Anexo XV

SUMMARY REPORT OF THE

COMMISSION ON THE LEADERSHIP OPPORTUNITY IN U.S. DEPLOYMENT OF THE CLOUD (CLOUD2) (*)

(*) Co-Chairs : Marc Benioff, Salesforce.com and Michael Capellas, VCE
Academic Co-Chairs : John Mallery, MIT , Michael R. Nelson, Georgetown
Vice-Chairs: Dan Reed, Microsoft and Jim Sheaffer, CSC

SUMMARY OF CLOUD2 REPORT

A single, massive cloud data center contains more computers than were on the entire Internet just a few years ago. A rich and diverse set of new devices is creating new models for content creation and access. Information technology (IT) companies are combining infrastructure, platforms, and services in new ways to transform the way computing resources and capabilities can be bought, delivered, and used. These changes are creating opportunities for businesses, governments, and individuals to tap the flexibility and power of the cloud to create new products, generate new market opportunities, deliver services more effectively and cost-efficiently, and change the way they interact with each other.

This report provides recommendations for facilitating the development and deployment of cloud services, with the ultimate goal of fostering innovation and economic growth, ensuring U.S. competitiveness, and creating jobs. The Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD2), a collaborative effort of 71 members primarily from industry, developed these recommendations at the encouragement of the Federal Chief Information Officer and the U.S. Department of Commerce. The recommendations focus on how the U.S. government, in cooperation with industry, academia, and other nations, can (1) adopt policies that will foster the development and growth of the cloud and (2) deploy the cloud effectively, making government work better, cheaper, and smarter. In addition, the Commission developed a "Buyer's Guide" that provides guidance to the Federal agencies on issues to consider in evaluating and implementing cloud services.

This report reflects a growing imperative to fully embrace and capitalize upon the power of cloud computing. As 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 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.

ACTIONABLE RECOMMENDATIONS — TRUST, TRANSNATIONAL DATA FLOWS, TRANSPARENCY, AND TRANSFORMATION

As the Commission was defining the key elements and questions that occur around the transition to cloud, four themes emerged -- Trust, Transnational Data Flows, Transparency, and Transformation -- and we have grouped the recommendations accordingly. The transition to cloud computing will involve technology, policies, people, and processes, and the themes and recommendations touch on all of these.

TRUST

Trust in the cloud results from a combination of factors that enable individuals and organizations consuming cloud services to be confident that the services are meeting their computing needs, including security, privacy, and availability. To facilitate trust, the Commission makes four recommendations in this area:

TRUST - 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.

This recommendation builds on efforts by cloud providers, the National Institute of Standards and Technology (NIST), relevant associations and standards bodies to assess and evolve current domestic and international best practices and standards as they pertain to delivering trust in the cloud, including in areas related to security, privacy, transparency, and accountability. It also complements Federal efforts underway on programs such as the Federal Risk and Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (S-CAP). Other recommended actions to facilitate trust in the cloud include developing cloud-related security metrics and integrating cloud expertise into existing structures that enable information-sharing related to IT security.

TRUST - RECOMMENDATION 2 (IDENTITY MANAGEMENT): INDUSTRY AND GOVERNMENT SHOULD ACCELERATE THE DEVELOPMENT OF A PRIVATE SECTOR-LED IDENTITY MA-

NAGEMENT 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.

A robust identity management ecosystem enables higher-level transactions to occur electronically and enables credentials to be utilized across multiple services and websites. The Commission notes that a more robust authentication system would facilitate the transition of a wider variety of workloads and interactions to cloud services. Also, multi-use credentials would facilitate interoperability and allow customers to assemble the systems most appropriate for their workloads.

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. The Commission also supports Federal efforts to strengthen and deploy strong authentication techniques for governmental employees and agency services.

TRUST - 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 actions to be taken 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 regarding criminal activity against clouds, such as breaching of data.

TRUST - RECOMMENDATION 4 (RESEARCH): GOVERNMENT, INDUSTRY, AND ACADEMIA SHOULD DEVELOP AND EXECUTE A JOINT CLOUD COMPUTING RESEARCH AGENDA.

Research is 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. 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. Industry should undertake short- and medium-term research where practical impacts are clear and investment risk is lower, while government research agencies, like the National Science Foundation (NSF) and the Defense Advanced Projects Research Agency (DARPA), should fund universities and other organizations to conduct long-range basic research activities.

TRANSNATIONAL DATA FLOWS RECOMMENDATIONS

The globalization of business and trade and the ability to operate cloud-based services in any location around the world has led to an exploding volume of data sources and stakeholders and the constant flow of data across national borders. This creates new opportunities but also adds complexity to cloud adoption, with data, process, and people residing on multiple continents with different laws and cultures.

TRANSNATIONAL DATA FLOWS - 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.

Existing U.S. privacy laws are sector specific and state specific. As this approach differs from that of other regions, there is concern in some quarters that this may impede the transnational flow of data with other countries, especially those in Europe. Development of a comprehensive, technology-neutral privacy framework would help demonstrate that the U.S. and U.S. companies take privacy seriously, provide a basis for international discussions around mechanisms to resolve conflicting privacy policies, and foster a global market for cloud services.

TRANSNATIONAL DATA FLOWS - 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.

Under this recommendation, the Commission suggests three steps to increase 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. The three steps are: (1) modernize legislation (the Electronic Communications Privacy Act) governing law enforcement access to digital information in light of advances in IT; (2) study the impact of the USA PATRIOT Act and similar national security laws in other countries on companies' ability to deploy cloud in a global marketplace; and (3) have the U.S. government 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.

TRANSNATIONAL DATA FLOWS - 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.

The Commission recommends that the Federal CIO work with applicable agencies, such as the U.S. Department of Justice, and other relevant organizations to establish 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. In addition, cloud providers should assist their customers with technologies to facilitate e-discovery and information retrieval requirements, whether in support of regulatory compliance or litigation activities.

TRANSNATIONAL DATA FLOWS - RECOMMENDATION 8 (LEAD BY EXAMPLE): THE U.S. GOVERNMENT SHOULD DE-

MONSTRATE ITS WILLINGNESS TO TRUST CLOUD COMPUTING ENVIRONMENTS IN OTHER COUNTRIES FOR APPROPRIATE GOVERNMENT WORKLOADS.

Government agencies 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. The development of the frameworks, best practices, metrics, and standards to enable this approach (as discussed in the Trust section of this report) should help businesses and other governments take a similarly comprehensive approach to trusted cloud deployment.

TRANSPARENCY

Transparency by cloud providers will encourage the shift to the cloud by addressing some of the primary reasons Federal agencies and companies do not move to the cloud: uncertainty about how systems not in their possession will perform and fear of being unable to access or move their data.

TRANSPARENCY - 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 and managing performance of their current services. Development of tools and metrics to facilitate comparison of cloud

services will increase the confidence of commercial and government customers in their decisions about cloud services and will accelerate cloud adoption.

TRANSPARENCY - 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. Customers making the transition to the cloud often ask how they access or move that data, especially in cases where they are switching between cloud providers. Government and industry should collaborate on facilitating the rapid development and dissemination of data portability standards, formats, and practices, and other relevant tools. Cloud providers should be transparent about how they use these tools, and cloud customers should recognize that early consideration of data portability in selecting and implementing cloud services can reduce the risk of vendor lock-in.

TRANSFORMATION

The transition to cloud computing requires changes in technology, policies, people, and processes, with associated implications for Federal acquisition, technology infrastructure, and education and training.

TRANSFORMATION - RECOMMENDATION 11 (FEDERAL ACQUISITION AND BUDGETING): AGENCIES SHOULD DEMONSTRATE FLEXIBILITY IN ADAPTING EXISTING PROCUREMENT MODELS TO FACILITATE ACQUISITION OF CLOUD SERVICES AND SOLUTIONS. CONGRESS AND OMB SHOULD DEMONSTRATE FLEXIBILITY IN CHANGING BUDGET MODELS TO HELP AGENCIES ACQUIRE CLOUD SERVICES AND SOLUTIONS.

In our 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.

However, agencies should demonstrate flexibility in adapting current procurement models and existing contracts to take advantage of new cloud offerings. 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 the cloud. Agencies also need additional flexibility from Congress and the Office of Management and Budget on transitioning funds between capital expenditure (also known as acquisition) accounts and operating and maintenance expenditure accounts when adopting and implementing cloud solutions and services. We also recommend that Federal agencies, through the CIO Council, share 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.

TRANSFORMATION - 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. This may include allowing agencies to retain and redirect a portion of the overall budget savings realized from cloud adoption, providing seed money to agencies that help with the initial investments required in moving to the cloud, and giving public recognition and praise to agencies and individuals that enable early or innovative adoption of cloud computing.

TRANSFORMATION - 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.

Cloud services rely on connectivity, including the links between customers and data centers and between devices and the Internet. The Commission supports ongoing efforts to improve the nation's connectivity infrastructure through the deployment and adoption of both wired and wireless broadband and the transition to IPv6 to ensure a sufficient supply of addresses for the exploding number of internet-connected computers and devices.

TRANSFORMATION - 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. Education and training programs should support all of these transitions.