State eID Priorities, Issues and Trends

AAMVA 2012 International Conference
August 21, 2012

Chad Grant, Senior Policy Analyst
National Association of State Chief Information Officers
About NASCIO

- National association representing state chief information officers and information technology executives from the states, territories and D.C.
- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.
- Founded in 1969 – we’re a legacy system
Fiscal recovery uneven, slow revenue growth, budgets are better, federal deficit reduction impact?

CIOs seeking IT operational cost savings and alternative IT sourcing strategies

Opportunities for change and innovation

Living with the past - modernizing the legacy

IT security and risk! Game has changed

IT workforce: retirement wave, skills, recruiting

State CIO transition – major churn

State IT Landscape Today
Mid-Year Budget Cuts Continue to Decline

*FY 2012 mid-year budget cuts are ongoing

Source: NASBO, 2011
CIOs' view on IT budgets for 2013

- 80% of Federal grants go to states
- In the past, many CIOs saw budget decreases as an opportunity to improve by breaking down barriers, strengthening IT governance, developing creative solutions

- Optimistic outlook by state CIOs on IT budgets – 47% anticipate an increase for 2013

Source: NASCIO Midyear Conference, May 2012

States Only: Will your state IT budget grow or shrink and by how much?

- 9% a. Flat
- 47% b. Increase
- 25% c. Reduce by up to 10 percent
- 6% d. Reduce by up to 20 percent
- 13% e. What budget?
State CIO Transitions 2011-12

January 2011 - August 21, 2012

New CIO (32)
Acting/Interim CIO
## CIO Challenges, Concerns, Pain Points

<table>
<thead>
<tr>
<th>IT Governance: what works?</th>
<th>Lack of shared enterprise vision for technology</th>
<th>Supporting a legacy environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recruit and retain IT staff</td>
<td>Inadequate funding and budget constraints</td>
<td>IT procurement modernization</td>
</tr>
<tr>
<td>Managing mobile devices, BYOD</td>
<td>Information sharing/data exchanges</td>
<td>Identity management</td>
</tr>
</tbody>
</table>
View from the States: Priorities and Trends
State CIO Priorities for 2012

1. **Consolidation / Optimization**: centralizing, consolidating services, communications and marketing "enterprise" thinking, identifying and dealing with barriers

2. **Budget and Cost Control**: managing budget reduction, strategies for savings, reducing or avoiding costs, dealing with inadequate funding and budget constraints

3. **Governance**: improving IT governance, data governance, partnering, inter-jurisdictional collaboration, industry advisory boards, legislative oversight - achieving proper balance, agencies participating as members of a "state enterprise"

4. **Health Care**: the Affordable Care Act, health information and insurance exchanges, health enterprise architecture, assessment, partnering, implementation, technology solutions, Medicaid Systems (planning, retiring, implementing, purchasing)

5. **Cloud Computing**: scalable and elastic IT-enabled capabilities provided "as a service" using internet technologies; governance, service management, service catalogs, platform, infrastructure, security, privacy, data ownership, vendor management, indemnification, service portfolio management

6. **Security**: risk assessment, governance, budget and resource requirements; security frameworks, data protection, training and awareness, insider threats, third party security practices as outsourcing increases; determining what constitutes "due care" or "reasonable"

7. **Broadband and Connectivity**: strengthening statewide connectivity, public safety wireless network/interoperability, implementing Broadband Technology Opportunities Program (BTOP) grant

8. **Shared Services**: business models, sharing resources, services, infrastructure, independent of organizational structure, service portfolio management, marketing and communications related to organizational transformation

9. **Portal**: maturing state portal, e-government, single view of the customer/citizen, emphasis on citizen interactive self-service, accessibility

10. **Mobile Services/Mobility**: devices, applications, workforce, security, policy issues, support, ownership, communications, wireless infrastructure

*Italics*: New to list for 2012

Source: NASCIO State CIO Survey, October 2011
IT Security Risks in the States

- Critical infrastructure protection
- More aggressive threats – organized crime, unorganized crime, hacktivism
- Spam, phishing, hacking, and network probes up
- Advanced persistent threats
- Data breaches – trust impact!
- Insider threats, third party
- Securing mobile solutions, BYOD
- Identity and Access Management
- Inadequate funding
5. What percentage of your department’s overall IT budget is allocated to information security?

- 0%: 11%
- 1-3%: 50%
- 4-6%: 15%
- Greater than 11%: 7%
- Not applicable/Do not know: 17%

50 percent of the respondents indicated that 1-3 percent of their department’s overall IT budget is allocated to information security.

Source: 2010 Deloitte and NASCIO Survey: “State Governments at Risk”
Priority Technologies, Applications and Tools

1. Virtualization: servers, desktop, storage, applications, data center
2. Legacy application modernization / renovation
3. Cloud computing: software as a service, infrastructure, platform, storage
4. Mobile workforce technologies
5. Networking: voice and data communications, unified
6. Enterprise Resource Planning (ERP)
7. Identity and access management
8. Business Intelligence (BI) and Business Analytics (BA) applications
9. Document/Content/Records/E-mail management: active, repository, archiving, digital preservation
10. Public Safety Radio Network

Source: NASCIO State CIO Survey, October 2011
What are your State’s top five IT security initiatives?

- Information security strategy: 27%
- Information security governance (e.g., roles, reporting): 29%
- Aligning information security initiatives with those of the...: 21%
- Information security risk assessments: 58%
- Data protection: 60%
- Operationalizing information security: 15%
- Information security measurement and reporting: 42%
- Information security talent management: 4%
- Information security training and awareness: 54%
- Information security regulatory and legislative: 21%
- Information security infrastructure improvement: 33%
- Application security: 42%
- Identity and access management: 19%
- Security related to technology advancements (e.g.,...): 19%
- Information security compliance (e.g., internal / external...): 29%
- Managing insider threats: 4%
- Managing or outsourcing of security services: 10%
- Disaster recovery: 8%
- Business continuity: 6%
- Other (please specify below): 4%
- Not applicable/Do not know (please describe below): 0%

Identity and access management – 19%
State CIOs Recognize Why Identity Management Needs to be a Top Priority

- Supports national framework for interoperability providing interoperability and trust across multiple jurisdictions.
- Promotes state enterprise approach: avoids silos, avoids proprietary solutions. Adoption of the standards will reduce redundant credentialing efforts and expenditures.
- Follows the great work the states have led in improving drivers license issuance. FIPS 201 has a standardized identity proofing process and standardized issuance procedures. Provides strong proof of cardholder identity.
- Supports multiple applications & legacy infrastructure: issue once, use many times.
- Enables standards-based provisioning of access management and auditing
Digital Identity and the States

- States - nucleus of identity for individuals
- Identity - basis for providing services and sharing data across agencies
- Issue identity credentials - too many!
- Create identity silos
- Lots of technical, operational, policy and legal questions to resolve

States need a national framework for interoperability: a trusted federated identity model
Targets of Opportunity

- **Standardization**: IT and identity management costs driven by complexity and diversity – seek commodity solutions, encourage reuse. Need to align with Federal initiatives like NSTIC.
- **Rationalization**: Adoption of standards will reduce redundant credentialing efforts and expenditures.
- **Collaboration**: Federal, multi-state and local communication to enhance interoperability.
- **Innovation**: alternate operational models; enterprise services, not systems – more citizen centric. (states conduct millions of transactions a year)
NASCIO Perspectives: States and Digital Identity

- Complex problem – we need a shared vision and common objective across all state jurisdictions
- States “own” this issue - they need to resolve for their own purpose. Resolution will also support Federal needs
- Requires state-federal partnership & collaboration. DMV? Locals? Education?
- National framework for interoperability
State Government Challenges

- Value proposition and benefits
- Define the business drivers
- Architecture and standards
- Policies and business process
- Enrollment and issuance
- Funding and financing
- Acquisition and sourcing options
- Clarify the role of states (relying party, identity provider, etc.)
Enabling Services and Workflow

- Improve trust in the digital identity
- Streamline and re-engineer business processes
- Improve fraud detection

Enterprise Data Sharing and Management

- Support data sharing and interoperability
- Permits cross-departmental data analysis and forecasting
- Promotes evidence-based policy making

Protecting Critical Assets

- Supports multiple risk and access levels
- Access auditing
- Security, privacy, compliance
- Secure authentication

Operational Efficiencies

- Standards-based approach
- Simplified sign-on
- Automatic provisioning
- Password resets

Critical Service Capabilities

SICAM Guidance and Roadmap Business Drivers
If Digital Identity is a Priority...

What we should **not** do

- each state work independently
- use proprietary solutions
- disregard interoperability and a federated approach

What we should **do**

- work for a federated type solution
- standards based and competitively sourced
- ensure interoperability across governments
- promote the adoption of the NSTIC guiding principles and clarify the states role in the identity ecosystem
SICAM Document Background

- **Who participated**
  - NASCIO Digital Identity Working Group participants from across the country

- **Purpose**
  - Provide a standard, unified framework for all states to utilize and adopt
  - Provide definitions, architectural guidance, and describe processes
  - Develop a baseline for further discussion and improvement by NASCIO community

- **Scope**
  - Remote authentication of human users of state IT systems
  - Help identify and analyze risks during authentication process
  - Out of scope:
    - Authentication of system-to-system requests
    - Authorization to access resources was out of scope
    - Did not address electronic signature issues
SICAM Document Overview

- Goals and Objectives
  - Trust
  - Interoperability
  - Security
  - Process Improvements
- SICAM Maturity Model
- Principles, Processes, and Concepts
- Architecture Framework
- Implementation Strategy
  - Risk Assessment
  - Assurance Levels
  - Identity Proofing Requirements
  - Attribute Management
  - Governance
  - Architecture Compliance
SICAM Document Next Steps

- Release to stakeholder community
- Alignment with NSTIC Identity Ecosystem guiding principles
- Clarify the role of states with an emphasis on the governance structure
- Need to capture what the landscape looks like for state IdM. Benchmarking will enable states to track progress.
Looking Ahead

- Collaborate on building an identity ecosystem...2016?
- Support the emphasis on Chain of Trust
- *Leverage Federal initiatives*: more steering, less rowing?
- Identity implications of healthcare reform?
- Demand for secure identities by citizens
- Extending the enterprise: Federal, state, local, tribal, and territories?