting the costs of cloud computing over the course of a fiscal year. Cloud computing is designed to scale quickly to a customer's needs, providing maximum flexibility to the user. If the cloud service is based on a predictable subscription model (such as a standard monthly fee per user), these budget projections can be easily accommodated. If the cloud service is based on pay-as-you-go usage, however, it can be difficult to predict costs unless the user can precisely forecast future computing needs. To address this challenge, the Commission recommends that the current efforts to update and streamline the OMB 300 exhibit form and associated budget scoring include tools that facilitate and encourage the new business models associated with cloud. OMB and Congress should communicate to agencies that it recognizes budgeting for cloud is not like budgeting for traditional IT services and should assure agencies it will provide support and flexibility during and after the transition to the cloud.

To help agencies acquire cloud services, the Commission also recommends Congress and OMB demonstrate flexibility in changing budget models. Agencies currently face challenges transitioning funds between capital expenditure (also known as acquisition) accounts and operations and maintenance expenditure accounts when adopting and implementing cloud services and solutions. Most in-house information systems rely upon funding from capital expenditure accounts, while cloud services and solutions do not have intensive capital expenditures and are funded more from the operations and maintenance expenditure accounts. Agencies today, however, are hampered and even prevented from transitioning funds from the capital expenditure accounts to the operations and maintenance expenditure accounts, even when there are overall savings to be realized by the shift in IT approaches that requires the transition of the funds. This creates a disincentive for agencies to really drive savings and efficiencies through adoption of cloud services and solutions. Government must find ways to provide more flexibility for agencies to reduce and transition funds in the capital expenditure accounts to the operations and maintenance expenditure accounts as part of implementing innovative cloud solutions and achieving savings.

In making decisions about budgeting and acquisition, Federal agencies, through the CIO Council, would benefit from sharing best practices, tools for objective analysis of cloud performance, and ways to predict and document different contributors to the budgetary impact of switching

to the cloud. To ensure that the CIO Council can provide this support to Federal agencies, it should include experts from a wide array of communities, including chief financial officers, chief acquisition officers, human capital officers, and program managers. Additionally, staffing OMB's other councils, such as the CAO and CFO Council, with cloud expertise could ensure these councils can also provide support to agencies implementing cloud.

As agencies are creating their business cases and preparing to move to the cloud, it is important to remember that the adoption of cloud is a multi-stage process. Initial deployments by government may not take full advantage of the potential capabilities and benefits of the cloud, but these steps are necessary for customers to explore new (and sometimes fundamentally different) approaches to selecting, acquiring, and utilizing IT. When agencies are in a transition to the cloud, it is critical that they take care that the policies and standards of the cloud provider do not lock the agency into an early deployment model. Agencies should require that policies be flexible enough to allow evolution of use and innovation through the adoption of new infrastructure, services, and applications.

Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments.

Adopting a new technology can be difficult, and the transition of agencies to the cloud will require investment of time, resources, and political will by the Federal government. In recognition of this, the Commission recommends that OMB establish incentives and provide support for agencies beginning cloud adoption.

On the fiscal side, agencies may be hesitant to undertake a significant change to their IT structure during a time of budgetary constraint or may have difficulty finding and justifying the costs associated with an IT transition. One possible incentive is to allow agencies to retain and redirect a portion of the overall budget savings realized from cloud adoption. Another approach is to provide seed money to agencies that help with the initial investments required in moving to the cloud.

OMB could also support agencies in the cloud transition by providing assistance in the processes that govern the transition. OMB and GSA assistance on moving from static to more dynamic assessment and authorization processes, change management, and compliance with OMB guidance would help facilitate the transition.

In addition to financial support and process assistance, public recognition and praise for agencies that are early adopters of cloud computing or deploy the cloud in particularly innovative ways is important. Individuals within agencies who have played key roles in enabling a cloud transition should also be recognized with service or financial awards. This sort of public support should be complemented by public acknowledgement by agency and Administration

leadership that there are risks inherent in adopting a new technology infrastructure; this would provide some support for agency staff during the process of implementing the cloud transition.

Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services.

The Commission recommends that the Federal government and industry continue to expand deployment of high bandwidth networking, enhance network resilience, and advance IPv6 adoption to ensure ample broadband connections.

The Commission recommends government and industry initiatives designed to increase the deployment and adoption of both wired and wireless broadband, especially to underserved areas of the country. Efforts such as those advocated in the Federal Communications Commission's National Broadband Plan, including making additional spectrum available and expanding opportunities for opportunistic and unlicensed spectrum use, are necessary to allow cloud computing to function effectively and for businesses and citizens to realize the benefits of innovative new cloud technologies.

With rapidly rising demands for connectivity, the last batch of IPv4 addresses, assigned earlier this year, is unlikely to meet demand beyond the end of 2011. Since cloud computing depends on the connection of many individuals, devices, and locations, a quick transition to IPv6 is vital to ensuring the successful adoption and operation of cloud computing in the future. The Commission applauds the Government's move to enable the use of IPv6 on external servers by October 2012 and on internal networks by 2014.

Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services.

The transition to the cloud will require new capabilities for a variety of communities. The business community (and agency leaders) will need to understand how cloud changes the economics of their IT expenses and provides new capabilities through which to carry out their lines of business (or agency missions). Acquisition workforces will need new skills to gather and assess the information necessary to make informed purchasing choices. The responsibilities of IT workforces will expand to manage new cloud capabilities and, within cloud customers, the IT expertise needed will evolve as activities such as operations, maintenance, and development are shared or shifted to cloud providers.

Acquisition Workforce: The Commission commends GSA's outreach efforts to Federal agencies to provide materials, expertise, and support around investigating, procuring, and deploying cloud solutions. GSA could build on this work by creating a cloud educational portal to help

agency buyers, architects, administrators, and end users in understanding all aspects of cloud computing. Resources for this portal might include white papers, articles, and training materials.

IT Workforce: Government, using existing programs in technology education and workforce training,⁴ can facilitate and encourage academic institutions and educational organizations to develop and offer courses relevant to cloud, in partnership with industry. Industry and academia can help develop curriculum relevant to new technologies and skills (in partnership with the educational institutions and organizations), and support employee retraining.

Workforce education should embrace a spectrum from informal outreach to disseminate introductory or reference materials to targeted courses in specific skills and areas to integration of cloud-related topics into overall curricula in formal programs in computer science and engineering, project management, business schools, and other relevant areas. On the informal side, outreach to IT professionals could disseminate information about cloud issues, skills, and opportunities. Within the government, outreach and support networks for acquisition personnel would provide an opportunity to share experiences and best practices.

⁴ The Department of Labor, the Department of Education, and the National Science Foundation all have programs in technology education and workforce training that might support activities relevant to cloud computing.

CONCLUSION

In a time when the government is seeking to do more with less and the commercial sector is being called upon to create jobs and grow the economy, now is the time to act on the cloud. Cloud computing has ushered in vast improvements in the cost, agility and efficiency of computing. These benefits alone drive a strong business case; however, the more compelling return is the opportunity to leap forward; to discover new markets and improve how we interact with, serve, and support U.S. citizens, users and other nations. The cloud holds the potential to unlock widespread entrepreneurship of all shapes and sizes, and expand the scope to do entirely new things — innovations such as social networking, which we could not fully imagine just a decade ago, would not exist without IT's continued evolution to the cloud.

Despite the clear benefits of cloud computing, many challenges impede its widespread adoption. These challenges face both those ready to embrace the cloud and those grappling with doubts about making the move. Those who are ready address challenges such as training acquisition personnel and determining which workloads should be moved to the cloud; those who are hesitant have concerns about, for example, the security of and control over data stored and workloads processed in the cloud. If unaddressed, these challenges threaten to slow the acceptance of cloud computing and delay the enormous advantages and opportunities it provides. To address the challenges and allay concerns, the Commission has offered in this report a range of practicable recommendations; these show the way forward to those ready to adopt the cloud, and guide cloud providers and users in addressing the issues of those not yet prepared to shift.

The Commission recognizes that industry and government share responsibility for enabling cloud's adoption and for leading in the cloud evolution. Reflecting the urgency to provide incremental movement, create momentum and lead through actions, many of the recommendations target short-term tactical and operational advances. Complementing these are longer term recommendations that reflect the strategic importance of the evolution, and the mandate to look beyond the cloud we know today, to the opportunities it creates for the future.

It is the hope of this Commission that the Federal Government, industry and academia will implement these recommendations and be leaders in shaping how the future unfolds through the adoption of the cloud across the United States and around the world. Furthermore, these recommendations should demonstrate that cloud computing is not a new technology that needs further validation or analysis before it can be safely adopted; it is a natural evolution in computing. Those who recognize this and take early advantage of the benefits it offers will, in the coming decades, be the leaders not in only IT but in driving the cloud's evolution, and therefore, in driving business and mission results.

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
<p>Recommendation 1 (Security & Assurance Frameworks): Government and industry should support and participate in the development and implementation of international, standardized frameworks for securing, assessing, certifying and accrediting cloud solutions.</p>	•	•			•
<p>Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites.</p>	•	•		•	
<p>Recommendation 3 (Responses to Data Breaches): Congress should enact a national data breach law to clarify breach notification responsibilities and commitments of companies to their customers, and also update and strengthen criminal laws against those who attack computer systems and networks, including cloud computing services.</p>		•		•	
<p>Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda.</p>	•	•	•		•
<p>Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks.</p>		•			•

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
<p>Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud.</p>		•		•	
<p>Recommendation 7 (E-Discovery and Forensics): Government and industry should enable effective practices for collecting information from the cloud to meet forensic or e-discovery needs in ways that fully support legal due process while minimizing impact on cloud provider operations.</p>	•	•		•	
<p>Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads.</p>		•			•
<p>Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and Government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use.</p>	•	•		•	
<p>Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices.</p>	•			•	

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
<p>Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions.</p>		•		•	
<p>Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments.</p>		•			•
<p>Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services.</p>	•	•		•	
<p>Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services.</p>	•	•	•	•	