NJ-2013-002

State DOT Use of Web-based Data Storage

FINAL REPORT
January 2013

Submitted by

Aaron Overman
Hugh Louch
Cambridge Systematics, Inc.
Bethesda, MD 20814

NJDOT Research Project Manager
Alejandro Perez-Deleon

In cooperation with

New Jersey
Department of Transportation
Bureau of Research

DISCLAIMER STATEMENT

“The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the New Jersey Department of Transportation. This report does not constitute a standard, specification, or regulation.”

TECHNICAL REPORT
STANDARD TITLE PAGE

1. Report No. NJ-2012-002	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle State DOT Use of Cloud-based Data Storage		5. Report Date February 2013
		6. Performing Organization Code
7. Author(s) Aaron Overman, Hugh Louch		8. Performing Organization Report No.
9. Performing Organization Name and Address Cambridge Systematics, Inc. 4800 Hampden Lane, Suite 800 Bethesda, MD 20814		10. Work Unit No. 11. Contract or Grant No.
12. Sponsoring Agency Name and Address New Jersey Department of Transportation P.O. 600 Trenton, NJ 08625		13. Type of Report and Period Covered 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

This study explores the experiences of state departments of transportation (DOT) in the use of web or cloud-based data storage and related practices. The study provides results of a survey of State DOTs and presents best practices of state governments who are leaders in cloud-based services and relates these experiences to New Jersey's data storage needs. The study identifies key actions that New Jersey may wish to take advantage of opportunities in this area.

17. Key Words Cloud, internet, data, storage, infrastructure, service, software	18. Distribution Statement		
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No of Pages 14	22. Price

Form DOT F 1700.7 (8-69)

ACKNOWLEDGEMENTS

The authors of this report wish to thank in particular the staff of the New Jersey Department of Transportation (NJDOT), as well as personnel from the state Departments of Transportation of Colorado, Hawaii, Iowa, Illinois, Missouri, Montana, Nevada, New Hampshire, New York, North Dakota, Ohio, Pennsylvania, and Utah without whom the completion of this report would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES

Page

EXECUTIVE SUMMARY

Both public sector agencies and private firms are increasingly taking advantage of the internet to provide services and information remotely. Often referred to as the cloud, this approach provides remote access to data and applications. This study explores the experiences of state agencies in the use of the cloud with a focus on the experience of transportation agencies. The study identifies best practices in cloud-based data storage and other uses of the cloud by public sector agencies in the United States and offers insight into potential opportunities available to improve data storage techniques and provide cost savings through reductions in capital expenditures of information technology equipment in the State of New Jersey. The study included a literature review and a survey of 50 state departments of transportation (DOT), with 13 states responding to the survey.

The literature review collected and organized information from studies, reports, and web sites that describe the key topics across the United States for cloud-based data storage and other uses of the cloud. Focus areas included policies, procedures, and contracting and procurement strategies to include key concepts and best practice information that would be useful to compare use of cloud services in state DOTs and state governments.

The literature review was augmented by a survey program; designed to enhance and clarify practices, policies, and procedures of state DOTs in regard to their use of cloud-based services and storage.

Upon completion of the literature review and survey program, the research team identified key lessons learned that relate to topic areas of particular interest to NJDOT. The study identified national policy recommendations, and findings that may provide a basis for further investigation by NJDOT as it considers potential enhancements to agency data storage practices.

BACKGROUND

Data stored remotely over the internet, also known as the cloud, is rapidly gaining users in business and government, and in some cases is poised to supplant traditional in-house server-based storage of data. The Federal government has put in place a “cloud first” policy, with an aim toward consolidating server farms and saving costs, and at the same time improving the responsiveness of data providers to changes in agency demands. [(1)]

While the Federal government has mandated that its agencies move elements of their information technology (IT) infrastructure to the cloud, most states face no such requirement, and the level of adoption of the cloud varies.[(2)] States and other agencies and firms commonly cite security, cost, and other considerations that lead to some IT elements being well-suited to the cloud, and others that are more appropriately maintained through locally sited and state-owned assets.

OBJECTIVES

This study examined the current state of practice of state departments of transportation with regard to their use of cloud-based data storage, in order to assist the agency with future decision making on the need for investment in locally based data storage equipment, and to investigate other benefits of using the cloud that may prove to be good business practice for NJDOT.

Specifically, the study addresses the following issues:

- Deployment of cloud computing in the DOT and/or state government to deliver solutions that are currently too expensive to create or not feasible to implement on the current information technology infrastructure, and

- Offering an alternative to a continuous hardware upgrade cycle by utilizing cloud-based software and infrastructure as a service model.

INTRODUCTION

Both public sector agencies and private firms are increasingly taking advantage of the internet to provide services and information remotely. Often referred to as the cloud, this approach provides remote access to data and applications. This study explores the experiences of state agencies in the use of the cloud with a focus on the experience of transportation agencies. The study identifies best practices in cloud-based data storage and other uses of the cloud by public sector agencies in the United States, and offers insight into potential opportunities available to improve data storage techniques, and provide cost savings through reductions in capital expenditures of information technology equipment in the State of New Jersey. The study included a literature review and a survey of 50 state departments of transportation (DOT), with 13 states responding to the survey.

SUMMARY OF THE LITERATURE REVIEW

The study team identified and reviewed documents and materials important to identify key issues and comparisons of state and national use of cloud-based services in the government sector. Key references included national standards and definitions, published state policies, expert presentations, and other published documents from academia and the private sector.

Defining the Cloud

In 2011, the National Institutes of Standards and Technology published a definition of Cloud Computing, which lists the essential characteristics of the cloud (Table 1), possible service models that may be utilized to deliver cloud-based storage and services (Table 2), and the deployment models that have varying degrees of connectivity outside a single organization (Table 3). [3]

Table 1 – Essential characteristics of the cloud

Characteristic	Summarized Description
On-demand Self-Service	Users can automatically request and configure computing capabilities without the need to contact a human at the provider side
Broad network access	Services are available over a network using a variety of standard equipment types
Resource pooling	Resources such as memory, storage, bandwidth, and processing are shared among users, and are allocated dynamically according to demand
Rapid elasticity	Resources can expand and contract in a near-instant fashion upon user request
Measured service	Resources are measured for a usage dimension (such as processing capability, storage, or bandwidth), and are provided to the user allowing them to monitor use, and the provider to charge for only the usage demanded

Source: The NIST Definition of Cloud Computing, 2011 [3]

Table 2 – Cloud service models

Model	Summarized Description	Example
Software as a Service (SaaS)	A service available over the network where all aspects of the provider's software are maintained in the cloud, and only a basic client interface is available directly to the user	Google Drive, Hotmail
Platform as a Service (PaaS)	The user may create applications, and have control over their deployment and configuration, with the application running on a cloud-based server	Engine Yard
Infrastructure as a Service (IaaS)	The most flexible model; the provider maintains the fundamental computing resources, with the client choosing operating system and networking capability	Amazon.com Web Services

Source: The NIST Definition of Cloud Computing, 2011[3]

Table 3 – Cloud deployment models

Model	Summarized Description
Private cloud	Built and used for a single organization, may exist on or off organization's premises
Community cloud	Built and used by a community of users with shared concerns
Public cloud	Resources are available to the general public
Hybrid cloud	A combination of two of the above models, working together in a way that allows applications and data to flow between them

Source: The NIST Definition of Cloud Computing, 2011[3]

The NIST definitions provide a basis for discussing the elements of cloud computing that are generally understood among IT experts and users of these systems. Elements of the various models have benefits and risks that will be discussed in the next section.

Considerations of Cloud Usage

An agency deciding whether and how to deploy cloud-based technology to solve a particular IT challenge will be faced with many considerations that should be fully examined in the decision making process. These are grouped into the areas of cost, vendor, procurement, and security.

Cost Considerations

While the convenience provided by cloud-based services may be a primary motivation for users, States and agencies must at the same time be mindful that, without demonstrated capital and operating cost savings, an in-house strategy may be more appropriate. The National Association of State Chief Information Officers' (NASCIO) "Capitals in the Clouds" series suggests that the motivation to pursue cloud based strategies always needs to be driven by an analysis showing that cloud computing strategies are more economically efficient than traditional strategies.[4,5,6]

For individual users, cloud-based services are often viewed as "free" because they do not require out-of-pocket expenditures.[7] Companies offering such services typically support their provision at no cost through the tracking of user activity, and the delivery of targeted advertisements. Laws governing public agency data, and data security policies, lead agencies and governments to pursue paid contracts with cloud computing providers that expressly do not allow the reading or tracking of data owned by the agency for any purpose other than the agency's own business.[4] These costs can be significant, and a recent analysis conducted by the State of Wisconsin Division of Enterprise Technology found that the all-inclusive costs associated with transitioning their in-house Microsoft Exchange email service to a cloud-based, one would either result in a savings of 7 percent, or cost 11 percent more, depending on the vendor selected.[8] A 2010 Brookings Institution report "Saving Money Through Cloud

Computing" likewise found large variances in the expected cost savings for cloud utilization depending on the methodology used, with some analyses demonstrating large savings, and others showing increases in overall cost. [5]

Vendor Considerations

Entering into a relationship with a cloud service provider creates a different relationship than with a vendor that provides off the shelf, or even customized software. Because software elements and agency data typically reside off-site with the vendor or another party (e.g., a third party provider that uses Amazon Web Services), ensuring their safe storage and operation requires a greater level of trust with the selected vendor. The agency should be mindful of the providers' standing in the industry, their financial health, their approach toward, and availability of technical support resources, and other similar factors. [4]

Also important factors include how an agency brings a cloud provider on-board to provide services and defining the terms of disengagement, and the process for transitioning data from the current provider to a future provider (or bringing the data back in-house) should be documented with the vendor up front. [9] Where the cloud provider is based and the effect of any state laws upon that provider due to their location is also an element that needs to be carefully considered.

Procurement and Contracting Considerations

Understanding exactly how the cloud vendor will store and manage agency data and services is critical to establishing a contract that fully meets the agency's requirements. This is often displayed in a diagram of how the provider's hosting environment operates, and an evaluation of this structure should be an element in evaluating which provider will best meet the parameters specified in the procurement document. [10] Other important considerations include strict specifications on data ownership, and assurances on availability of data, or promised uptime of the services being procured. States may provide agencies with standard, approved terms and conditions for cloud-based services to ensure that contracts are fully compliant with state policies. Agencies also need to understand and document the vendor's policies and practices on data encryption, and their plans for disaster recovery. [11]

Security Considerations

For public agencies, data security is perhaps the most critical consideration in this list. Clouds that are fully hosted within an organization, or private clouds, provide a measure of data security that may not require any agreements with external providers. The State of Michigan has chosen this approach. [12,13] The State of Delaware does allow the utilization of cloud computing in its information security policy, but an extensive set of approvals, through several information technology committees, and the State's attorney general's office, is required. [14] The critical cloud security areas listed in Delaware's policy are the protection of sensitive data, access control and identity management. [2] Another security issue noted by many IT experts is the rogue user, or those who send

and store data to the cloud under a personal, individual account due to the convenience and flexibility provided by cloud storage solutions. Agencies should guard against these users who put the agency's data at risk under terms and conditions that have no regard for compliance with state policies. Utah handles this in a unique way that requires users to disclose use of external providers, which come from a state approved list. [15]

SUMMARY OF WORK PERFORMED

At the direction and oversight of NJDOT, the research team investigated use of the cloud by DOTs and state governments through the following work plan:

- Literature Review – Identified relevant information from existing studies and a web search, and described existing knowledge concerning topics pertinent to NJDOT. Information was collected through consultation of key resources including key concepts, and best practice information that would be useful to compare state DOT and state government use of cloud-based storage and services. The literature review is summarized above.

- Survey Program – Developed and conducted an email survey and phone interviews with responding states in order to augment and corroborate information gathered in the literature review.

- Best Practices of Use of the Cloud in State DOTs and State Governments – Included synthesizing the information collected in the literature review and survey program, and performing a comparative analysis of the surveyed states' use of cloud-based services in relation to the questions of particular interest to NJDOT.

- Findings and Conclusions – Reported on best practices in the states in cloud-based data storage and other uses of the cloud, and offered findings that may prove of value, and the basis for further investigation to New Jersey DOT in the consideration of potential improvements to its information technology infrastructure, and potentially moving to store some of its data remotely.

Survey Program

The research team conducted a survey to examine the use of web-based or cloud storage for DOT data. A contact list of state data managers was developed, and CS contacted them with a survey instrument to gauge their agency's use of, and support for, cloud-based data storage.

The survey included the following questions:

- Does your agency store any data (asset inventories, crash data, traffic counts, etc) via the internet "in the cloud"? (Defined as any off-site storage of data on a server not directly owned, or controlled by, your agency or government, by agreement with a third-party data hosting provider, with access to the data provided over the internet.)

- If not, do you plan to in the future?
- Would you be willing to talk to us further about your plans so we can compile practices?

Table 4 summarizes the main survey findings based on the information that was provided by the survey respondents. Only the state agencies that responded are included in Table 4.

Table 4 – Agency use of and support for cloud-based data storage

Agency	Stores data in the cloud	Plans to store data in the cloud	Does not and does not plan to store data in the cloud
Colorado DOT		■	
Hawaii DOT			■
Iowa DOT	■		
Illinois DOT	■		
Missouri DOT			■
Montana DOT	■		
Nevada DOT			■
New Hampshire DOT		■	
New York State DOT			■
North Dakota DOT		■	
Ohio DOT			■
Pennsylvania DOT			■
Utah DOT		■	

Current Practices

Seven out of the 13 respondents (54 percent) had positive responses with respect to cloud data storage. Three out of those seven agencies currently store data in the cloud, while the four other agencies may consider plans to do so.

In 2007, the **Hawaii DOT** worked with Mandli Communications in order to implement cloud data storage for all the photolog/videolog data (such as Google streetview), but it did not work out too well according to the agency's survey respondent. The DOT continues to use an off-site third party data warehouse for its real-time, and continuously monitored traffic data; this was initially done with Econolite using a facility in Orange County, and is now done with IRD in Canada.

The **Colorado DOT** does not directly use cloud data storage; however, it purchases from a vendor environmental data that is hosted and accessed through a thin client application.

Elsewhere, the **Iowa DOT** harvests AVL data related to snow plows from a vendor's Amazon cloud. Harvested data is normalized, and referenced back to the state road network in DOT databases.

The **Illinois DOT** does some "cloud" hosting of data currently, but not for matters such as asset inventories, crash data, or traffic counts. According to the Department's CIT, there are some unique situations in which the DOT decides to go down the path of external access.

Even though the **Utah DOT** does not store any data at an enterprise level in "the cloud" currently, their GIS department uses ArcGIS Online Cloud Based storage, as sort of a "sandbox" for working drafts of GIS data.

Also, the **Nevada DOT** does not have any specific or approved contracts for Cloud Storage (IaaS) at this time, although they have a couple of systems (SaaS) in the cloud with data associated with those systems.

The **Montana** DOT is using a cloud-based SaaS, called MS2, to collect and disseminate vehicle count and classification data at the state's network of permanent count stations. [(16)] MS2's website claims other state DOT users in Alaska, Arizona, Colorado, Georgia, Illinois, Indiana, Massachusetts, Michigan, and Washington, D.C.

In **New Hampshire**, the NHDOT Traffic Research does not presently store any data "in the cloud", as all traffic data collected/processed are stored on DOT/State of NH servers.

Looking Ahead

There are states where the cloud option is being considered as a future option, such as in **Colorado**, where the DOT is beginning to explore the cloud data storage option more seriously and recently migrated all email and calendar functions to Google; or in **North Dakota** where there are talks that the North Dakota DOT would explore this option in the future, despite current legislative hurdles.

The **New Hampshire** DOT is presently contemplating a database conversion to an available commercial product, with some commercially available traffic database products offering a cloud based storage system. No final decision has been reached on the matter yet, and even though it cannot be conclusively stated that this will be pursued, it continues to be an option.

As local storage costs go up, and cloud platforms are increasingly offered as a service from private vendors, **Utah's** DOT is curiously looking into that hosting option for some data, particularly large amounts of LiDAR and imagery.

The **Nevada** DOT does not have solid plans to adopt cloud data storage at this time; however, this option would be evaluated on a case-by-case basis in accordance with the agency's potential benefits.

Best Practices in the States

While many states have explored the use of cloud computing, many of them have deemed it unsafe or inappropriate for state business. On the other hand, a small number of states have adopted "cloud first" strategies similar to that of the Federal government, and have deployed cloud computing strategies meeting the NIST definition. The states listed below have been at the vanguard of adopting cloud computing policies and installations, and can serve as models for other states wanting to move toward a broader adoption of private, hybrid, and public clouds to better address their agencies information technology needs.

Michigan

The State of Michigan was one of only two states to receive an "A" grade from the Center for Digital Government 2012 Digital States Survey. A primary area in which it excels is in the deployment of cloud-based services, which they have primarily tailored in a private cloud architecture called MiCloud. This was the first published state government cloud computing strategy in the nation upon its adoption in 2010.

In Michigan's case, the use of a private cloud avoids the great majority of security issues associated with off-site external provider storage, and has an added benefit of much higher data transmission speeds due to its physical location within the state linked with statewide high-speed transmission networking capabilities. Much like utilizing a private provider, MiCloud allows agencies to sign up for storage capabilities using a self-service intranet website and the costs are established up front based on the precise amount of storage required. MiCloud charges $0.01167/GB/day to its users, which is over 80 percent cheaper than commercially available storage solutions. Most MiCloud users never have to interact with an actual human to set up, reconfigure, or change their hosting options, with all common customer service requests available directly to the user, and handled automatically by the system's software.

The state's IT leadership considers the standard terms and conditions that accompany off-site data storage and hosting agreements to be unconstitutional because of their common need to indemnify the provider. This was a driving reason behind the state pursuing its private cloud strategy. The state also believed that shaping an external service to be compliant with the state's security policies would destroy any cost advantage of using the cloud. Importantly, the state has built the system using an Open Virtualization Format, which in the future allows the state to readily engage with external hosting providers, should they choose to move in this direction. The state intends to maintain a central linkage between the statewide MiCloud and external service providers, in part to solve any technical, legal, security, and policy issues at a single point of contact, and remove the need for agency IT staff to handle these matters. [12,13]

Utah

The State of Utah was the only other state receiving an "A" in the Digital States Survey and it, like Michigan, is a leader in deploying a private cloud for state agencies to use in an automated fashion. The state provides the full spectrum of Saas, IaaS and PaaS provisioning. A primary driver behind Utah's decision to pursue a cloud strategy was the need to close data centers to save costs; the state took 38 existing data centers and consolidated them into only two. The state realized one-time capital cost savings by eliminating the need to replace aging equipment, documented massive energy savings (enough to power 978 homes for one year), and has recognized a reduction in staffing needed to provide direct customer service to users. (17)

Utah has also embraced and adopted policies for a hybrid cloud, which combines elements of a private cloud, and publicly available storage and computing resources. The state's Technical Architecture Review Board has approved a standard approach for dealing with external cloud computing providers, and integrates these external services with private cloud elements when it makes sense from a cost and data security standpoint. (18)

The state's "Policy on Use of External Service Providers for Data Storage" dictates that the state must explicitly approve the provider for use with storage of state information, and the provider must pass a departmental security review. Furthermore, the state must have a contract with the provider that specifically addresses central management, use, storage of, and deleting of sensitive data. To date, Dropbox, Evernote, SugarSync, and Google Docs have been approved as data storage and cloud-based service providers under the policy. The policy requires users to explicitly disclose the use of external services so that the state may access them at any time, and restricts their use to nonconfidential, nonsensitive state data. (15)

Delaware

The State of Delaware has established some rigorous policies and procurement guidelines for utilization of cloud computing resources. Along with hosting a private cloud intended to eliminate the need for an extensive set of server replacements, the state also is moving to utilize the public cloud subject to some important restrictions.

Delaware considers the following elements to be non-negotiable in agreements with external providers:

- The State retains full ownership of the data
- The data are not allowed to reside offshore
- The provider must encrypt all non-public data in transit to the cloud
- In the event of termination of the contract, the Service Provider shall implement an orderly return of State of Delaware assets, and the subsequent secure disposal of assets

In addition to these broad principles, Delaware provides a detailed set of specific terms and conditions that must be present in any contract with a cloud-based provider, and has integrated cloud computing into its information security policy with an established process for approving contracts with external providers. [2,14]

Western States Contracting Alliance

In a relatively unique arrangement for cloud-based data hosting, the states of Oregon, Utah, Colorado and Montana utilized a multistate compact, and a contracting alliance, to procure a public cloud, hosting each state's GIS data remotely. Montana led the effort and was supported by the other states.[16] The Request for Information (RFI) was written in such a way that any state could participate in the contract, via the National Association of State Procurement Officials Cooperative. Cost savings was the driving reason behind the effort to move this data to the cloud. Because there are many similar needs across states, models such as this may provide greater access to cloud-based services in the future, without the need to undergo an expensive, and time consuming, independent procurement process in each state. [19]

National Organizations

Organizations such as TechAmerica (a lobbying group for the U.S. technology industry) and NASCIO have developed bodies of literature regarding public sector cloud benefits, risks, and best practices. [20,4,21] In addition to the state examples described in the previous chapter, these recommendations can help shape the deployment of cloud computing strategies for New Jersey DOT.

Before embarking on a cloud computing deployment, TechAmerica and NASCIO recommend that public sector agencies fully understand the needs of their users so that the proper service model(s) can be explored. They also stress the need to authenticate users, the need for a data portability strategy in order to prevent getting locked-in with a single provider, and for ongoing monitoring of risks and vulnerabilities to the system.

Once the agency fully understands the policy and security considerations, the organizations recommend creating a roadmap with multiple phases, allowing limited cloud deployments, testing their effectiveness, and following on with expansion. A cost-benefit analysis should be conducted, along with a documented case for what operational benefits the agency expects to realize. Preparation and planning are key elements of a successful deployment, and individuals from the IT leadership, as well as the end users, should form a collaborative team from the beginning of the project through to delivery. [20,4]

They stress the need to develop standard terms and conditions that will apply across all cloud services and matching these with the development of any IT policies on the cloud.

CONCLUSIONS AND RECOMMENDATIONS

The New Jersey Office of Information Technology's published policies do not currently include provisions allowing for the use of cloud-based data storage solutions. However,

cloud computing was noted as the most cited group priority at the state's Chief Information Officer (CIO) Collaboration Council in July 2012, and received a higher score from the council members than any other IT priority. Broad support for the development of cloud computing solutions appears to exist across the executive branch agencies within the state.

The most successful state governments in terms of cloud deployments have chosen to undertake a combination of policy and standards development, alongside a procurement strategy that takes into account agency needs. NJDOT should continue to track developments of statewide initiatives regarding the cloud, and continue to advocate for procurement and deployment of a private, or hybrid, cloud for its data storage requirements.

There are two potential pathways for NJDOT to pursue. Both involve applying statewide approaches where the DOT is one client among agencies within the State.

1. NJDOT could advocate for statewide deployment of a private/hybrid cloud, where the state sets up an internal cloud, and state agencies interface with it as they would an external hosting provider. This approach is similar to the State of Michigan and its MiCloud service.

2. NJDOT could advocate for development of statewide standards and/or a preapproved list of data hosting vendors. This would allow the DOT to customize its own solution, independent of what other agencies might do, and developed statewide standard terms and conditions will protect the DOT from a data security and legal standpoint. This approach is similar to how Delaware and Utah have chosen to approach the cloud.

NJDOT may also be able to realize significant one-time, and ongoing, cost savings by utilizing cloud-based services. In an environment of shrinking budgets in the public sector, the cloud may offer opportunities to expand services, while spending fewer dollars as compared to continuously upgrading its own equipment. The Western States Contracting Alliance expects to save between 62 and 88 percent in annual storage costs by utilizing cloud-based GIS data storage through private vendors. [19] As noted earlier in the report, Michigan is able to offer private cloud storage services at a cost 80 percent less than using a private vendor, [13] while Utah is saving over $4 million annually by consolidating its network of servers into a hybrid cloud. [18] The potential cost savings for New Jersey by moving some data and software to cloud-based services are likely to be significant.

BIBLIOGRAPHY

1. Kundra, Vivek. Federal Cloud Computing Strategy. Washington, D.C.: 2011.

2. State of Delaware Department of Technology and Information. Cloud and Offsite Hosting-- Keeping State Data Secure (memorandum). Dover, Delaware: 2011.

3. National Institute of Standards and Technology. The NIST Definition of Cloud Computing. Gaithersburg, Maryland: 2011.

4. National Association of State Chief Information Officers. Capitals in the Clouds: The Case for Cloud Computing in State Government, Parts 1 through 4. Lexington, Kentucky: 2011.

5. West, Darrell M. Saving Money Through Cloud Computing. Washington, D.C.: 2010.

6. ISACA. Calculating Cloud ROI: From the Customer Perspective. Rolling Meadows, Illinois: 2012.

7. Alford, Ted and Gwen Morton. The Economics of Cloud Computing: Addressing the Benefits of Infrastructure in the Cloud. 2010.

8. State of Wisconsin Department of Administration, Department of Enterprise Technology. Enterprise E-Mail and E-Mail Cloud Computing Comparative Cost Analysis. 2011.

9. McDonough, Bob. Taking the Nebulous Out of the Cloud (presentation). 2011.

10. National Institute of Standards and Technology. Cloud Computing: A Review of Features, Benefits, and Risks, and Recommendations for Secure, Efficient Implementations. Gaithersburg, Maryland: 2012.

11. Betcher, Thomas J. Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners. Eugene, Oregon: 2010.

12. State of Michigan. ICT Strategic Plan Appendix K – MiCloud.

13. State of Michigan. MiCloud Services Solution Details. 2011.

14. State of Delaware Department of Technology and Information. State of Delaware Information Security Policy. Dover, Delaware: 2007.

15. State of Utah Enterprise IT Management. Policy on Use of External Providers for Data Storage. 2010.

16. State of Montana. Montana ITSM SaaS System Case Study. Helena, Montana.

17. State of Utah Enterprise IT Management. Creating Utah's Cloud Infrastructure. 2010.

18. Woolley, Robert. State of Utah Strategy for Cloud Computing (presentation). 2011.

19. Multi-State GIS Cloud Services Assessment Team. RFI Response Assessment, Business Case and Recommendation.

20. TechAmerica Foundation State & Local Government Cloud Commission. The Cloud Imperative: Better Collaboration, Better Service, Better Cost. Washington, D.C., 2012.

21. National Association of State Chief Information Officers, TechAmerica, and Grant Thornton. The 2011 State CIO Survey. 2011.