Government Information Quarterly 27 (2010) 245–253

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Identifying the security risks associated with governmental use of cloud computing

Scott Paquette [a,*], Paul T. Jaeger [b], Susan C. Wilson [b]

[a] College of Information Studies, University of Maryland, College Park, MD 20740, USA
[b] University of Maryland, College Park, MD, USA

ARTICLE INFO

Available online 13 April 2010

Keywords:
Cloud computing
Risk management
IT security
IT governance
Grid computing
Governmental computing

ABSTRACT

Cloud computing, which refers to an emerging computing model where machines in large data centers can be used to deliver services in a scalable manner, has become popular for corporations in need of inexpensive, large scale computing. Recently, the United States government has begun to utilize cloud computing architectures, platforms, and applications to deliver services and meet the needs of their constituents. Surrounding the use of cloud computing are many risks that can have major impacts on the information and services supported by this technology. This paper discusses the current use of cloud computing in government, and the risks–tangible and intangible–associated with its use. Examining specific cases of government cloud computing, this paper explores the level of understanding of the risks by the departments and agencies that implement this technology. This paper argues that a defined risk management program focused on cloud computing is an essential part of the government IT environment.

1. Introduction

Cloud computing, which allows for highly scalable computing applications, storage, and platforms, is increasing in importance throughout government information technology (IT) strategy. Cloud computing providers offer a variety of services to individuals, companies, and government agencies, with users employing cloud computing for storing and sharing information, database management and mining, and deploying web services, which can range from processing vast datasets for complicated scientific problems to using clouds to manage and provide access to medical records (Hand, 2007). Recently, President Barack Obama and Chief Technology Officer (CTO) Vivek Kundra have both expressed the vision to explore the cloud as a key component in the federal IT transformation, and therefore agency use of cloud computing capabilities has increased (Jackson, 2009; Miller, 2009b).

Although many benefits are reported in cloud computing use, a great deal of risk is associated with the implementation, management, and use of cloud computing technologies. In a government context, both tangible risks (such as the risk of unauthorized access, infrastructure failure, or unavailability) and intangible risks (such as confidence in the technologies capabilities, and public access) are introduced along with the functionality and benefits provided by cloud applications. The government's ability to manage these risks will be a key determinant in the success of cloud computing.

This paper discusses the nature of cloud computing and risk management in a governmental context. The risks associated with cloud computing are identified, focusing on both the tangible and intangible risks which can present challenges for IT management. We argue that much evidence exists that cloud computing has become a strategic direction for many government agencies and is already employed in critical areas of the government's IT infrastructure. However, a prudent and in-depth risk management program must accompany the use of this new technology in order to prevent unwanted technical consequences, and even greater problems from a government information management perspective.

2. The nature of risk and risk management

The word "risk" is derived from the Italian *risicare*, which translates to English as "to dare." At the origin of the word is the implication that risk is not a fate, but a choice individuals make depending on internal or personal factors, and the environment in which we live (Bernstein, 1998). Others define risk as the possible impact or result of an event on assets of an organization, and the corresponding consequences that occur (Stoneburner, Goguen & Feringa, 2004). Risk is not defined or classified by the size of the risk, but by the balance of expected and unexpected consequences. In economic terms, this is known as "value at risk," which is a statistical measure that defines the consequence of a loss by the chance of occurrence or confidence level (Crouhy, Galai & Mark, 2006).

A basis for all discussions of risk is its relationship to the idea of reward. This concept is easy to define and observe with risks associated with market-tradable instruments, as a cost of the risk is determined by the market and is easily compared to the expected rewards. More often, a challenge exists for organizations when the risk cannot be associated with a well-understood or widely-accepted cost. In this case,

* Corresponding author.
E-mail addresses: spaquett@umd.edu (S. Paquette), pjaeger@umd.edu (P.T. Jaeger), scwilson@umd.edu (S.C. Wilson).

0740-624X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.giq.2010.01.002

organizations are susceptible to engaging in high-risk activities that may yield short-term benefits based on a misunderstanding or ignorance of the risk involved and the unrealistic rewards. It is because of this particular failure in managing risk that organizations develop risk management programs in order to identify, mitigate, and manage risks to achieve acceptable rewards (Crouhy et al., 2006).

Risk management is "the process of understanding, costing, and efficiently managing unexpected levels of variability in the financial outcomes for business" (Crouhy et al., 2006, p. 8). It includes the activities involved in selecting and implementing mitigation measures to bring risk to an acceptable level within an acceptable cost. Here, the important term is "acceptable," which must be defined based on a risk-reward framework which will encompass the value of a particular asset, and the consequence for its loss (both from a short-term and long-term perspective). Risk management is not a defensive activity, but the process of developing a risk-adjusted strategy that balances opportunity with consequence of actions (Crouhy et al., 2006).

Included in any definition of commercial or public-sector risk are the risks associated with information, information systems, and technology. These system risks are of special interest to those who are charged with the management and operation of an organization's information technologies. Systems risks are potential system losses, breaches, or failures which may mean "modification, destruction, theft, or lack of availability of computer assets such as hardware, software, data, and services" (Straub & Welke, 1998, p. 442). Common examples of identified systems risk might include computer abuse and misuse, disaster scenarios realized, violations of access restrictions, and exposure of intellectual property resident in computer systems. Systems security risk, a subset of systems risk, refers to a situation wherein the firm's information or information system technology are not sufficiently protected against damage or loss (Straub & Welke, 1998).

In regard to these systems risks, the U.S. Department of Commerce states that the purpose of maintaining a systems-focused risk management program is to

1) Better secure information technologies that process organization information;
2) Provide the necessary information to management in support of decision making surrounding the deployment of IT assets; and
3) Support management's authorization or accreditation of IT based on risk-focused assessments (Stoneburner et al., 2004).

Further, "risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions" (Stoneburner et al., 2004, p. 6). Most risk management programs exist in organizations through being tightly tied to a standard system's development life cycle (SDLC) in order to manage risk at all stages of technology development and deployment.

Outsourcing is a strategy for managing the risk of information technologies in organizations that has recently become popular. A key benefit as purported by advocates of outsourcing is the ability of the client and the vendor to share both the risks and rewards of their information technology. In fact Dibbern, Goles, Hirschhiem and Jayatilaka (2004) state "due to vendor opportunism … some companies have formed relationships with multiple vendors in order to mitigate the risks" of IT deployment (p. 32). IT managers often claim that outsourcing their information systems reduces the technological risk and uncertainty that would have been managed by an organization (Clarke, Zmud & McCray, 1995) at their time and expense and likely, outside of the organization's core competency.

To understand the risks associated with outsourcing related activities, "it is essential to identify the array of potential undesirable outcomes that could occur with respect to the outsourcing arrangement" (Aubert, Patry & Rivard, 2005, p. 12), which can be expressed by the magnitude of losses and the probability of such an occurrence. Even though risk management entails a high level of complexity and the conclusions reached are sometimes far from precise, identifying the risks of outsourcing allows the risk to be managed. These findings can become the basis for managing the risk surrounding one particular type of IT outsourcing, the use of the cloud.

3. What is cloud computing

Cloud computing refers to an emerging model of computing where machines in large data centers can be dynamically provisioned, configured, and reconfigured to deliver services in a scalable manner, for needs ranging from scientific research to video sharing to e-mail (Wyld, 2009). While usually described as a single entity, cloud computing can comprise several components at once: cloud infrastructure, cloud platform, and cloud application. *Cloud infrastructure* is the provision of a computer infrastructure as a service–both computational resources and storage–such as Amazon's Elastic Compute Cloud (EC2) and S3 services (Youseff, Butrico, & Da Silva, 2008). This infrastructure allows users to configure the infrastructure themselves, including the rapid expansion of their infrastructure based on network requirements. *Cloud platform* is the provision of a computer platform or software stack as a service, such as Google's App Engine or Salesforce.com. *Cloud applications* are web services that run on top of a cloud platform or infrastructure and are made available to the organization's users or customers. They can include applications that are commonly known to the public including YouTube's video hosting applications and Google's GoogleDocs set of office applications.

Cloud providers already offer a variety of services to individuals, companies, and government agencies, with users employing cloud computing for storing and sharing information, database management and mining, and deploying Web services that can range from processing vast datasets for complicated scientific problems to using clouds to manage and provide access to medical records (Hand, 2007). The incredible level of information and processing capacity level of data available in the cloud–the petabyte scale–allows for entirely new approaches to data analysis (Anderson, 2008). Individuals may use cloud computing simply to store e-mail and other documents, where large corporations and scientists can use the vast computing power available to add a new dimension to their current IT infrastructure (Wyld, 2009).

Cloud computing opens up the possibility that a major cloud provider such as Google could ultimately become "the world's primary computer" (Baker, 2007, para. 5). Cloud computing represents a centralization of information and computing resources–quite contrary to the imagery that the label evokes–and many individuals, corporations, and government agencies are already frequent or constant, though often unknowing, users of cloud computing. The speed at which cloud computing has permeated Internet activities is increasing exponentially. Although many users may not be familiar with the term, the reality is that most users are already taking advantage of the cloud through Web-based software applications and on-line data storage services, like Google, YouTube, and Flickr (Buyya, Yeo & Venugol, 2008; Horrigan, 2008).

The notion of cloud computing not only changes an organization's infrastructure, but how they do business. As federal CIO Vivek Kundra has stated, " … it's a fundamental change to the way our government operates" (Wyld, 2009, p. 16). Accordingly, the federal government has already begun to implement cloud computing within their IT strategies. In early 2009, the General Services Administration (GSA) announced that the primary e-Government portals–USA.gov and its Spanish-language companion site, GobiernoUSA.gov–would be supported by cloud computing contracted with Terremark Worldwide's proprietary Enterprise Cloud platform (Beizer, 2009; Kash, 2009). Further, the Obama Administration has also expressed interest in the large-scale use of cloud computing for government storage and processing ("Will cloud computing work in the White House, 2009).

This focus on the electronic provision of information by the Obama Administration certainly would bring government closer to the social expectations of many citizens. The vast majority of government information is now born digital, and users want electronic access to it (Kubicek, 2008; Priebe, Welch & MacGilvray, 2008). A 2008 study found 77.4% of people seeking government information or services regularly used Google or another commercial search engine (Burroughs, 2009). However, providing ever-increasing amounts of government information, communication, and services on-line raises serious issues about equality for people with limited technological means to access e-Government (Bertot, Jaeger, Shuler, Simmons & Grimes, 2010; Jaeger & Bertot, In Press; Shuler, Jaeger, & Bertot, In Press).

4. Government use of cloud computing

Governments, and in particular the United States federal government, have begun to incorporate cloud computing infrastructures into the work of various departments and agencies. Under the leadership of CTO Vivek Kundra, cloud computing is used as a tool to facilitate information sharing, applications processing, and as a cost saving measure from traditional technological architectures. The following section examines the current level of adoption by the federal government, including examples of how it is leveraged to serve constituents.

4.1. Early use

Federal adoption and use of cloud technologies has been an inevitable response to informal use by its employees, agencies, departments, and contractors (Mark, 2008). Federal use of cloud applications has been both a reactive measure and a strategic decision. Instant messaging applications, use of personal e-mail accounts utilizing cloud platforms over government web servers started with the availability of those applications, with little restriction or blocking. As concerns over hacking and virus infection grew, some federal agencies began to institute service blocking as a protective measure until formal policy could be issued.

Recognizing the inevitability of the cloud's presence in federal IT work (Wyld, 2008), the GSA issued guidance prior to Obama's presidency. *Social Media and Web 2.0 in Government* offered an initial roadmap for the new administration's information strategy, which includes discussion on using cloud applications to carry out some of the government's work. It recommends that to incorporate cloud applications, federal supporters, and designers should follow a grassroots, groundswell approach of a few strategic implementations to show their value and garner acceptance (Goodwin, 2008). So, in addition to simply migrating www.usa.gov and www.gobierno.gov to the cloud, GSA expanded the portals' services to access additional cloud applications such. Typical of early, public facing sites, however, the portals are not interactive and require no entry of personal information by the requestor. The National Institute of Standards and Technology (NIST) released a 2009 document where it not only attempted to define the nebulous term "cloud computing," but also provide some guidelines for governmental implementation. It identified their essential characteristics (ubiquitous network access, resource pooling, rapid elasticity, and measured service) along with multiple delivery and deployment models (Wyld, 2009).

4.2. Formal, strategic direction

President Obama and CTO Vivek Kundra have both expressed their interest in exploring the cloud as a strategic component in the federal IT transformation (Jackson, 2009; Miller, 2009c). Reasons stated for wanting to explore cloud computing in federal IT transformation include "to open up the government to its citizens," "bring government into the 21st century," and spur innovation (Obama, 2009b). The recession of 2008–2009 may also serve as another stimulus to leverage "on demand" services while mitigating the risks (e.g., security, privacy, reliability) and rewards (e.g., cost savings, access flexibility). The cloud could be an antidote to the "wastefulness of the current, fragmented model of IT supply" (Gourley, 2008). To this end, by migrating a number of web-delivered services to the public, such as www.usa.gov and the GovGab Blog at http://blog.usa.gov/roller/, the GSA predicts that its web maintenance costs will be reduced by 50% (Beizer, 2009), although the amount of time anticipated to register the savings is undefined.

To underscore the Administration's vision of the government and citizens as necessary and integral components of the federal information sharing model, Kundra has regularly referred to citizens as "co-creators" (Knowlton, 2009). After consultation with Google to explore the use of GoogleDocs as a government medium in order to foster large-scale collaboration, he commented "What I use in my personal life is much more advanced than what I had at work. Why wouldn't we invest in what all the employees are using at home anyway" (Hart, 2009, p. A13).

In March, 2009, President Obama confirmed his commitment to cloud computing by establishing Patrick Stingley as the federal Chief Technology Officer of the Federal Cloud (a.k.a. "cloud czar"), billeted at the GSA (Cohen, 2009). Well aware of the need to leverage the $70 billion federal IT budget, Stingley began with a mandate to create a development plan for the federal cloud capability to span all federal departments and agencies. GSA Chief Information Officer (CIO), Casey Coleman, suspended the position within six weeks of Stingley's accession, commenting that the timing to establish that position was "just a little premature" (Hoover, 2009). This did not deter GSA's commitment to supporting Kundra's cloud initiative, but certainly implies that approaching the cloud on such a broad implementation perhaps requires more planning than anticipated.

4.3. Current applications for information sharing

Currently, federal use of cloud environments predominantly focuses on information sharing and communications rather than data processing. As such, it relies on publicly-available products and some private vendors. Whether in response to the suggested standard (Goodwin, 2008), President Obama's support for the use of expanded technologies, or simply recognizing the value of this informal channel of communication, many (although not all) federal websites include links to popular cloud applications. As right-to-know regulations are revisited (Obama, 2009a), it will become clear whether these applications see increased user traffic and, by extension, whether citizen collaboration and use is influential.

More agencies are realizing that limited presence through cloud applications can serve a number of community involvement initiatives and can address a wider audience. For example, the Department of Veterans' Affairs (VA) uses YouTube to host videos embedded in its public website (http://www.oefoif.va.gov/) (Miller, 2009a), particularly to engage younger, returning service personnel (such as those returning from the wars in Iraq and Afghanistan). To accommodate mobile devices such as iPhones, the VA offers a site (http://m.va.gov/) re-formatted for greater accessibility. The U.S. Agency for International Development (USAID) has embraced similar capability. On December 19, 2008, the National Institute of Standards and Technology (NIST) also launched a YouTube channel to provide a rich library of lectures and training (http://www.youtube.com/user/usnistgov).

Despite their reputation for technological conservatism, many members of Congress have found that resisting the use of cloud applications to reach out to their constituency (and presumably each other) is difficult. The U.S. House and Senate have both collaborated sites that have a cloud infrastructure such as YouTube for their respective channels. These sites specifically convey videos *from* the

representative or authorized agent; uploads from the public are not permitted.

4.4. Applications and information processing

Beyond communication, the federal government is exploring methods to leverage cloud technology in a number of application-oriented ways. Some agencies have begun to use the cloud for information processing; in other words, they are using it as an application and processing server rather than simply a repository. Somewhat surprisingly, the Department of Defense (DOD) was one of the first entities to formally embrace the cloud environment in this way. The Defense Information Systems Agency (DISA) first awarded contracts to Hewlett-Packard, Apptis, Sun Microsystems and Vion for on-demand (a.k.a. software-as-a-service, or SAAS) data storage and processing services in 2006, under the aegis of its Defense Enterprise Computing Center (Mark, 2008). This service has matured into DISA's Rapid Access Computing Environment (RACE) (Beizer, 2009) and serves more than 3 million DOD users with 18 processing centers, 1,400 applications, 180 software vendors, 18,000 copies of executive software, 45 mainframes, and more than 4,500 servers (Beizer, 2008). Its operations are typical of a transaction system: the customer (usually an in-house or contractor developer) submits a credit card or purchase order number through a front-end portal (developed in this case in Cluster Resources' Moab software) and describes the work to be performed and the environment needed. Upon purchase approval, the requestor purchases a computing environment. Access security is managed by public key infrastructure (PKI) credentials, or common access cards. Alfred Rivera, Director of Computing Resources at DISA commented that RACE is the jumping off point for cloud work; the expanded "Federated Development Certification Environment" to support publication and access of DISA information is next in line for development. Whether this and future applications leverage commercial clouds (such as Google, Amazon, or salesforce.com) is being very cautiously considered (Harris, 2008).

The costs of collaboration within and across the government and citizens–travel, logistics, fees, and the like–are drivers to consider alternate methods, such as virtual worlds (Military Training: Actions Needed to More Fully Develop the Army's Strategy for Training Modular Brigades and Address Implementation Challenges, 2007). Recognizing that many of the newer members of the workforce have sophisticated computer skills, the federal government has initiated a number of cloud-delivered environments that support the social aspects of information sharing. Through avatars, chats, and other interactive capabilities, employees can complete on-line learning from their desks, model policy decisions, and collaborate with colleagues worldwide to discuss research techniques and findings. The following are some examples of the types of cloud-delivered environments being used within various organizations the federal government:

- The Air Force deployed *MyBase*, a 3-D virtual recruiting and training platform deployed in Second Life in December, 2008. It was made available to the public, and includes the ability to model base configurations, deploy on-line conferences, and welcome civilians and soldiers to its representation of real physical bases. Similarly, the National Guard has developed U.S. Nexus to provide the same capabilities and is scheduled be deployed in November, 2009 (O'Hara, 2009).
- Second Life figures in the Centers for Disease Control and Prevention's (CDC) mission of sharing real-life health alerts through avatars in the on-line community. It is also finding that its presence is felt through outreach and community building (Weinrich, 2006).
- The National Oceanic and Atmospheric Administration (NOAA) *NOAA Virtual World* allows the agency to share its laboratories, classes, research discussions, and conference spaces with students, citizens, policymakers, and scientists worldwide. A key initiative is this environment's ability to test data virtualization, or collaborative geographic information systems (Lipowicz, 2009).

Federal acceptance and use of cloud applications appears to be growing ahead of solid policy to provide a well-considered and secure plan that takes into account many of the general concerns about cloud computing, such as privacy, data availability and security, access control, appropriate licensing and service agreements, and durability of the vendor. Beyond President Obama's executive orders, the standards and policies developed and promulgated through NIST are either still in draft format or have not been formally operationalized (Jaeger, Lin & Grimes, 2008; Mell & Grance, 2009; "Recommended security controls for federal information systems and organziations, 2009; "Standards for Security Categorization of Federal Information and Information Systems, 2004). As recognized in private industry, cloud computing "is accelerating in adoption … the policy stuff is a big impediment. This is a place where the government has a strong role to play" (Condon, 2009).

5. Risks specific to government use of cloud computing

The introduction of any new technology to an organization brings many risks associated with the implementation and use. As mentioned in the previous section on risk management, it is important to not only recognize the risks associated with any new or implemented technologies, but to create a strategy that allows organizations to better manage and mitigate these risks. Prior to signing the first contract or agreement, it is vital to have in place a proper risk management program that can proactively and routinely identify, monitor, assess, and manage the systems and technology risks to avert their occurrence or mitigate their impacts. Although the potential for cost savings on infrastructure is a strong selling point for migrating to a cloud computing environment, the costs associated with the additional systems risks must be understood and accepted.

Introducing the cloud environment in an organization as vast and complex as the government exacerbates the intricacies and potential risks enormously, as implied in a statement within the United States' 2010 Federal Budget:

Implementing a cloud-computing platform incurs different risks than dedicated agency data centers. Risks associated with the implementation of a new technology service delivery model include policy changes, implementation of dynamic applications, and securing the dynamic environment. The mitigation plan for these risks depends on establishing a proactive program management office to implement industry best practices and government policies in the management of any program. In addition, the federal community will need to actively put in place new security measures which will allow dynamic application use and information-sharing to be implemented in a secure fashion. (*United States Federal Budget*, 2010, p. 157)

The following sections discuss the various forms of risk associated with cloud computing, and highlight key elements essential for any risk management plan intending to identify, manage and mitigate these risks.

5.1. Tangible/known risks

Initially, it appears that an overarching risk to implementing cloud computing to support federal IT needs is defining "the cloud" with adequate specificity such that it would be disambiguated from an enterprise, a distributed network, or an outsourced terrestrial data warehouse. Currently there are some standards for managing federal enterprise data, architectures, and security (Balding, 2009), but no standards are yet ratified for the cloud's components. Because the federal cloud could be realistically viewed as an enterprise, one might assume that enterprise standard would govern its content and use. However, if identified as a cloud, the standards are unclear.

Once the decision is made to integrate the cloud into the federal IT world, the governing agencies would left be to determine the scope of implementation. Until the question of whether the federal government would be considered to be a single entity or whether the cloud would be implemented on a department-specific or agency-specific basis is resolved, the risk of a piecemeal implementation is quite high, and one with which the federal government grapples currently (e.g., first responder communications systems, security-oriented traveler identification) (Cooney, 2008). In order to appropriately assess the risks that are introduced to an organization when using cloud computing, these four categories based on the Economist's Business Risk model (Managing Business Risks in the Information Age, 1998) can be used to identify possible risks: access, availability, infrastructure, and integrity.

5.1.1. Access

An organization's private data must be secured to ensure that only authenticated users are allowed the access authorized by the customer–the federal agency, in this case–and that any unwanted or outside access requests are denied. In an enterprise or distributed network, this is a routine protocol, but the cloud infrastructure presents new challenges beyond the usual issues of remote access, data transfer across public telecommunication lines, and intrusion detection and control through constant system monitoring. The unique schema for physical data storage, for example, may well house multiple clients' data on one physical device. This shared physical server model requires the vendor to ensure that each separate customer's data remains segregated so that no data bleeding occurs across virtual servers. To further complicate the issue, a single file or data storage area may be distributed among multiple physical servers over several states; this may distribute the risk of a single point of failure, but creates multiple possible points for intrusion. If the vendor's servers span multiple countries, data access and distribution may very well be subject to the privacy laws and precepts of the host country that do not synch well with American regulations (Jaeger, Lin, Grimes & Simmons, 2009).

The vendor must ensure that all access privileges can be audited by the customer or their external auditors. In federal information processing, requirements to comply with federal privacy and information integrity laws are common for traditional enterprise systems but are not explicitly defined for the cloud. The cloud infrastructure must also provide the required logging, tracking, and monitoring capabilities that would be commonly found on an internal server (Armburst, Fox, Griffith, Joseph, Katz, Konwinski et al., 2009), but the extent and protocols of implementing these services would need to be defined in a service level agreement (SLA) between the agency and the vendor. As a third-party storage vendor, maintaining currency of user access and authentication profiles is challenging. If this information were to be compromised from internal and external sources, sensitive federal data may easily be placed at risk.

Beyond assessing the integrity of the information stored in the cloud, an interesting component of IT auditing is identifying the source of the information and how it is subsequently used, and by whom. In terrestrial systems, once data are removed from a server, it is difficult to track it to its new, non-connected location. In this scenario, the cloud may actually ease this problem by including tracking metadata (such as IP addresses) to its new location. For example, a recent study concluded that sensitive medical data stored in the cloud could be amalgamated with other databases to compromise confidentiality and identify patient identities and other electronic data. It is estimated that the market for this "scrubbed" patient data could exceed $5 billion as the United States moves towards electronic medical records, although some of these data sales would be in violation of the Health Insurance Portability and Accountability Act (HIPAA) (Zetter, 2009).

The cloud environment spans the world. Access may also be subject to the conventions and laws of the country in which servers are housed. Currently, no federal policy addresses how the government information is accessed or managed on non-domestic sources. While information may be requested, at this point, the laws of the host country regarding the access and release of that information still prevail (Richey, 2009).

5.1.2. Availability

A key selling point to cloud computing has been the potential for 100%, non-interrupted availability to the customer. For large vendors, maintaining 24/7 up time is crucial to their business, as customers demand no less to support their mission-critical efforts. However, outages do occur, and can be unexpected and costly to a customer. Research from the University of California, Berkley tracked availability for major cloud vendors and recorded four major outages (i.e. 1 h or greater in length) during the first 4 months of 2008. The causes of these outages ranged from overloads on the systems to programming errors that caused the system to fail. The issue in these cases stems from the fact that the cloud vendor is a single provider; the failure of the company is the single point of failure (Armburst et al., 2009) and the clients were either unaware or unconcerned that the vendor had no redundancy or back-up mechanisms in place. In a period of less than 60 days, Apple MobileMe, Google Gmail, Citrix, and Amazon S3 all reported outages or periods of unavailability from 2 to 14 h; in March 2009, Microsoft Windows Azure was down for 22 h (Hoover, 2009). At an estimated $100 billion a year market value by 2011 (Klems, 2008), the outage financial cost for just these examples alone can certainly reach into the millions of dollars, not to mention the additional cost caused by the loss of confidence by these organizations' own customers and associates.

Natural disasters and other unexpected events can cause cloud services to become unavailable. For example, in June 2009, a lightning strike at one of Amazon.com's EC2 data centers caused its cloud service to go off-line for approximately 4 h. This was the third time in the past 2 years that such a wide-spread outage was experienced (Miller, 2009b).

The vendor must be able to calculate the demand for its services, which is, in fact, a calculation based on the demand for its customers' services. This inexact science has the potential for error which can lead to the cloud being over capacity. Once a cloud reaches a capacity greater than 80%, local computers and cloud servers will "thrash" by constantly moving data between disks and computer memory, causing computers to become almost unresponsive. If the cloud is not designed with enough slack resources to manage a situation where over capacity occurs, the entire cloud can fail. As Greenberg (2009) states, the control to mitigate this risk "is that when clouds reach their capacity limit, they could be architected so that applications can request no more computing capacity. They could gracefully degrade each applications' usage, which could prohibit the application from working, but allow the cloud itself to remain functional" (p. 2). Any outage caused through overcapacity will have costs (both financial and reputation) to the customer. In assessing bids for cloud services, federal procurement specialists would need a deep understanding of the risks and impacts of even a minute's outage and acceptable levels of downtime on a site-wide basis before a contract could be awarded.

Another risk to availability is how the priority of users on the cloud is determined should the overcapacity threshold is reached. If capacity begins to approach the 80% threshold and compromising some services or performance is necessary, the vendor will most likely protect their own services and pass the degradation in service to their customers. This risk once again points to the need of the customer to understand the capacity of the cloud and how their account will be managed. This is not easy, as a cloud's reserve capacity is not transparent, and data on this subject are not made public by major cloud providers due to competitive reasons. One indicator may be the electrical usage by a vendor, which is one indication of the amount of technology employed for their cloud (Jaeger et al., 2009). Variability in performance speaks loudly as a risk to cloud users, as they will demand a service that is predictable and able to reliably meet their service level requirements.

As cloud computing becomes popular and major corporations and government entities become customers, the services will naturally become targets for malicious attacks by hackers. Cloud vendors will need to understand the risks presented by those who can launch a number of sophisticated denial of service attacks (Armburst et al., 2009); this risk was realized recently by Facebook and Twitter (Ortutay, 2009). Reliance on these outsourced vendors could have resulted in a significant loss of communication within, across, and with federal agencies. At this point, the impact of this outage to federal users is still not assessed.

Another point to consider is the availability of the vendor itself. If the vendor goes out of business or is subsumed by another vendor, the custody, safety, and availability of the data it had stored may be in question. In 2008, the cloud vendor The Linkup unceremoniously ceased operations with little notice to its 20,000 customers. According to CEO Steve Iverson, "at least 55% of the data was safe. How much of the remaining 45% was saved is not clear" (Brodkin, 2008).

5.1.3. Infrastructure

The underlying cloud infrastructure and environment must be designed and implemented to be flexible and scalable. Unfortunately, the history of designing, delivering, and managing very large scale federally-developed systems (e.g. FBI's Virtual Case File system, and the Department of the Treasury's in-house data processing networks) does not offer many success stories to build upon. If not implemented properly, the government risks significant challenges and costs in migrating information to different technologies as the third-party vendor upgrades its processing and storage environment. If this type of upgrade is managed in-house, resident IT professionals can more readily manage migration and harmonization of data, users, and processes. But the procedures that a cloud vendor executes in scaling its environment is managed without the input of its customers, and may change or nullify the services the customer requires.

Customers require the ability to increase bandwidth, speed, and response time. In some cases, the cost to move data to a cloud infrastructure has proven quite costly in terms of time (bandwidth) and money. Some cloud users have resorted to using physical media to send data (Armburst et al., 2009) in order to expedite changes in their business needs.

All IT systems are subject to regular considerations of their life spans and durability. The question arises as to how long certain technologies will exist. The need for interoperability, the ability to switch providers, compatibility between vendors, and avoidance of migration issues will all be demanded by customers. As the government approaches the cloud, this will likely be very problematic as there are no universal, ratified standards within the industry or through NIST that would govern these issues (Mell & Grance, 2009).

A further risk to cloud implementation is the proprietary nature and lack of standards surrounding the application program interfaces (APIs). APIs are seldom made public, making it difficult to design applications and services that are compatible between multiple vendors. This can indeed limit the ability of an agency to award a contract to a competing vendor, and may create a monopoly situation by locking an agency into a single source.

A significant concern in implementing the cloud into the government, especially when system security is a very high priority, is the issue of compliance. In-house IT developers and contractors who develop, deploy, and manage federal systems are subject to the same compliance regulations. FISMA (Federal Information Security Management Act) (PL 107-347) through Federal Information Processing Standard (FIPS) 199 dictates what can and cannot be done with federal data; this Act pre-dates cloud computing. From an information processing standpoint, working in the cloud necessarily excludes FISMA compliance. Section 3544(b) requires that the "senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through" potential risk and harm from unauthorized access, disruption, use, as well as developing, implementing, and assessing levels of risk. While under review by the Information Technology Association of America (ITAA), the government appears to be moving ahead without clear standards (Mark, 2008).

5.1.4. Integrity

Integrity includes a number of arenas that are critical to averting or mitigating the risks that affect the accuracy of information managed. Data validity and quality, security, and durability speak to the system's operations; integrity is especially difficult when assessing the validity of second generation (i.e. derived) data. The decisions and processes involved in determining which vendor to use and how the system is managed are equally relevant. Integrity also addresses cost and schedule management as well as program efficacy and performance. These are always challenging for federal acquisitions and contract management processes.

Any information housed within a cloud infrastructure must maintain its integrity–its accuracy within its context–to be of value to the customer. The cloud provider must ensure that all precautions are taken to guarantee that data within the cloud storage does not become corrupt or altered; this is not a safe assumption without a defined SLA. Recently, a cell phone provider that stored customer data (such as personal text messages, contact lists, etc.) in a Microsoft subsidiary-provided cloud became unavailable when the provider lost that data. Customers had to wait days to be informed that a possibility (but no guarantee) existed that their data may be able to be restored. However, the extent of data recovery, the level of data integrity, and the timeline to restore remain to be seen (Cubrilovic, 2009).

Here the question of responsibility and liability emerges. If a problem were to occur, who would be responsible or liable for the problem and for ensuing results and remediation? Could responsibility even be determined based on the infrastructure? Without detailed SLAs, these issues will become quite difficult for both the vendor and government to resolve.

Due to a lack of federal policy and a dearth of challenging case law, who owns information (and its metadata and forensics) once it is remanded to a cloud's custody is not clear. For example, if a soldier or federal employee posts to a federal blog housed in a cloud, the terms of service between the agency and the cloud would drive who owns and controls that information. But if the individual is not aware of those terms and that information is breached, who would assume that liability? This presents interesting implications in the double-edged sword that is the balance between free expression, information accuracy and verifiability, and accountability.

Many of the above risks are similar to risks the government experiences when outsourcing IT technology. When outsourcing occurs, it becomes very important that the contract language reflect the requirements and needs of the government in order to ensure the service provider has a concrete understanding of their obligations when providing the service. This language usually is focused on the service level agreement which details performance standards and measurements (Chen & Perry, 2003), but also must incorporate the requirements of the government's risk management plan in order to provide assurance on the security and privacy of both data and services.

5.2. Intangible/unknown risks

There are many law and policy issues raised by cloud computing that could become problematic for government agencies, both as cloud users and as cloud providers (Armburst et al., 2009; Jaeger et al., 2008; Jaeger et al., 2009). For government agencies, and agency

employees, as users (whether the cloud is commercially or agency-operated), these issues may include:

- Access to, and use of, the cloud where and when it is needed without hindrance or interruption from the cloud provider or third parties–a big part of access for government agencies will be the sheer volume of usage that may tax cloud provider capacities;
- Reliability of the cloud, especially for the task of running "mission-critical" applications, of which government agencies tend to have many;
- Continuous service, as a loss of service could have dramatic impacts on government functions and may result in a loss of confidence in government programs;
- Security to prevent unauthorized access to both data and code, particularly securing the huge amounts of sensitive personal and government data;
- Safety mechanisms, so that the provider will be restricted from monitoring or trawling through the government information kept in the cloud;
- Data confidentiality and privacy, particularly for all the personally identifiable individual information and sensitive corporate information that agencies have about citizens and companies;
- Preservation of information and documents, as many laws require the short-term or permanent retention and preservation of federal records;
- A clear delineation of liability if serious problems occur, which could be very significant if a government agency is affected;
- The protection of any intellectual property rights that might be involved, such as patent data being stored in a cloud;
- Regulation and control of the information that is created and modified using cloud services;
- Interoperability of technology, as an agency may use many different technologies, formats, and storage technologies;
- Portability of data and resources between different parts of the cloud, as well as the ability of different government agencies to interact and collaborate within the cloud;
- Capacity to be audited, per government regulations and requirements; and
- Location of legal jurisdiction, if an agency has a claim against their cloud provider.

And while all of the issues above clearly are of concern to government agencies as users of cloud services, many agencies are also considering becoming cloud providers. Government agencies as providers of clouds will have to focus on such issues as:

- **Benefits**—A new technology should introduce a financial or other benefit. To date, no data exist from which to determine whether any significant cost savings would result from implementing a cloud that would serve as vast an organization as the federal government. Furthermore, no data exist that could be used to better anticipate unplanned or unidentified costs.
- **Confidence in cloud delivery and management**—The credibility of the installation of new technological infrastructure is based in part on past successes. If the federal government has a spotty record of delivering, managing, and controlling past IT projects, the question should be asked as to whether there is sufficient confidence that the project will be managed reliably and transparently if a cloud environment is established with outsourced vendors.
- **Sustainability**—The durability of new technologies is assessed in hindsight. Will the government's demonstrated enthusiasm for the cloud be sustained? Will the cloud be a fad that is subject to the instabilities of budget priorities and changing values (Daconta, 2009)?
- **Inclusion of all citizens**—Many users have limited or no access to computers and/or the Internet, while many others have limited comfort, technical skills, or government literacy that constrains their ability to use e-Government. While cloud computing offers many potential benefits to agencies, it also has the potential to further disenfranchise citizens that are not active users of the Internet. As technologies such as cloud computing allow more governmental services to be moved online, this problem will be intensified. This problem occurs because of the proliferation of many forms of technology; cloud computing adds to the potential disconnect to many citizens.
- **Current and Continuing Public Access**—Is it reasonable and appropriate to outsource management of the national trust–the documents of the American government–to a commercial entity? Perhaps one of the most controversial and deep-reaching risks drives to the precepts that underscore American identity. It was imperative, to the founders of America, that the artifacts of the government be available for public review, both for participation in governance and for creating a long-term record of the republic (Quinn, 2003). These sacred duties–the provision of information to ensure an informed citizenry and the continuing custody and conveyance of American documents in any media–transcend the cloud environment but beg the question of what information should be managed only by a federal agency in order to promote a healthy republic.

Previous federal government efforts to quickly adopt and adapt to a new technology have not always been successful, especially with the presence of many unknown factors. A useful example can be found in the ongoing attempts to increase the availability and equality of broadband access. After more than a decade of government programs involving both the direct distribution and redistribution of government dollars through the Universal Service Fund, the results are mixed. Broadband has become increasingly available, but primarily in urban areas that already enjoy significant technological, economic, infrastructure, and geographic advantages in access (Gabel, 2007; Grubesic, 2006; Mack & Grubesic, 2009). Large portions of the nation–particularly rural and poor areas–still lack adequate broadband access, while some states have become so successful at applying for the federal funds that these government funding advantages serve to exacerbate the existing disparities in access (Jaeger, Bertot, McClure & Rodriguez, 2007; Jaeger, McClure & Bertot, 2005). The significant unknowns in both the programs and in the factors of broadband adoption led to predictions of the current results a decade ago (Crandall & Waverman, 2000; Rosston & Wimmer, 2000; Shuler, 1999). Had broadband programs been developed with a greater understanding of the risks and factors in adoption, the ultimate outcomes may have been much closer to the original policy goals.

6. Conclusions

Given the relatively undeveloped and unproven state of federal cloud policies and the widespread unknowns that weave into the question of whether the federal government can successfully identify and manage the risks of working in a cloud environment, proceeding with caution until policies, standards, and technical proficiency are addressed will help the government avoid any unwanted risks. The conventional wisdom at this point suggests that without deliberate planning in scope, deployment, management, privacy, security, and the other considerations that should pertain to all federal programs, the cloud is a "red herring" that demands a wait-and-see approach (Daconta, 2009).

The comment in the 2010 federal budget–"In order to achieve these goals, pilot programs will provide a model for scaling across the Government" (*United States Federal Budget*, 2010, p. 157)–is worth noting. If one considers the breadth of the federal IT worlds, it is apparent that a "one size fits all" approach would be an inappropriate perspective. The needs of the DOD, for example, would likely differ significantly in amount of processing power, security constraints and liability, user base, geography, and other considerations than the needs of the Department of Transportation (Harbick, Ritchey, & Fontecilla, 2009). Each departmental agency would likely need to be evaluated individually for its needs and constraints. Conceivably, this could

reshuffle the federal IT organization from solutions by department and subordinate agencies to clustering delivery of cloud services to agencies with similar needs, regardless of the overarching department.

The key issue is one of governance, and specifically the IT governance mechanism's ability to identify, assess, and mitigate the risks surrounding the government's use of cloud computing. IT governance, as a subset of organizational governance, is focused on both external and internal compliance initiatives (Weill & Ross, 2004). It attempts to provide a mechanism where all stakeholders have a say in the decision making process. It should incorporate both decision making processes and assignment of accountability within the IT organization. The formation of IT policy within the governmental realm would be included in this governance umbrella. It should be noted that while government CIOs are capable of governing and controlling items within their agencies and departments, a key challenge presented by cloud computing is the difficulty that exists in fully managing and controlling cloud providers outside the government. This once again illustrates the need for strong service agreements and a thorough understanding of the risks of cloud computing.

In order for the government to have the ability to identify opportunities for cloud technologies, and implement them within the governmental IT and policy structures without exposing the departments to unwanted or unforeseen risk, an appropriate governance structure must be created to oversee an effective risk management program. This program would manage policies intended to mitigate not only the common and easily identifiable tangible risks presented by cloud use, but those intangible risks that are specific to government operations and that affect all citizens. Without the appropriate level of oversight and governance, the tendency to implement cloud infrastructure and worry about the consequences later will lead to unpredictable and undesirable consequences to the nation's information.

References

Anderson, C. (2008). The end of theory: the data deluge makes the scientific method obsolete.*Wired* (February 27, 2009 Retrieved June 12, 2009 from http://www.wired.com/science/discoveries/magazine/16-07/pb_theory).

Armburst, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2009). Above the clouds: a Berkley view of cloud computing (Retrieved June 12, 2009, from http://radlab.cs.berkeley.edu/).

Aubert, B. A., Patry, M., & Rivard, S. (2005). A Framework for information technology outsourcing risk management. *The DATABASE for Advances in Information Systems*, *36*(4), 9–28.

Baker, S. (2007). Google and the wisdom of the clouds (Retrieved February 27, 2009, from http://www.msnbc.msn.com/id/22261846/).

Balding, C. (2009). U.S. Government creates cloud computing security group (Retrieved April 15, 2009, from http://cloudsecurity.org/2009/03/04/us-government-creates-cloud-computing-security-group/).

Beizer, D. (2008). DISA debuts self-service computing (Retrieved Aril 15, 2009, from http://fcw.com/Articles/2008/07/14/DISA-debuts-selfservice-computing.aspx).

Beizer, D. (2009). USA.gov will move to cloud computing Retrieved April 15, 2009, from http://www.fcw.com/Articles/2009/02/23/USAgov-moves-to-the-cloud.aspx.

Bernstein, P. L. (1998). *Against the gods: The remarkable story of risk.* New York, NY: John Wiley & Sons, Inc..

Bertot, J., Jaeger, P. T., Shuler, J. A., Simmons, S. N., & Grimes, J. M. (2010). Reconciling government documents and e-Government: Government information in policy, librarianship, and education. *Government Information Quarterly*, *26*, 433–436.

Brodkin, J. (2008). Loss of customer data spurs closure of online storage service "the link up" Retrieved March 14, 2009, from http://www.networkworld.com/news/2008/081108-linkup-failure.html?hpg1=bn.

Burroughs, J. M. (2009). What users want: assessing government information preferences to drive information services. *Government Information Quarterly*, *26*, 203–218.

Buyya, R., Yeo, C. S., & Venugol, S. (2008). Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. *Paper presented at the 10th IEEE International Conference on High Performance Computing and Communications*.

Chen, Y. -C., & Perry, J. (2003). Outsourcing for e-Government: managing for success. *Public Performance and Management Review*, *26*(4), 404–421.

Clarke, T. D., Zmud, R. W., & McCray, G. E. (1995). The outsourcing of information services: transforming the nature of business in the information industry. *Journal of Information Technology*, *10*(221–237).

Cohen, R. (2009). The U.S. federal government defines cloud computing.*Cloud Computing Journal* (Retrieved June 10, 2009, from http://cloudcomputing.syscon.com/node/954002).

Condon, S. (2009). Experts: policy could make, break cloud computing Retrieved August 7, 2009, from http://news.cnet.com/8301-13578_3-10201461-38.html.

Cooney, M. (2008). Lots of excuses, little use of encryption on government mobile computers Retrieved August 7, 2009, from http://www.networkworld.com/community/node/30482.

Crandall, R., & Waverman, L. (2000). *Who pays for universal service?* Washington, D.C.: Brookings Institute.

Crouhy, M., Galai, D., & Mark, R. (2006). *The essentials of risk management.* Toronto, ON: McGraw-Hill.

Cubrilovic, N. (2009). Letting data die a natural death Retrieved October 13, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2009/10/11/AR2009101100109.html?nav=hcmodule.

Daconta, M. (2009). Cloud computing and five other IT fads that aren't always right for government Retrieved May 4, 2009, from http://gcn.com/Articles/2009/08/10/Reality-Check-IT-fads-not-fit-for-government.aspx.

Dibbern, J., Goles, T., Hirschhiem, R., & Jayatilaka, B. (2004). Information systems outsourcing: a survey of analysis of the literature. *The DATABASE for Advances in Information Systems*, *35*(4), 1–97.

Gabel, D. (2007). Broadband and universal service. *Telecommunications Policy*, *31*, 347–358.

Goodwin, B. (2008). Social networks and government Retrieved April 2, 2009, from http://www.usa.gov/webcontent/technology/social_networks.shtml.

Gourley, B. (2008). Wall Street crisis, enterprise technology and cloud computing Retrieved May 6, 2009, from http://ctovision.com/2008/09/wall-street-crisis-enterprise-technology-and-cloud-computing/.

Greenberg, A. (2009). If the clouds burst Retrieved June 11, 2009, from http://www.forbes.com/2009/06/04/cloud-computing-nist-intelligent-technology-cloud-computing.html.

Grubesic, T. H. (2006). The spatial taxonomy of broadband providers in the United States: 1999-2004. *Telecommunications policy*, *32*, 212–233.

Hand, E. (2007). Head in the clouds. *Nature*, *449*, 963.

Harbick, R., Ritchey, R., & Fontecilla, R. (2009). Cloud computing: myth or reality? Retrieved April 17, 2009, from http://gcn.com/articles/2009/03/06/commentary-cloud-computing.aspx.

Harris, D. (2008). DISA CIO: Cloud computing "something we absolutely have to do" Retrieved May 6, 2009, from http://www.on-demandenterprise.com/features/DISA_CIO_Cloud_Computing_Something_We_Absolutely_Have_to_Do_31270309.html.

Hart, K. (2009). Tech firms seek to get agencies on board with cloud computing. *Washington Post*, A13 March 31, 2009.

Hoover, J. N. (2009). GSA backs away from federal cloud CTO appointment Retrieved June 9, 2009, from http://www.informationweek.com/news/showArticle.jhtml?articleID=217800386.

Horrigan, J. B. (2008). Use of cloud computing applications and services Retrieved February 27, 2009, from http://www.pewinternet.org.

Jackson, J. (2009). Agencies tap online channels to spread the word on swine flu outbreak Retrieved May 5, 2009, 2009, from http://gcn.com/Articles/2009/05/04/UpDate1-CDC-swine-flu-networking.aspx?s=gcndaily_050509&Page=1.

Jaeger, P. T. & Bertot, J. in press. Designing, implementing, and evaluating user-centered and citizen-centered e-Government. *International Journal of Electronic Government Research.*

Jaeger, P. T., Bertot, J., McClure, C. R., & Rodriguez, M. (2007). Public libraries and Internet access across the United States: a comparison by state from 2004 to 2006. *Information Technology and Libraries*, *26*(2), 4–14.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: computing in the policy cloud? *Journal of Information Technology & Politics*, *5*(3), 269–283.

Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday*, *14*(5).

Jaeger, P. T., McClure, C. R., & Bertot, J. (2005). The e-rate program and libraries and library consortia. *Information technology and libraries*, *24*(2), 57–67.

Kash, W. (2009). USA.gov, GobiernoUSA.gov move into the Internet cloud Retrieved February 15, 2009, from http://gcn.com/articles/2009/02/23/gsa-sites-to-move-to-the-cloud.aspx?s=gcndaily_240209.

Klems, M. (2008). Merrill Lynch estimates "cloud computing" to be $100 billion market (Retrieved March 14, 2009, from http://markusklems.ulitzer.com/node/604936).

Knowlton, B. (2009). White House names first Chief Information Officer. *The New York Times* (Retrieved from http://thecaucus.blogs.nytimes.com/2009/03/05/white-house-names-first-chief-information-officer/).

Kubicek, H. (2008). *Next generation FoI between information management and Web 2.0. Paper presented at the 2008 International Conference on Digital Government Research, Montreal, QC.*

Lipowicz, A. (2009). Living NOAA's Second Life (Retrieved March 6, 2009, from http://www.fcw.com/Articles/2009/03/23/Eric-Hackathorn-NOAA.aspx).

Mack, E. A., & Grubesic, T. H. (2009). Forecasting broadband provision. *Information economics and policy*, *21*, 57–67.

Managing business risks in the information age. (1998). New York, NY: The Economist Intelligence Unit.

Mark, R. (2008). Do federal agencies belong in cloud computing networks? Retrieved April 30, 2009, from http://www.eweek.com/c/a/Government-IT/Should-Feds-Climb-on-the-Cloud/.

Mell, P., & Grance, T. (2009). Perspectives on cloud computing and standards from http://www.scribd.com/doc/13427395/Effectively-and-Securely-Using-the-Cloud-Computing-Paradigm.

Military training: Actions needed to more fully develop the Army's strategy for training modular brigades and address implementation challenges. (2007). (GAO-07-936). Washington, D.C.

Miller, E. (2009). The Verterans Administration goes Web 2.0 Retrieved June 11, 2009, from http://blog.sunlightfoundation.com/taxonomy/term/Facebook/.
Miller, R. (2009). Lightning strike triggers Amazon EC2 outage Retrieved June 11, 2009, from http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage/.
Miller, R. (2009). Obama tech team envisions federal cloud Data center knowledge, from http://www.datacenterknowledge.com/archives/2009/01/20/obama-tech-team-envisions-federal-cloud/.
O'Hara, C. (2009). Virtual learning gets second wind from Second Life Retrieved May 6, 2009, from http://fcw.com/articles/2009/05/04/feature-virtual-learning.aspx.
Obama, B. (2009). Revocation of certain executive orders concerning regulatory planning and review Retrieved August 1, 2009, from http://www.whitehouse.gov/the_press_office/Revocation-Of-Certain-Executive-Orders-Concerning-Regulatory-Planning-And-Review/.
Obama, B. (2009). January 21 Retrieved May 1, 2009, from http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.
Ortutay, B. (2009). Twitter service restored after hacker attack.*The Baltimore Sun* Retrieved from http://www.baltimoresun.com/technology/bal-twitter-outage-0806,0,2941226.story.
Priebe, T., Welch, A., & MacGilvray, M. (2008). The U.S. Government Printing Office's initiatives for the federal depository library program to set the stage for the 21st century. *Government Information Quarterly*, *25*, 48−56.
Quinn, A. C. (2003). Keeping the citizenry informed: early congressional printing and 21st century information policy. *Government Information Quarterly*, *20*, 281−295.
Recommended security controls for federal information systems and organziations. (2009) Retrieved August, 2009, from http://csrc.nist.gov/publications/nist-pubs/800-53-Rev3/sp800-53-rev3-final.pdf
Richey, W. (2009). Swiss Bank UBS to name American clients with secret accounts Retrieved August 9, 2009, from http://news.yahoo.com/s/csm/20090731/ts_csm/aubs.
Rosston, G. L., & Wimmer, B. S. (2000). The "state" of universal access. *Information Economics and Policy*, *12*, 261−283.
Shuler, J. A. (1999). A critique of universal service, e-rate, and the chimera of the public's interest. *Government Information Quarterly*, *16*, 359−369.
Shuler, J. A., Jaeger, P. T., & Bertot, J. in press. Implications of harmonizing e-Government principles and the federal depository library program to set the stage for the 21st Century. *Government Information Quarterly*.
Standards for Security Categorization of Federal Information and Information Systems. (2004), from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
Stoneburner, G., Goguen, A., & Feringa, A. (2004). Risk management guide for information technology systems. Washington, DC.
Straub, D., & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, *22*(4), 441−469.
United States Federal Budget. (2010). Washington, DC.
Weill, P., & Ross, J. W. (2004). *IT Governance.* Boston, MA: Harvard Business School Press.
Weinrich, N. (2006). The CDC's Second Life Retrieved August 1, 2009, from http://www.social-marketing.com/blog/2006/11/cdcs-second-life.html.
Will cloud computing work in the White House. (2009). *NPR* Retrieved August 21, 2009, from http://www.npr.org/templates/story/story.php?storyId=98578519.
Wyld, D. (2008). The blogging revolution: government in the age of Web 2.0 Retrieved April 2, 2009, from http://www.businessofgovernment.org/pdfs/WyldReportBlog.pdf.
Wyld, D. (2009). Moving to the cloud: an introduction to cloud computing in government *E-Government Series*. : IBM Center for the Business of Government.
Youseff, L., Butrico, M., & Da Silva, D. (2008). *Toward a unified ontology of cloud computing. Paper presented at the Grid Computing Environments Workshop at GCE 2008, Austin, Texas*.
Zetter, K. (2009). Medical records: stored in the cloud, sold on the open market.*Wired Magazine* Retrieved August 21, 2009 from http://www.wired.com/threatlevel/2009/10/medicalrecords.