# State of the States: Priorities, Trends and Issues

**Government Smart Card
Interagency Advisory Board (IAB) Meeting
March 26, 2014**

**Doug Robinson, Executive Director
National Association of State Chief Information Officers**

# Today's State IT Landscape

✓ Fiscal recovery:  CIOs still seeking IT operational **cost savings,** alternative IT sourcing strategies and **collaboration**

✓ **State CIO Balancing Act:**  supporting legacy,  business process transformation, innovation

✓ **Cybersecurity threats!** New technologies, new risks, governance is hard, collaboration needed

✓ **Technology as a service:** systems-centric *to* services

✓ State CIO transitions, continuing IT **workforce** retirements, skills gap, recruiting challenges

## 5) How would you characterize your IT budget this fiscal year? (State Government Only)

**18%** A. Increased by 10% or more

**45%** B. Flat

**21%** C. Reduced by up to 10% or less

**8%** D. Reduced more than 10%

**9%** E. What budget?

NASCIO
NASCIO TWO THOUSAND THIRTEEN
MIDYEAR CONFERENCE
April 28 - May 1 | Washington, D.C.

MISSION: Connect
POSSIBLE Collaborate
Innovate

Interactive
Sponsors

CISCO.

Deloitte.

# What percentage of your state IT workforce is eligible for retirement in the <u>next year</u>? (State Government Only)

**17%** A. 10%

**33%** B. 20%

**17%** C. 30%

**8%** D. 40%

**25%** E. More than 40%

*View from the State CIOs*

**Driving the Enterprise Imperative**

**Balancing Legacy and Innovation**

# State CIO Priorities for 2014

1. Security

2. Consolidation/ Optimization

3. Cloud Services

4. Project & Portfolio Management

5. Strategic IT Planning

6. Budget and Cost Control

7. Mobile Services/ Mobility

8. Shared Services

9. Nationwide Public Safety Broadband Network

10. Health Care

# IT and Solution Priorities 2014

1. **Cloud computing:** software as a service, infrastructure, platform, storage
2. **Security** enhancement tools
3. **Mobile** workforce : technologies, solutions
4. **Enterprise Resource Planning** (ERP)
5. **Virtualization:** servers, desktop, storage, applications, data center
6. **Legacy** application modernization/renovation
7. **Business Intelligence** (BI) and Business Analytics (BA)
8. **Disaster Recovery/Business Continuity**
9. **Identity** and access management
10. **Networking:** voice and data communications, unified

CIOs seeking enterprise approaches and solutions - governance

Cybersecurity requires governance and investment

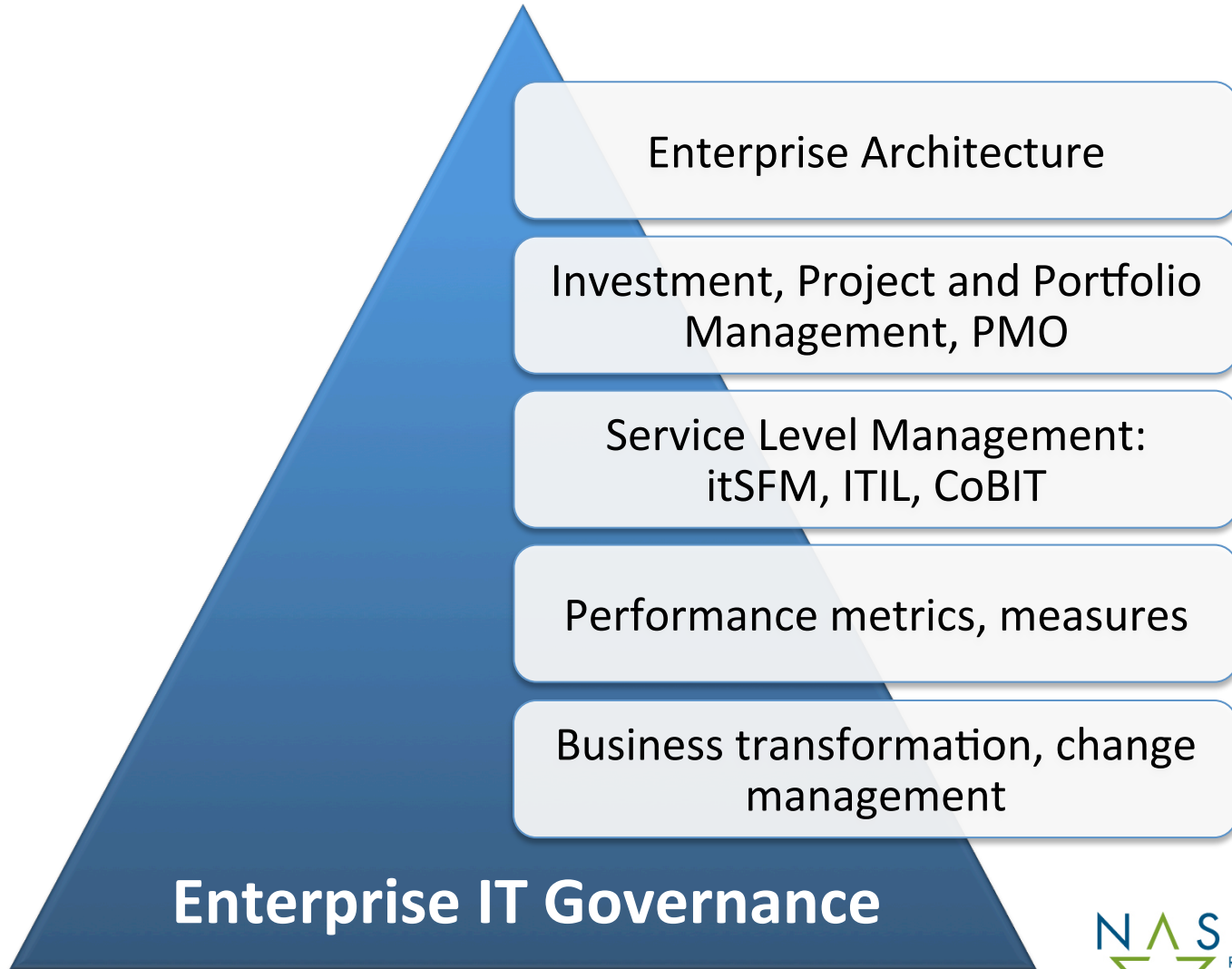Outsourcing and the use of shared services models increasing

Consolidation and cloud services growing

Dissatisfied with IT procurement

# Growing Maturity: IT Governance, Frameworks and Business Disciplines

# IT Project and Portfolio Management

**Do you use a formal IT enterprise portfolio management process to support decisions regarding planned initiatives, projects, or ongoing IT services such as application support?**

| | | | | 0% | |
|---|---|---|---|---|---|
| 63% | | 28% | | 2% | 7% |

- ■ Yes
- ■ No
- ■ Do not know
- ■ Does not apply
- ■ Other

**How effective are your state's practices for oversight of large IT projects?**

0%

| 4% | 52% | 31% | 13% |
|---|---|---|---|

- ■ No formal project oversight practices
- ■ Not at all effective
- ■ Somewhat effective
- ■ Effective
- ■ Very effective

NASCIO
Representing Chief Information
Officers of the States

# Growing IT Security Risks in the States

| | | |
|---|---|---|
| Protecting legacy systems | Malicious software | Inadequate policy compliance |
| Mobile devices and services | Use of social media platforms | Use of personally-owned devices (BYOD) for state business |
| Adoption of cloud services; rogue cloud users | Foreign state-sponsored espionage | Third-party contractors and managed services |

Source: Deloitte-NASCIO Cybersecurity Study, October 2012

# Cybersecurity

Please characterize the current status of the cybersecurity program and environment in state government.

| | Percent |
|---|---|
| Adopted a cybersecurity framework based on national standards and guidelines | 78% |
| Acquired and implemented continuous vulnerability monitoring capabilities | 78% |
| Developed security awareness training for workers and contractors | 78% |
| Established trusted partnerships for information sharing and response | 75% |
| Created a culture of information security in your state government | 73% |
| Adopted a cybersecurity strategic plan | 61% |
| Documented the effectiveness of your cybersecurity program with metrics and testing | 47% |
| Developed a cybersecurity disruption response plan | 45% |
| Other | 6% |

States are adopting a cybersecurity framework and implementing monitoring capabilities.

# Cybersecurity

What major barriers does your state face in addressing cybersecurity?

| | Percent |
|---|---|
| Increasing sophistication of threats | 83% |
| Lack of adequate funding | 77% |
| Inadequate availability of security professionals | 55% |
| Emerging technologies | 42% |
| Lack of visibility and influence within the enterprise | 25% |
| Lack of support from business stakeholders | 21% |
| Inadequate competence of security professionals | 19% |
| Lack of clarity on mandate, roles and responsibilities | 13% |
| Lack of legislative support | 12% |
| Other | 10% |
| Lack of executive support | 6% |

NASCIO
Representing Chief Information
Officers of the States

# Act and Adjust:  A Call to Action for Governors for Cybersecurity

National Governors Association, September 26, 2013

- Establish a governance and authority structure for cybersecurity
- Conduct risk assessments and allocate resources accordingly
- Implement continuous vulnerability assessments and threat mitigation practices
- Ensure that the state complies with current security methodologies and business disciplines in cybersecurity
- Create a culture of risk awareness.

# IT Consolidation: A Key Strategy for Years

*To address budget issues and control operational costs*

**Facilities:** reducing data centers, equipment, operational costs

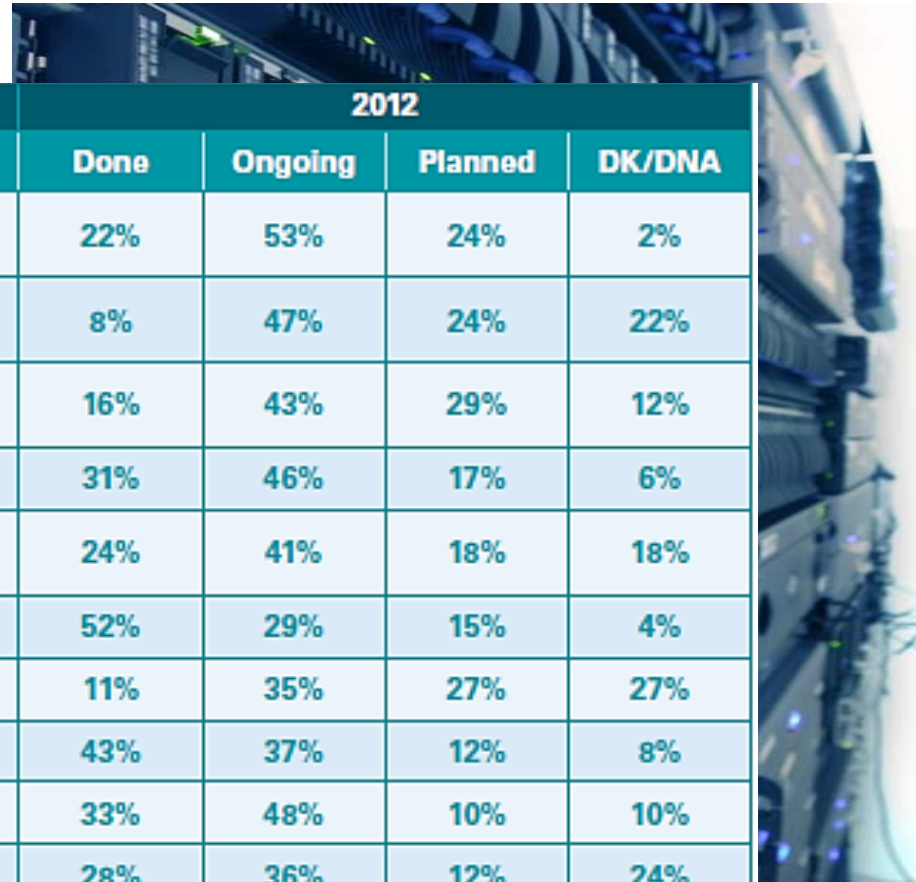**Enterprise services:** networks, email, telecommunications, imaging, wireless

**Server consolidation:** reducing footprint, operations, security impact, backup/recovery

**Applications:** enterprise, similar business functions

**IT personnel and staffing**

# What is the Status of IT Consolidation?

| Item being consolidated | 2013 | | | | 2012 | | | |
|---|---|---|---|---|---|---|---|---|
| | Done | Ongoing | Planned | DK/DNA | Done | Ongoing | Planned | DK/DNA |
| Backup/disaster recovery | 28% | 59% | 14% | 4% | 22% | 53% | 24% | 2% |
| Business applications | 19% | 48% | 19% | 21% | 8% | 47% | 24% | 22% |
| Content management | 15% | 45% | 26% | 17% | 16% | 43% | 29% | 12% |
| Data centers | 31% | 60% | 17% | 2% | 31% | 46% | 17% | 6% |
| Desktop support | 29% | 31% | 25% | 20% | 24% | 41% | 18% | 18% |
| Email | 53% | 37% | 10% | 6% | 52% | 29% | 15% | 4% |
| Imaging | 6% | 40% | 21% | 35% | 11% | 35% | 27% | 27% |
| Security | 32% | 50% | 20% | 6% | 43% | 37% | 12% | 8% |
| Servers | 30% | 63% | 16% | 4% | 33% | 48% | 10% | 10% |
| Staff | 38% | 30% | 23% | 15% | 28% | 36% | 12% | 24% |
| Storage | 30% | 54% | 18% | 4% | 27% | 57% | 8% | 8% |
| Telecom | 56% | 39% | 12% | 4% | 62% | 28% | 8% | 2% |

*Source: NASCIO-TechAmerica –Grant Thornton LLP 2013 State CIO Survey*

NASCIO
Representing Chief Information
Officers of the States

- Project has been cancelled

- Planning stage

- Project is ongoing

- Project is done
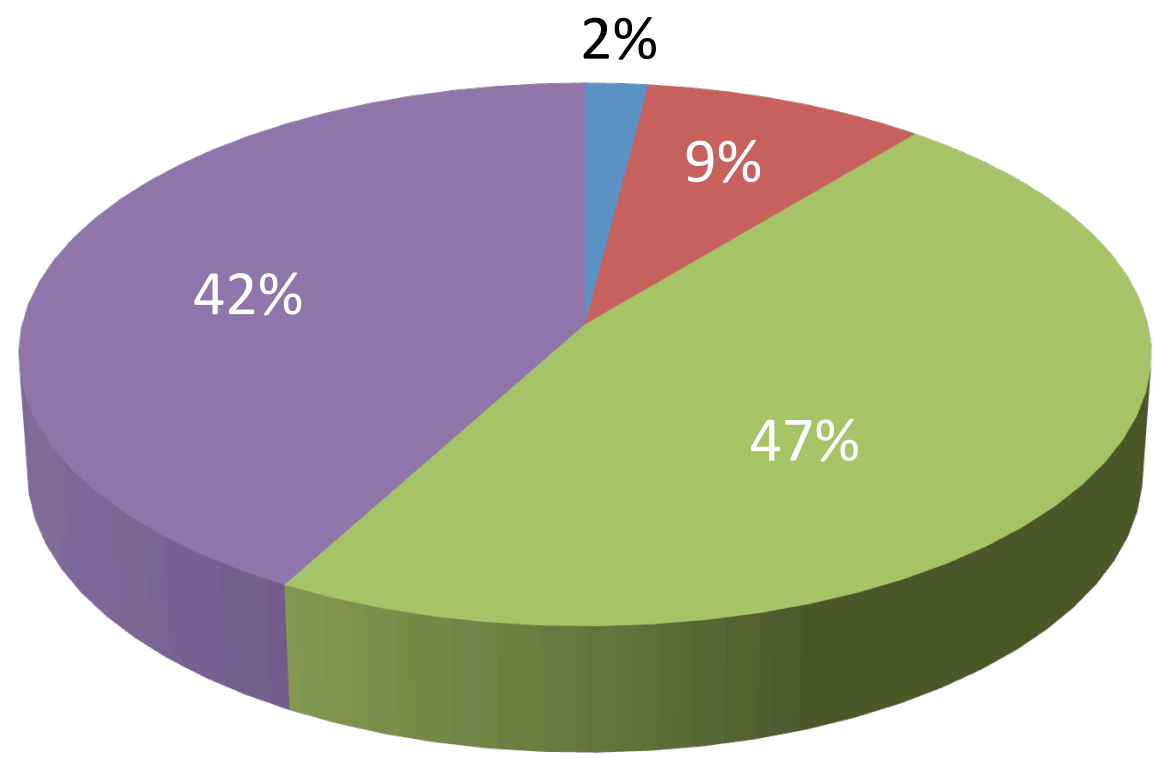
**Enterprise email consolidation a top priority**

# States Moving Toward Technology as a Service

- Cost savings and efficiency
- Flexibility and scalability
- Rapid provisioning
- Better data security



## Cloud services as an option

- Move from systems-centric to services-centric
- Shift spend from O&M to new services
- Support collaboration, transparency, insight

# Cloud Services

| What is your state's status regarding cloud services? | | |
|---|---|---|
| | **2013** | 2012 |
| The state is already highly invested in cloud services | 6% | 15% |
| The state has some applications in the cloud and is considering others | 68% | 56% |
| The state is still investigating cloud services | 22% | 19% |
| The state has considered cloud services but has rejected it | 2% | 0 |
| Other | 2% | 10% |
| Don't know/does not apply | 0% | 0 |

| What categories of services have you migrated or do you plan to migrate to the Cloud? (select all that apply) | |
|---|---|
| E-mail and collaboration | 64% |
| Storage | 48% |
| Geographic Information Systems | 48% |
| Disaster recovery | 44% |
| Program/business applications (e.g., licensing, unemployment insurance, workers' comp, etc.) | 42% |
| Office productivity software (e.g., word processing) | 37% |
| Digital archives/electronic records | 31% |
| Citizen relationship management | 25% |
| Open Data | 25% |
| Enterprise Resource Planning | 23% |
| Imaging | 15% |
| Other | 15% |

# Cloud Services

| How has your state procured third-party cloud services? | | |
|---|---|---|
| | 2012 | **2013** |
| Used an existing procurement vehicle not specifically designed for cloud services | 65% | 65% |
| Created a specific procurement vehicle for cloud services | 44% | 47% |
| Leveraged cloud services procurement vehicles created by multijurisdictional consortia | 15% | 31% |
| Leveraged cloud services procurement vehicles created by the federal government | 6% | 16% |

Because of state procurement challenges, expect continued growth in multistate and cooperative purchasing options in 2014.

NASCIO
Representing Chief Information
Officers of the States

Mobility

**Within the state CIO's strategic agenda and IT operational plans, how would you characterize mobile devices and applications?**

- 29%
- 58%
- 8%
- 2%
- 4%

■ Essential   ■ High Priority   ■ Low Priority   ■ Not a Priority   ■ Don't Know
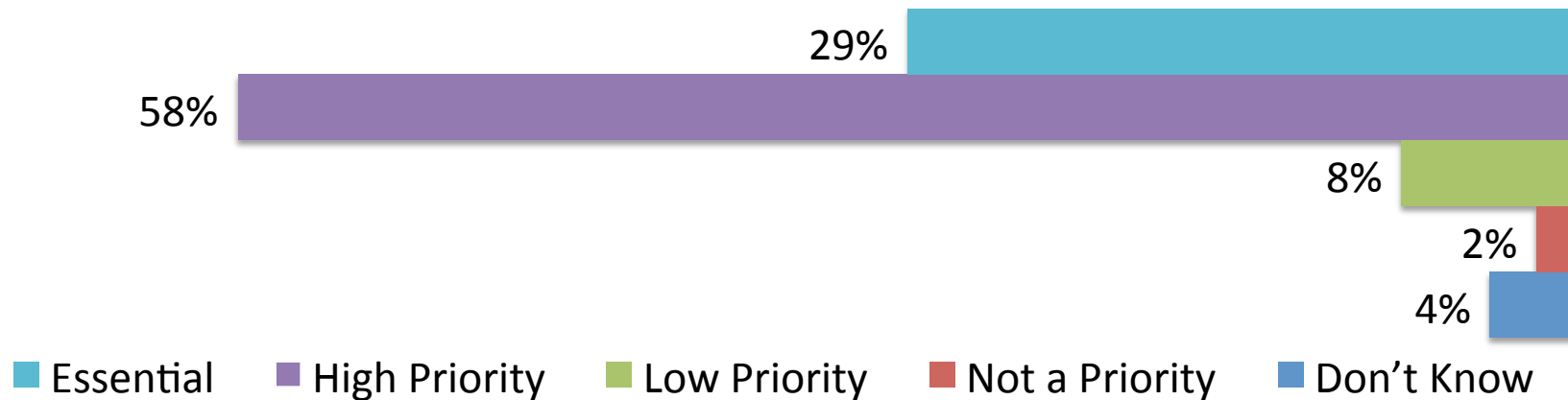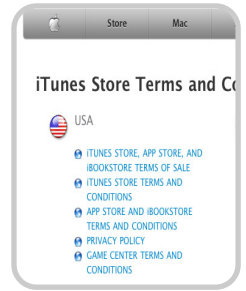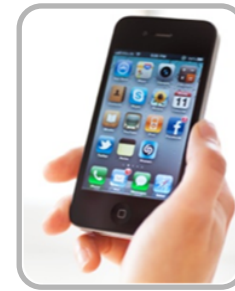
| Direction strategic or ad hoc?  Policy? | Managing mobile devices?  MDM?  BYOD? | Security and privacy | Managing business and end-users | Lack of technical expertise: apps,  security | Native apps, web or both? | Legal Issues? Terms of Service from apps stores? |

# Considerations: Productivity, Data Sharing, Citizen Services, Mobile Apps, BYOD

## How is your state managing mobility?

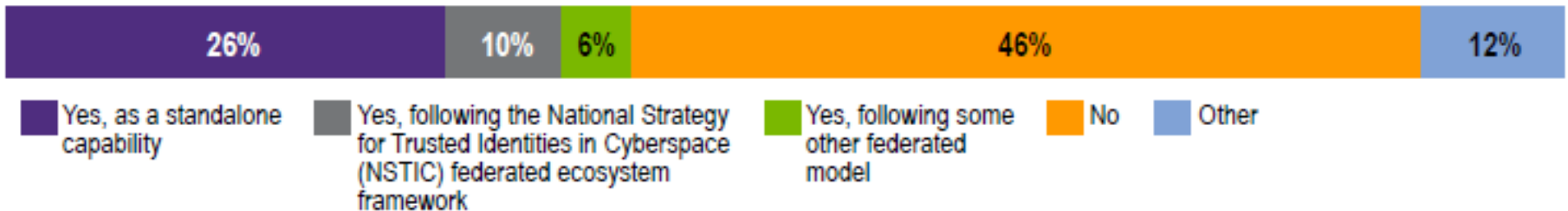| | 2012 | 2013 |
|---|---|---|
| Totally fragmented and uncoordinated | 12% | 10% |
| A few coordinated government-wide projects and initiatives, but mostly fragmented efforts | 46% | 49% |
| Mostly coordinated government-wide projects and initiatives, a few fragmented efforts | 32% | 37% |
| All mobility projects well-coordinated government-wide | 6% | 0% |
| Don't know/does not apply | 4% | 4% |

# Identity and Access Management (IAM)

Which best describes the status of your state's current approach to identity and access management?

|  | Percent |
|---|---|
| Enterprise model fully implemented in the executive branch | 8% |
| Enterprise model under way - partial implementation | 42% |
| Still investigating an enterprise model | 21% |
| No plans for enterprise IAM implementation | 2% |
| Decentralized IAM at agency level | 17% |
| No IAM initiatives at all | 6% |
| Other | 4% |

# Identity and Access Management (IAM)

Has your state attempted to extend its IAM solution to identify and authenticate constituents seeking to access state services?

| 26% | 10% | 6% | 46% | 12% |
|-----|-----|-----|-----|-----|

- Yes, as a standalone capability
- Yes, following the National Strategy for Trusted Identities in Cyberspace (NSTIC) federated ecosystem framework
- Yes, following some other federated model
- No
- Other

CIOs say that the most significant barriers to adoption of an enterprise IAM strategy are:

- decentralized environment of the state
- cost
- complexity of legacy systems
- lack of governance

# State CIOs Recognize Why Identity Management Needs to be a Top Priority

Support for a national framework that provides interoperability and trust across multiple jurisdictions.
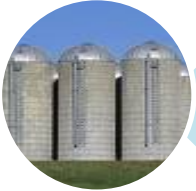
Promotes state enterprise approach: avoids silos, avoids proprietary solutions.  Adoption of the standards will reduce redundant credentialing efforts and expenditures.

Follows the great work the states have led in improving drivers license issuance. 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

# SICAM: A Framework for State Action

**Goals and Objectives**

- Trust
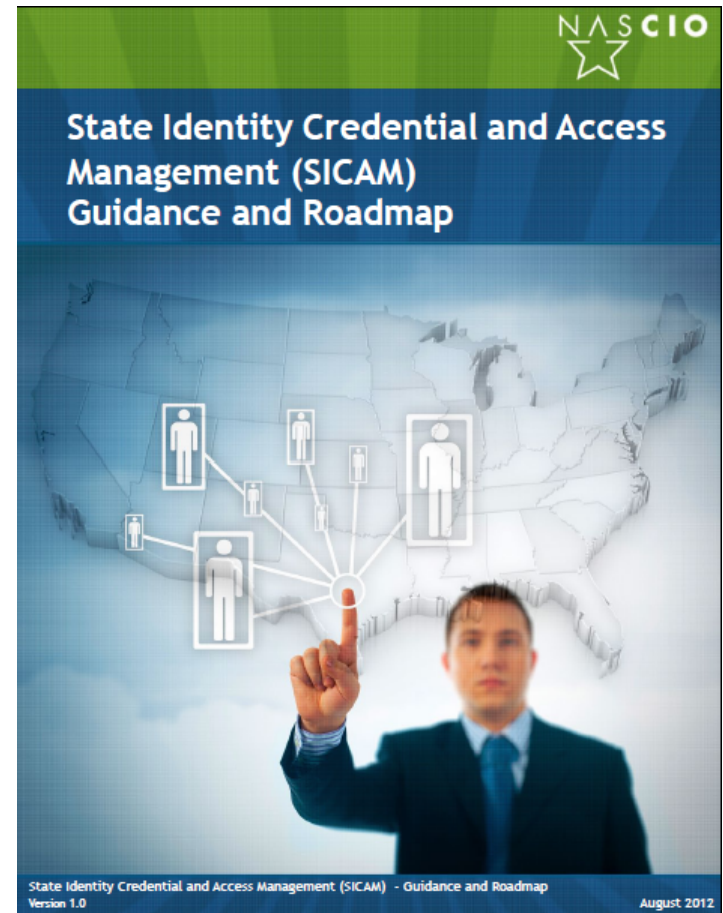- Interoperability
- Security
- Process Improvements

**SICAM Model for Assurance Levels**

**Principles, Processes, and Concepts**

**Architecture Framework**

**Implementation Strategy**

- Risk Assessment
- Assurance Levels
- Identity Proofing Requirements
- Attribute Management
- Governance
- Architecture Compliance

State Identity Credential and Access Management (SICAM) Guidance and Roadmap

State Identity Credential and Access Management (SICAM) - Guidance and Roadmap
Version 1.0

August 2012

# Do I Smell State Trends?

**2014 and Beyond...**

Digital identity ecosystem; NSTIC TrustMarks

Growing state IAM adoption; SICAM version 2; FirstNet IAM

NIEF QuickStart Project; NSTIC pilots in states

More social, mobile, analytics; PIV-I

More IT consolidation, optimization, shared services, cloud services

NASCIO
Representing Chief Information Officers of the States