# NASCIO Call-to-Action:

## The Necessity for Maturing Identity and Access Management in State Government

November 2012

*NASCIO Staff Contact:*
Chad Grant, Senior Policy Analyst, NASCIO

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



For those of us who have come to rely upon the Internet for day-to-day actions related to work, keeping in touch with friends, and banking, among so many others, it has become second nature to log-in to our accounts with passwords. We power-up our smartphones, tablets, laptops, and the numerous other devices that now connect us to resources on the internet, including ever increasing services and products which previously required in person presence.

Like all advances, these new capabilities inevitably have their own set weaknesses that perpetrators can exploit. On the internet, 11.7 million Americans fell victim to identity theft over a two year period, resulting in the loss of billions of dollars.[i] That is an astonishing number, but one of the biggest contributing factors to identity theft has been the cache of passwords we have tucked away in our memory or haphazardly jotted down. Not all, but most would confess that we simply re-use the same password over and over to simplify our lives. Identity thieves surely appreciate this simplification.

As state leaders act to streamline services, consolidate IT infrastructure and perform more efficiently, trusted digital identities and their authentication becomes a critical enabler with the digital ecosystem. All levels of government and the private sector, are confronted by this challenge and are working together to create common policy, guidelines, standards, and responsibilities to protect cyber assets and ensure appropriate mechanisms are in place for a coordinated identity ecosystem. In states, Chief Information Security Officers (CISOs) have placed a renewed emphasis on cyber security strategies – making data protection one of the top five initiatives.[ii]

In general, a few key factors that states should consider prior to advancing an identity and access management strategy:

- What critical service capabilities or business drivers would push your state leaders to adopt an enterprise-wide approach to identity and access management?
- How can your state use identity and access management to enable services and workflow?

## Call to Action Summary

- Promote the SICAM Guidance and Roadmap to improve business processes and efficiencies, and reduce cyber risks.
- Support SICAM guiding principles and incorporate within state initiatives and strategic planning.
- Participate in NASCIO Work Groups to share, obtain and mature best practices.
- Access your state's progress in breaking down silos and streamlining services.
- Evangelize the business drivers of SICAM and highlight examples of ROI to states.

- How can identity and access management help your state protect critical assets?
- What operational efficiencies can be gained with an enterprise-wide approach to identity and access management?
- How can your state increase data sharing and management with a secure and privacy enhancing framework?
- Does your state have significant administrative and technological overhead caused by siloed, incompatible, and un-audited identity management systems? Can you demonstrate a Return on Investment (ROI) for consolidated services?
- Is your state in the planning stages of an enterprise-wide project like Enterprise Resource Planning (ERP) or Human Resources (HR) information systems? How can states leverage identity management for enterprise-wide projects?

***The National Association of State Chief Information Officers (NASCIO) calls on state CIOs and state leaders to integrate the State Identity Credential and Access Management Guidance and Roadmap (SICAM) as a domain discipline within their states existing enterprise architecture. Enhanced security, Return on Investment (ROI) and increased compliance is co-conditional on the organizational alignment and governance structuring. The authority granted to state CIOs to implement SICAM may vary, but it is critical that states use an enterprise-wide approach to identity management.***

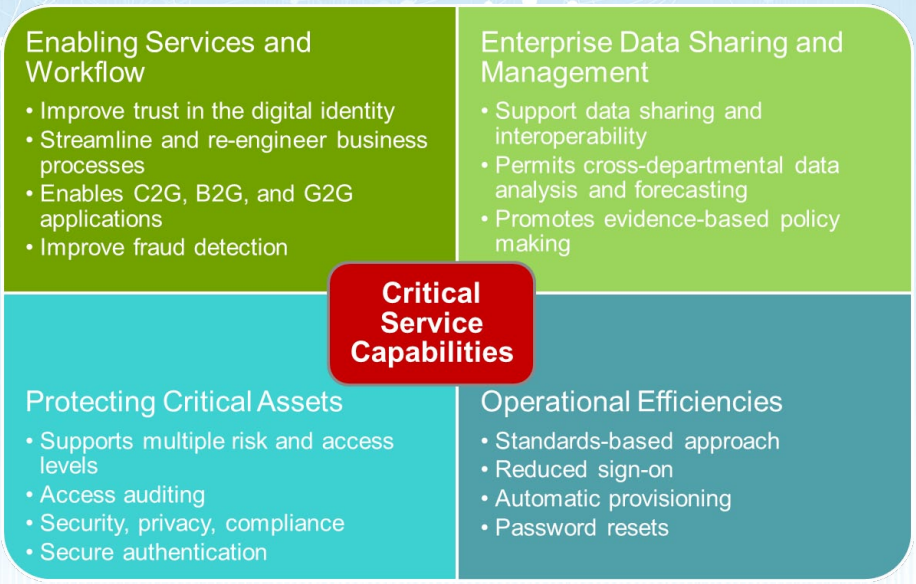
**States are the Nexus of Identity**

Some countries in the world have adopted a national identifier for logical and/or physical access, transactions, and exchanges. The constitutional structure and practices in the United States emphasized the state primacy in this role. State and local governments are the nexus of individual identity. States provide the public with cradle to grave forms of identification, such as birth certificates, driver licenses, marriage and death certificates, and numerous other forms of identification used on a daily basis.

In providing these services, states collect, aggregate, exchange, and store Personally Identifiable Information (PII) presenting states with increased responsibilities, risks and liabilities. Further, traditionally programs, benefits, or services were developed with a single purpose identity, credential, and access management strategies. While single purpose identities were appropriate for 20th century programs, it now burdens states with high operating costs, increased PII liability and data conflict, decreased enterprise efficiencies, and negative user experiences. By taking an enterprise approach to identity and access management, states can improve critical service capabilities within the state operations and with trusted external partners while better managing their risk and liability.

The NASCIO community has recognized the need for a state-based strategic vision for identity, credential, and access management efforts. Working with thought leaders, and leveraging public and private sector best practices, NASCIO developed and published the State Identity and Credential Access Management Guidance and Roadmap (SICAM).

The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries. This will significantly reduce administrative and technological overhead




caused by siloed, incompatible, and un-auditable identity management systems, lead to improved business processes and efficiencies, and reduce cyber security risk. The architecture, principles, and implementation approaches outlined in the SICAM Guidance and Roadmap can be leveraged by states in support of increasing service capabilities. The chart above highlights the benefits of an enterprise approach to identity management.

***NASCIO urges state leaders to adopt SICAM as the basis for an enterprise approach to identity and access management. States like Michigan and Virginia have already included identity and access management into strategic plans as a way to manage access to enterprise resources (systems and data) by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity.***[iii]

**A Holistic Approach with Fewer Silos Means Big Benefits**

A key aspect of access management is the ability to leverage an enterprise identity for numerous purposes. Logical and physical access is often viewed as the most significant part of ICAM from a return on investment perspective. To maximize that return, a successful access management solution is dependent on identity, credentials, and attributes for making informed access control decisions, preferably through automated mechanisms. The level of investments made must allow for the construction and development of all the foundational elements from which ROI is derived. Lack of strong ROI benchmarks and support evidence has hindered broader adoption of ICAM as a service.

Challenges that states will need to address [iv]:

- Insider threats
- Non-repudiation
- Least privilege/need-to-know
- Segregation of administrative (provider) vs. end user (client)
- Interface and access
- Delegation of authorizations/ entitlements
- Password management (communication, retrieval); different requirements across clients
- Resource hogging with unauthorized provisioning
- Complete removal of identity information at the end of the life cycle

- Attacks on identity services
- Eavesdropping on identity service messaging
- Dynamic trust propagation and development of trusted relationships among service providers
- Transparency: security measures must be available to the customers to gain their trust
- Developing a user-centric access control where user requests to service providers are bundled with their identity and entitlement information
- Real-time provisioning and de-provisioning of user accounts
- Lack of interoperable representation of entitlement information
- Interoperability with existing IT systems and existing solutions with minimum changes
- Dynamically scale up and down; scale to hundreds of millions of transactions for millions of identities and thousands of connections in a reasonable time
- Privacy preservation across multiple tenants
- Multi-jurisdictional regulatory requirements

There are several major state led ICAM implementation efforts underway to leverage enterprise identity services. These efforts include health and benefit programs, driver licenses, and department of licensing and regulation programs. Once completed, these efforts might provide strong ROI benchmarks and support evidence support broader adoption of ICAM as a service.

***NASCIO encourage state leaders implementing enterprise approaches to identity and access management and SICAM to document and benchmark ROI elements. Use cases and best practices could then be offered as a way to exchange business drivers and solutions.***

**Harmonizing Public & Private Efforts**

Individual consumers and public and private sector organizations, communities and professions drive demand and requirements for services and delivery models found in today's identity ecosystem. While many applications require unique capabilities, many share common characteristics. Hundreds of organizations, associations, consumer interest groups and thousands of the public at large participated in a national discussion to create a strategy to evolve our identity ecosystem to support our new requirements and future needs. NASCIO and several states thought leaders played a critical role in this discussion.

The resulting national vision, entitled the National Strategy for Trusted Identities in Cyberspace (NSTIC), was signed by the President and released by the White House in April 2011. The NSTIC strategy is a vision for enhancing online choice, efficiency, security, and privacy while improving online digital identity trust, authentication, and resiliency. As the demand for secure credentials increases, the ecosystem will foster a vibrant marketplace that allows people to choose among multiple identity providers - private and public - that would issue trusted credentials that prove identity. A market place that allows citizens to Bring Your Own Identity (BYOI) could rapidly replace legacy and outdated system characteristics such as the vulnerable user name and password and the costly single purpose credentials.[v]

NASCIO is working to support a proper foundation for the identity ecosystem, essential to obtaining the envisioned levels of interoperability and core principles set forth in the NSTIC. The NASCIO SICAM Guidance and Roadmap seeks to align and reinforce NSTIC principles by focusing on the following objectives:

- **Increased security**, which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, SICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.
- **Compliance with laws**, regulations, standards and state policies.
- **Improved interoperability**, specifically between states using credentials along with other third party credentials that meet the requirements of the federated trust framework.
- **Enhanced customer service**, facilitating secure, unified, and user-friendly transactions – including information sharing – translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.
- **Elimination of redundancy**, both through agency consolidation of processes and workflow and the provision of government-wide services to support SICAM processes. This results in extensibility of the IT enterprise and reduction in the overall cost of security infrastructure.
- **Increase in protection of personally identifiable information (PII)** by consolidating and securing identity data through the use of encryption, improving access controls, and automating provisioning processes.
- **Enhanced Privacy**, transparent process and notice regarding the collection, use, dissemination and maintenance of information.
- **Voluntary**, self-determining participation within an identity and access management system.

Across the state enterprise, state CIOs and IT professionals must routinely coordinate, harmonize, and attest to compliance with diverse, inconsistent, and un-integrated federal department and agency programs and technical and policy requirements. Concurrently, they are challenged with maintaining and enhancing priority enterprises services with state and local government, regional authorities, and the private sector. Responsibilities span diverse state functions such as benefit programs, health care, law enforcement and public safety, transportation, and tax collection – and hundreds more.

In this environment, states leaders routinely conduct publically and privately funded pilots and prototyping efforts. Examples include NSTIC funded trust framework pilots, U.S. Department of Health and Human Services (HHS) funded health exchange pilots, U.S. Department of Homeland Security (DHS) and U.S. Department of Transportation (DOT) funded Department of Motor Vehicle (DMV) validation architectures, DHS and DOJ funded screening and communications efforts. Each one of these possesses an identity and access management element.

Not every state has received pilot funding for identity management, but states should reinforce the SICAM principles and leverage their experience by benchmarking and documenting major ICAM efforts and lessons learned, supporting cross community awareness, and accelerate learning for more effective community adoption and implementation.

***With the release of the SICAM Guidance and Roadmap, NASCIO has made an initial effort to align and reinforce key NSTIC principles of privacy enhancing and voluntary, secure and resilient, interoperable, cost effective, and easy to use. States should consider the potential benefits of adopting these guiding principles when strategizing on state initiatives.***

**Taking an Active Role in the Identity Ecosystem**

The NSTIC National Program Office (NSTIC NPO) is coordinating and facilitating with ecosystem community members to create the necessary governance structure for the ecosystem. NPO released "Recommendations for Establishing an Identity Ecosystem Governance Structure" in February 2012 that provided guidance for a formal NSTIC Steering Group that would be led by the private sector and self-sustaining in the future.

Initial governance development has begun. An Identity Ecosystem Steering Group (IDESG) is now formed and a Secretariat functions is established.[vi] Several Working Groups and Standing Committees are beginning to meet regularly and NASCIO, in addition to several states, have already signed up for and are participating in the IDESG, working group and committee efforts. Additionally, the NPO has funded 5 initial proposals consortium-based proposals to encourage ecosystem participation and development.

While many states would quickly jump at the opportunity to host an IdM pilot, unfortunately the NPO funding is not nearly sufficient to do so. States should be coordinating with other states and collaborating with key stakeholders, such as the NASCIO State Digital Identity Working Group and the American Association of Motor Vehicles Administrators (AAMVA) eID Working Group, in order to share best practices and develop a community of active participants from various levels of government.

***NASCIO encourages interested state leaders to participate in SICAM and NSTIC trust framework processes, pilots, and best practices. The NASCIO State Digital Identity Working Group is seeking input, participation and support on SICAM. Additionally, the NSTIC Steering Group membership is open to any individual, states and organizations interested in contributing to the mission of NSTIC, click here.***

**Final Recommendations to States**

NASCIO recognizes the important role of states in the Identity Ecosystem and urges members to support the guiding principles of SICAM in implementing an interoperable enterprise identity management solution in the states. Aligning SICAM with the vision of NSTIC is only in its infancy, but during this process state CIOs should anticipate being called upon to provide guidance on coordinating identity management systems. Extensive work will need to be done in order to provide a gap analysis of IT resources needed to meet the levels of assurance needed for integrating an enterprise-wide identity management solution. NASCIO calls on state CIOs, state CISOs, and other state leaders to:

- Promote SICAM as a critical framework within the enterprise architecture domain.
- Support the guiding principles of SICAM and incorporate these values in state initiatives and strategic planning.
- Participate in the NASCIO Digital Identity Work Group so that best practices and guideline's performed within state departments and

agencies.

- Take an active role in guiding the IDESG by participation in the working groups and standing committees.
- Access your state's progress in breaking down silos of identity management and promote the SICAM Guidance and Roadmap as a way to improve business processes and efficiencies, and reduce cyber risks.
- Evangelize the business drivers and ROI that SICAM can have by assuring the identity of an entity is verified and granted an adequate level of access based on an assured identity.

---

[i] U.S. Department of Justice, Bureau of Justice Statistics, December 2010. http://www.ojp.usdoj.gov/newsroom/pressreleases/2010/BJS11044.htm

[ii] 2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Col laboration and Compliance, October 2012. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2012.pdf

[iii] State of Michigan, "IT Strategic Plan: Enterprise Architecture (Appendix J)," 2012. http://www.michigan.gov/documents/itstrategicplan/Appendix_J_Enterprise_Architecture_327699_7.pdf

[iv] State of Hawaii, "Information Assurance and Cyber Security Strategic Plan," October, 2012. http://oimt.hawaii.gov/wp-content/uploads/2012/09/Governance_Info-Assurance_Cyber-Security.pdf

[v] Gartner, 2013 Planning Guidance: Identity and Privacy, November 2012. http://www.gartner.com/id=2221415

[vi] NSTIC Secretariat, Press Room, August 27, 2012. http://www.idecosystem.org/page/press-room