NASCIO
Representing Chief Information Officers of the States

NASCIO Cloud Computing Series

Capitals in the Clouds

Part IV – Cloud Security: On Mission and Means

NASCIO Staff Contacts:
Charles Robb
Senior Policy Analyst,
Security and Privacy

Eric Sweden
Program Director,
Enterprise Architecture & Governance

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@AMRms.com
www.NASCIO.org

The Changing Landscape

There is no debate that cloud computing has arrived as a viable alternative for state government to deliver scalable and cost-effective IT capabilities including services, applications, platforms, and infrastructure.[1] State CIOs find themselves exploring strategic opportunities, technologies, shared services, and other offerings as ways to improve operational efficiency, optimize service delivery, and lower costs. As cloud adoption grows, the strongest driver presently is cost reduction, which is especially compelling given the continuing slow economic recovery in the states. State CIOs clearly recognize the need for operational cost reduction while seeking enterprise solutions, especially traditional state provisioned IT services like email and storage. In addition, performance efficiencies can also be gained if cloud computing solutions are properly planned, designed, and implemented.

As described in previous issue briefs in this series, the *concept* of shared resources is not new. Cloud computing does bring some new and critical considerations, depending on what service and deployment models are used. The approaches the states pursue will be a mix of private, public, and hybrid depending on the unique circumstances for each state. State government information technology officials, policy makers, business analysts, and security

professionals must filter through the hype in evaluating cloud computing in general and cloud deployment alternatives. Security must be a critical element of this examination.

Although it may not be obvious from the hype, the variability of cloud models, market choices, vendor capabilities, and the variability of state situations make it overly simplistic to say cloud computing is the answer. One size does not fit all. Without saying that "we" in government are unique – we've all heard that before from individual agencies – we have to say to vendor partners, we can do this when we're sure we're on a common wavelength within the context of laws, our strategic needs, our business drivers, the legacy environment, and known costs. Above all, we need to be able to guarantee our data is secure, and that the provider understands just how complex state government security requirements may be. In evaluating external cloud providers, even public cloud services, there is the reality that such services may actually more fully comply with security requirements and be more secure than internal agency-specific IT resources or state-wide enterprise services.

Cloud services must necessarily be governed and managed with the same or higher rigor than existing government IT services. The management and oversight could be potentially *higher* when a state government is "entrusting" to an outside provider the responsibility, accountability, and risk for delivering government business services. Accountability and risk cannot be completely transferred to an outside provider. However, it may be shared when cloud services are employed.

The requirements and performance levels for security and information assurance in the cloud environment are subject to the same operating discipline as any other environment. Statutory requirements are as applicable to cloud services as they are to any other approach for managing state government information assets; the obvious difference is state government will be, in some cloud deployment scenarios, delegating traditional state roles and responsibilities for security to an external provider through a contractual agreement. This approach is certainly not new to the state IT business model, however off-premise, third party hosted cloud services bring new and different dimensions to the conversation. The specifications for such services must not only describe the basic capability being provided, but must also identify the relevant requirements that surround the delivery of such services. These requirements must be reviewed and potentially updated to comply with state government requirements for security, privacy, availability, response time, backup and recovery, continuity of operations, and records management.

The Move to Cloud: Enterprise Security Architecture is Vital

Protecting the state's digital infrastructure and citizen information is a top priority for State CIOs. This does not change in a cloud services world and in fact *may be amplified*. Guided by accepted security principles, policies, practices, and frameworks, the security domain within the enterprise architecture now expands to embrace cloud services. Released by NASCIO in 2011, ***The Heart of the Matter*** recommends a core security services taxonomy for critical IT security services to facilitate the analysis of requirements, sourcing options, and costs for delivering appropriate security. An earlier NASCIO brief, ***Desperately Seeking Security Frameworks – A Roadmap for State CIOs***, describes the framework of security standards that states use to develop enterprise policies, standards, and controls to maintain information security in state governments. These are elements of security architecture designed to reduce risk and maintain and improve the trust in state government.

It is these standards and core services that state CIOs, chief information security officers, and the security programs they manage apply in their analysis of cloud computing solutions.

It is up to the CIO, aided by security staff, to steer a path through what can be a labyrinth of uncertainty, while staying focused on cost effective solutions and risk reduction.

The Security Frameworks brief and other NASCIO policy research have emphasized, however, the significant variance at the state level in the security architecture and standards being applied, due to decentralized agency approaches, stove-piped funding, and variation in federal requirements that render the state environment less uniform than that of their federal counterparts. The states, for example, do not have to comply with a uniform security compliance standard like the Federal Information Security Management Act of 2002 (FISMA) as federal agencies must. Security programs associated with individual lines of business within states have garnered varying levels of support, so that, for example, health-related security programs (HIPAA) may be significantly better supported than others; the case is the same for criminal justice (CJIS) and tax agencies (IRS Publication 1075). The trend has been that as state IT has been consolidated and rationalized, the security programs have been more uniformly supported, and an enterprise approach is highly visible in leading-edge IT environments. However, as national assessments and surveys have pointed out, IT security at the state level is generally underfunded, and in individual situations not as mature as expected, with some decentralized programs facing greater challenges than their more highly consolidated neighbors.

The same variety of funding levels from program to program has also contributed to a landscape in which very large legacy systems live alongside systems built with considerably more modern architectures. These twin variables, the built environment and non-uniform security standards, complicate enterprise planning as it addresses cloud computing, and pose the risk that lines of business will pressure CIOs to advance into the cloud to meet strategic objectives that are local rather than enterprise in nature. It is up to the CIO, aided by security staff, to steer a path through what can be a labyrinth of uncertainty, while staying focused on cost effective solutions and risk reduction.

The Early Adopters: State Approaches

In general, states have taken a slow and, we would argue, prudent approach to cloud adoption. CIOs have been busy looking at the literature and technical capabilities of cloud, consulting with peers across the country, examining proven use cases, exploring the legal issues, and continuing to monitor the FedRAMP process as it clarifies security requirements and identifies viable cloud providers. The general state approach to cloud adoption has been in the development of private cloud solutions and in the migration to enterprise email solutions in both private and public cloud scenarios. In these initiatives, states are learning from each other. And, more state and state agency partnering is evolving as cloud computing is being examined across the various lines of business, disciplines, and professional associations that serve state government. All of this activity is converging on a developing government strategy for maturing and harvesting the value of cloud computing. Delaware and Michigan offer examples.

- **Delaware Cloud-First**

The federal government's cloud-first policy has at least one state convinced in the case of Delaware, which developed a comparable cloud-based program beginning in 2011. To ensure that security concerns were addressed by agencies as they acquire cloud services, the Delaware Department of Technology and Information staff invested much time and effort in developing new terms and conditions for inclusion in the state's standard procurement process.

What was critical in this effort, Delaware CISO Elayne Starkey explained, is that multiple perspectives were represented in their deliberations. "With our prime focus on protecting citizen data," Starkey said, "we felt it was possible to mitigate risks significantly and to establish a common understanding of what services can move to the cloud quickly and what may at present not be good candidates."

Starkey noted that business leaders in Delaware were excited by the hype surrounding cloud technologies and eager to adopt them quickly. Through discussions at a series of meetings with business and fiscal leadership, systems architects, engineers, telecommunications staff, and subject matter experts, they developed twelve terms and conditions that must be included in all RFPs where external cloud solutions may be considered. Along with these, they developed twenty statement of work (SOW) clauses, which are used where the sensitivity of information to be maintained in the cloud solution dictates. Both the terms and conditions and the SOWs are available on Delaware's website.[2]

- **Michigan MiCloud**

The state of Michigan has taken a proactive approach to cloud adoption though its MiCloud initiative, which encompasses a private data center cloud that provides services to state and local governments there. As Michigan's strategic IT plan notes, MiCloud, provides governance and direction for cloud-computing efforts, with a focus on proving, piloting, and sourcing the state's government cloud offerings. With a focus on transforming government operations, Michigan is moving toward leveraging the cloud to provide clients with rapid, secure, and lower-cost services. Michigan's perspective is that not all functions are adequately supported by cloud today. MiCloud is regarded as a key component of

Michigan's enterprise sourcing strategy, which is secure because it's private and on premises. Through MiCloud, Michigan is using a unified and tiered approach to manage both primary and secondary business support functions. Targeted functions are based on business criticality, security requirements, and legal constraints.[3]

- **Enterprise Email and Office Productivity in the Cloud**

Many state governments have moved or are in the process of migrating to email in the cloud, either in public cloud or private cloud scenarios. At a panel discussion at NASCIO's 2011 annual conference, state CIO participants commented that email can be regarded as a "commodity" service and represents the low hanging fruit for cloud consideration. That has certainly been borne out in the number of adoptions, with examples from Colorado, Florida, Minnesota, Nebraska, New York, North Dakota, Ohio, Oregon, Utah, and Wyoming, already in the process of moving to or already up and running in cloud systems.

[It] is critical that states work to ensure that a common vision and interpretation of security requirements is established among all the stakeholders of an enterprise email solution.

These early adopters are of interest from a security perspective because of differences of opinion and experience in terms of the capacity of given cloud solutions to meet enterprise security requirements. As press reports indicate, adoption of cloud email in Los Angeles County California in 2010 was problematic due to the claimed inability of their solution to meet criminal justice (CJIS-related) security requirements imposed by the police department. Solutions in the states of Florida and Minnesota do meet CJIS requirements according to security staff in both states, though as one CISO pointed out, "we're not really compliant until an audit demonstrates we are, and we're not to that stage yet." The trend in request-for-proposal (RFP) language for those states going out to bid for cloud email solutions is toward greater and greater specificity in terms of security requirements. Direct reference, for example, to FISMA standards is increasingly present in procurement language.

Beyond the identification of security standards, however, it is critical that states work to ensure that a common vision and interpretation of security requirements is established among all the stakeholders of an enterprise email solution. A claimed ability to meet FISMA requirements, IRS 1075 requirements, HIPAA, or any other security standard, hinges on the validation of that by the Federal agency that is imposing and interpreting the standard in the first place. This underscores the importance of the identification of a core set of security requirements and controls at the federal level and a uniform interpretation of those as they are applied by states across the full range of agency lines of business. As part of NASCIO's continuing advocacy effort focused on federal reform, it continues to be critical that the harmonization and rationalization of federal security and audit requirements be pursued.

- **State of Florida – Building Partnerships**

Florida CISO, Mike Russo cites long term involvement and discussion with the FBI staff as key to gaining agreement that Florida's enterprise email system meets Criminal Justice Information Systems (CJIS) security requirements. The enterprise security program in Florida, like that in other best practice states, has involved agency-level chief information security officers dating from September 11th, leading to a deep understanding of the security requirements across horizontal lines of business, as well as the vertical lines of federal, state, and local government. This established a level of trust between public

safety agencies on all three levels of government and a capability to define requirements appropriately in discussions with the platform provider and the system integrator and the delivery of an enterprise email system regarded by Florida as among the most robust in the nation.

Federal Approach and the Role of FedRAMP

The federal government's approach to cloud computing was driven forward significantly by former US CIO Vivek Kundra's commitment to a cloud-first strategy and through the 2010 *25 Point Implementation Plan to Reform Federal Information Technology Management*. A key element of the 25 Point plan was the requirement placed on agencies that they identify three "must move" services for migration to the cloud, one of which was to be migrated within a year, and the other two within eighteen months. To support that migration, the Federal Risk and Authorization Management Program (FedRAMP) was initiated to ensure agencies would meet security requirements derived from FISMA, through use of carefully vetted products. At the same time that several federal agencies, including the General Services Administration, the Department of Agriculture, and NOAA, began migration to cloud email solutions, work by the National Institute of Standards and Technology (NIST) began clarifying key technical controls that would have to be present in cloud services to guarantee the security of data at varying levels of risk.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant agency security assessments.

FedRAMP is a federal government-wide program mandated by the Office of Management and Budget that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. It establishes a common set of security requirements and a baseline for evaluating and authorizing cloud service providers. Through FedRAMP, vetted cloud service providers gain an authorization to operate from the Joint Authorization Board, comprised of representatives of the Department of Defense, the Department of Homeland Security, the General Service Administration, and federal CIOs. An approved list of third party assessment organizations is maintained by the FedRAMP Program Management Office. Further, approved providers applying for authorization to operate must use an accredited third party assessment organization. The initial authorizations for cloud providers are slated for mid-2012.

FedRAMP will maintain a repository of approved cloud systems. Cloud systems not already approved can be subjected to the FedRAMP approval process which culminates with the granting of an authorization to operate (ATO) for that service, or a rejection of the cloud system if it does not meet FedRAMP requirements. Entrance criterion for FedRAMP approval is the successful passing of an assessment by a certified third party assessment organization.

Authorizations to operate must be continually maintained in order for a cloud system to remain in the FedRAMP repository. FedRAMP requirements must be articulated in contracts and terms of service agreements. FedRAMP provides templates with standard language for contract clauses.

Third party assessment organizations (3PAO) must in turn be accredited by meeting ISO/IEC 17020:1998 for independence and management competency,

and the FISMA for technical competency. Essentially 3PAOs must maintain competency, independence, and rigor. Accreditation must be maintained through the FedRAMP conformity assessment. The outcomes of such an assessment will result in maintenance, suspension, or revocation of accreditation of the 3PAO. 3PAOs approved and accredited are listed on the website for FedRAMP – www.FedRAMP.gov.

To reiterate a previous point, cloud systems must be managed against the same standards and best practices as internally developed systems. Those standards and best practices entail enterprise architecture, governance, data management, records management, security, and privacy. FedRAMP requires the assessment of cloud systems in accordance with FISMA. This is consistent given federal agencies are already required to assess and authorize information systems in accordance with FISMA. FedRAMP is merely reinforcing this compliance requirement with any cloud service.

FedRAMP will be a valuable resource for state and local government going forward. It should be used as a reference in vetting cloud providers, potentially requiring current ATO status for a vendor to be considered, and require maintenance of ATO status in state government terms and conditions.

Emerging Risks: The Rogue Cloud User

State IT security programs appear to be swimming against the current when it comes to controlling use of personal storage by employees and contractors eager to exploit always-connected access to state data, whether from their personal devices, other portable tools, or their home computers. In February 2012, the state of Delaware, queried other state CISOs on their policies toward use of online file storage sites, asking three straightforward questions:

1. Does your security or acceptable use policy allow use of online storage services?
2. Do you block employees from navigating to sites like Dropbox and Google Docs?
3. If you allow use, what steps do you take to reduce the risk of non-public data leaving your organization?

The majority of states appear not to explicitly forbid external storage use, but all CISO's believe there is significant risk in the uncontrolled use of these services.

Sixteen states responded to Delaware's inquiry, and the issues were also discussed in NASCIO's Security and Privacy Committee during its March 2012 call. The majority of states appear not to explicitly forbid external storage use, but all CISO's believe there is significant risk in the uncontrolled use of these services. A number of states are allowing individual agencies to establish policies, with the expectation that those agencies that are routinely dealing with sensitive data will tightly control or forbid external storage. From an enterprise perspective, both policy-based and technical controls have been implemented in efforts to manage or constrain

use, and a number of states are identifying approved solutions which adequately protect data according to its assigned level of sensitivity. Even the states that have taken the strongest positions on disallowing use see significant pushback from agencies, and most allow business exceptions to established policies.

While a few states note that they've not seen much use yet, states that are monitoring and or blocking access to cloud storage note their astonishment at the numbers of employees that are using free external online storage. Michigan's CSO Dan Lohrmann noted, "A few years ago, we had an employee who was sending data from their PC to a free data storage service which we found out was hosted in China. Thankfully, this individual was not storing any sensitive data at the time, but was considering using the 'free' storage for more mission-essential files. We have since put in controls to ensure that external data storage in the cloud is done with appropriate levels of compliance. Other employees were using services that were not intended for businesses or government enterprises, but individuals. The terms and conditions for those cloud services forbid business use without the appropriate license purchase and consent to legal language that was in conflict with the state indemnification laws."

Lohrmann also commented that security programs are going to find they need extra staff just to monitor this usage, unless technical controls, clearer policies, and better employee and business-level awareness take effect.

Forward-looking programs, as always, are striving to find ways to say "yes" to agencies and end-users without assuming undue risk. The state of Utah in its recent guidance on use of the iPad tablet for business purposes identified a specific external storage provider, recognizing that business requirements and user expectations offer strong justification for the use of external services. NASCIO has addressed the issue of mobile device use and exploding mobile device use in prior briefs and will continue to research and survey best practice in this area.

It is important to note that state government personnel cannot comply with security requirements if they are not aware of them, especially use of free, third party hosted cloud services. Employees, policy makers, and volunteers may have the best intentions in mind when employing external services for data storage, processing, analysis, and reporting. In most instances, they clearly don't understand the potential security risks. Therefore, any effective security program must engage employees and policy makers as necessary partners in securing state government knowledge assets. Security is not "done to them" or "done for them." Rather, it is accomplished "with them." Building such a partnership requires the necessary politics, communication, presentation, marketing, and relationship building to ensure everyone in state government embraces security as an essential dimension of the business of government.

Recommendations

This report has provided a discussion of some of the issues regarding cloud security and privacy. The discussion will continue going forward as new lessons are learned and new requirements arrive. In summary the following recommendations are presented. Treat these recommendations in the spirit of, "this is what we know at this time." Stay tuned to NASCIO and other knowledge centers for future recommendations.

- ***Mobilize internal support for cloud adoption through education and awareness, while clearly articulating the new security and privacy risks***

  The movement to cloud services will be transformational and will require early education on the changing business model and relationships. Before embarking on a major cloud initiative, gain clear support from budget directors, procurement officers, chief operating officers, and agency department heads. Legislators, especially those with jurisdiction and influence over IT resources, should be consulted. Be clear to communicate the value proposition of cloud services and potential savings while emphasizing the commitment to security and privacy.

- ***With cost reduction as the major driver of cloud adoption in state government, CIOs must weigh the benefits and risks of cloud computing in terms of cost versus security and privacy concerns***

  A singular focus on cloud cost savings is short-sighted. For third-party hosted cloud solutions, be prepared to negotiate the service levels while remaining resolute about security requirements. The determination of the "best" cloud model may be a hybrid solution that will increase the total costs over the long term. What may be presented initially as a "bargain" may eventually evolve into a very expensive alternative, once the service and performance requirements are added.

- ***Continue to temper expectations about savings opportunities and to examine risk and requirements***

  Provide briefings to policy makers regarding the hype and the value of cloud services. Emphasize the fact that initial presentations on pricing may look extremely attractive, but there are many necessary safeguards and requirements related to security, privacy, records management, and continuity of operations that must be provided depending on the type and classification of data and information. Such requirements dramatically affect the final pricing. Further, existing real costs must be fully accounted for and established as a baseline for comparison.

- ***Educate policy makers on the differences: consumer cloud versus industrial strength requirements of state government***

  With the broad adoption of consumer cloud services for email, social media, and storage, the general perception of state policy officials, legislators, and other decision makers may be biased by the "this is easy" belief. "Free" cloud services are now heavily advertised to the

consumer. Anticipate this view and be ready with good answers on the differences, especially concerning security requirements and protecting citizen information.

- ***Examine the state's standard terms and conditions for procurement and consider modifications to address cloud computing***

  Partner with the state procurement official, legal staff, and domain experts to review current procurement regulations, policies, and practices that inhibit the consideration of external cloud service offerings. Assess the need for revised contract provisions to protect the security interests of the state. For example, refer to work in the State of Delaware.

- ***Communicate and educate government officials on the terms of service presented and assumed for third party cloud services***

  Provide interpretation of such terms of service and the potential risks for government employees and citizens. Government personnel, contractors, and citizens must understand that contracting for third-party cloud services without proper legal and security review can result in citizen and government data being publicly released. This action puts the citizen and government at risk and can result in litigation that involves the employee or contractor that engaged the service.

- ***Where state data is highly sensitive, start with a private cloud solution first***

  States like Utah and Michigan have presented an excellent example for "getting started." Begin with publicly available data and core enterprise services as a first step in moving toward a cloud first strategy.

- ***Develop an enterprise security policy that controls unauthorized use of cloud services while enabling legitimate business needs***

  Determine how to best achieve the awareness and trust to help ensure employees and agencies engage the CIO's office to evaluate and enable business needs with appropriate business and IT services. Create or procure a fully compliant cloud storage service that meets the needs of specific users.

- ***As with any policy, expect compliance issues and continually scan network traffic to uncover the use of unauthorized cloud services***

  Security awareness and education must be continually maintained. There should be a major effort at building awareness followed by a strategy for maintaining such. When non-compliance with policy is discovered, the response should be to uncover the underlying business need for engaging unauthorized cloud services, and learn how to make the awareness program more effective. The CIO's office will need to create and maintain a communications and marketing strategy to ensure state government understands the capabilities that office provides for enabling business needs through internal as well as external service providers. It must also ensure that it offers properly vetted cloud services as part of its portfolio of services.

- ***Consider a cloud broker approach***

  The state of Minnesota has been developing and maturing this role within the office of the state CIO. There will be a continuing development of new roles such as "broker", "service portfolio manager," and other roles that will eventually have established best practices, scope, responsibilities, and, potentially, professional qualifications and certifications. Security should certainly be an element of the broker role.

- ***Work with Federal government to develop common interpretation of security requirements so that comprehensive cloud requirements can be identified and relied upon***

  Federal initiatives and guidance will continue to be a valuable resource for state government. NASCIO will continue to advocate for a harmonization with respect to federally funded programs and security requirements. Stay tuned to NIST, GAO, OMB, the Federal CIO Council, and federal agencies regarding issue exploration, best practices, strategies, and progress reports related to cloud computing.

- ***Stay tuned to FedRAMP as it evolves and leverage approved vendors***

  This will be a valuable resource and reference to state and local government in planning, designing, and implementing cloud services. For example, FedRAMP approved providers should be referenced when evaluating cloud providers. The FedRAMP list of cloud service providers (CSP) with a current authorization to operation (ATO) will provide an essential "starter list" of approved vendors.

Appendix – Cloud References

The Australian Government Cloud Computing Strategic Direction Paper
www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf

The Department of Finance and Deregulation, through the Australian Government Information Management Office, has consulted with government agencies, industry and the public to develop an Australian Government Cloud Computing Strategic Direction paper to explore the opportunities and impacts of cloud computing.

Cloud Computing Use Cases Group (Google group)
http://groups.google.com/group/cloud-computing-use-cases

This group is devoted to defining common use cases for cloud computing.

Computer Crime & Intellectual Property Section, United States Department of Justice
www.justice.gov/criminal/cybercrime/ssmanual/

The purpose of this publication is to provide Federal law enforcement agents and prosecutors with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations. Chapter 3 of this publication presents the Stored Communications Act (SCA). The significance of the SCA is that it imposes The SCA governs how investigators can obtain stored account records and contents from network service providers, including Internet service providers ("ISPs"), telephone companies, and cell phone service providers.

Cloud Customers' Bill of Rights
Information Law Group LLP - www.infolawgroup.com

The InfoLawGroup has issued a "Cloud Customers' Bill of Rights" to serve as the foundation of a cloud relationship, allow for more transparency and enable a better understanding of potential legal risks associated with the cloud.

Detailed descripton of the Cloud Customers' Bill of Rights
www.infolawgroup.com/2010/10/articles/cloud-computing-1/cloud-computing-customers-bill-of-rights/

The Cloud Security Alliance (CSA)
https://cloudsecurityalliance.org/about/

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Federal Cloud Computing Strategy
www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

This Federal Cloud Computing Strategy is designed to:
Articulate the benefits, considerations, and trade-offs of cloud computing
Provide a decision framework and case examples to support agencies in migrating towards cloud computing
Highlight cloud computing implementation resources
Identify Federal Government activities and roles and responsibilities for catalyzing cloud adoption

The Jericho Forum (The Open Group)
www.opengroup.org/jericho/

Jericho Forum is the leading international IT security thought-leadership association dedicated to advancing secure business in a global open-network environment. Members include top IT security officers from multi-national Fortune 500s & entrepreneurial user companies, major security vendors, government, & academics. Working together, members drive approaches and standards for a secure, collaborative online business world.

National Institute of Standards and Technology Cloud Computing Program
www.nist.gov/itl/cloud/index.cfm

The long term goal of this program is to provide thought leadership and guidance around the cloud computing paradigm to catalyze its use within industry and government. NIST aims to shorten the adoption cycle, which will enable near-term cost savings and increased ability to quickly create and deploy enterprise applications. NIST aims to foster cloud computing systems and practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios.

The TechAmerica Foundation
http://www.techamericafoundation.org/leading-cloud-thinkers-to-government-cloud-is-imperative-for-better-collaboration-better-service-and-better-cost

The TechAmerica Foundation released recommendations from the State and Local Government Cloud Commission (SLG-CC) that will assist state and local governments in navigating the adoption of cloud computing. The roadmap is designed for state and local officials who seek to deliver better service and cost savings to their constituents. This practical guidance and set of recommendations comes from the leading thinkers on cloud computing.
http://www.techamerica.org/Docs/fileManager.cfm?f=taf_slg_cc.pdf

The Open Cloud Manifesto
www.opencloudmanifesto.org/

Dedicated to the belief that the cloud should be open. This effort intends to initiate a conversation that will bring together the emerging cloud computing community (both cloud users and cloud providers) around a core set of principles. We believe that these core principles are rooted in the belief that cloud computing should be as open as all other IT technologies.

Acknowledgements

The following individuals were consulted or provided helpful review comments in the development of this brief:

Chris Buse, Chief Information Security Officer, State of Minnesota

James Earl, J.D., Executive Director, Technological Crime Advisory Board, State of Nevada Management and Budget

Christopher G. Ipsen, CISSP-ISSAP, CISM, Chief Information Security Officer, State of Nevada, Department of Information Technology

Daniel Lohrmann, Chief Security Officer, Department of Technology, Management and Budget, State of Michigan

Paulina Orlikowski, USPS State & Local Division, Portfolio Manager, HP

Andris Ozols, Chief Policy Advisor, State of Michigan, Department Technology

Rodney Peterson, Senior Government Relations Officer & Managing Director of Washington Office, EDUCAUSE

Doug Robinson, *Executive Director, NASCIO*

Mike Russo, CISSP, PMP, CFE, CGEIT, State Chief Information Security Officer, Chief of Staff, State of Florida

Elayne Starkey, CISO, State of Delaware

David Taylor, Chief Information Officer, State of Florida

Endnotes

[1] This issue brief is part IV in a series on cloud computing and will focus on security issues. Previous issue briefs in this series are available at www.nascio.org/publications.
[2] See http://dti.delaware.gov/pdfs/pp/Cloud-External-Hosting.pdf.
[3] See http://www.michigan.gov/documents/dmb/Appendix_K_354571_7.pdf.

DISCLAIMER
NASCIO makes no endorsement, express or implied, of any products, services, or websites contained herein, nor is NASCIO responsible for the content or the activities of any linked websites. Any questions should be directed to the administrators of the specific sites to which this publication provides links. All critical information should be independently verified.

This project was supported by Grant No. 2010-DJ-BX-K046 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.