Harmonizing Federal Cyber Regulations & Normalizing the Audit Process

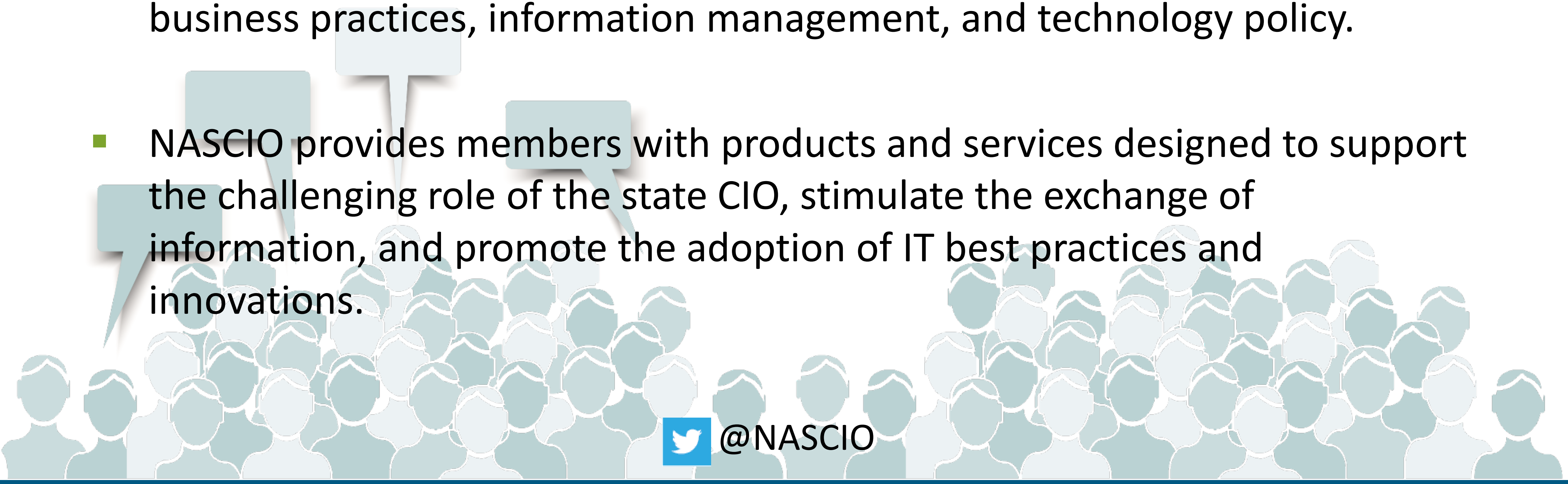
Yejin Cooke, NASCIO Director of Government Affairs

About NASCIO

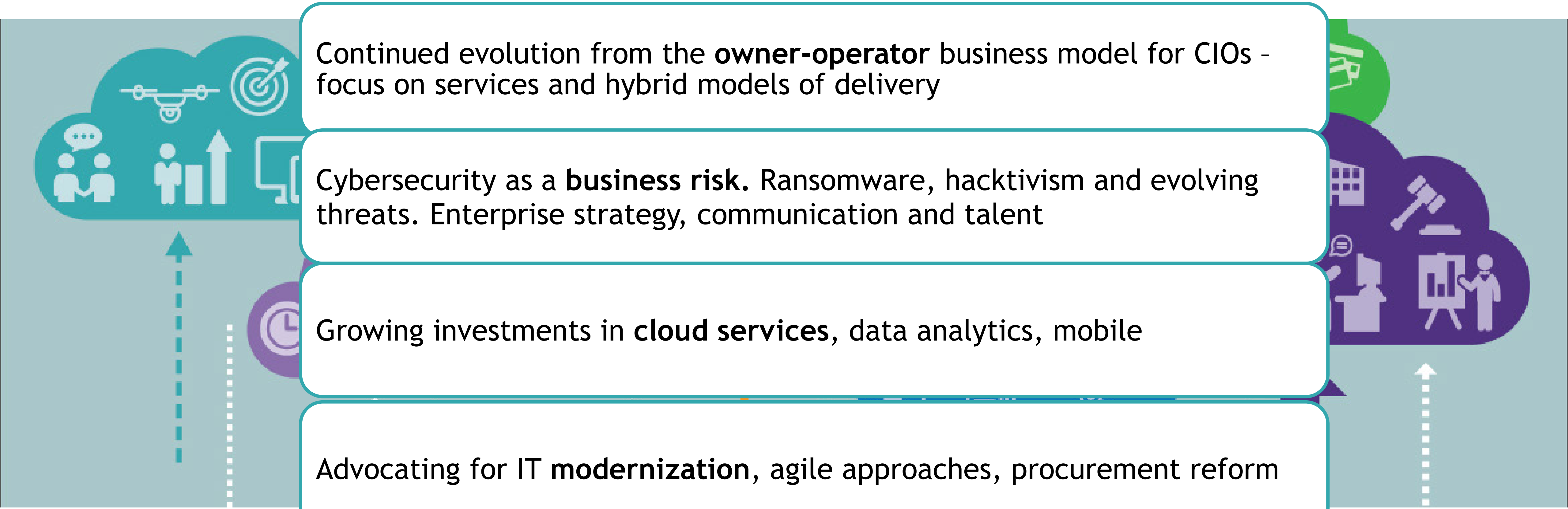
- National association representing state chief information officers and information technology executives from the states, territories and D.C.

- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.

- NASCIO provides members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations.



@NASCIO



2017 budget cuts in many states. Budgets for FY 2018 remain cautious – 1% growth. CIOs pressured to find **cost savings,** driving consolidation, optimization strategies.

Continued evolution from the **owner-operator** business model for CIOs – focus on services and hybrid models of delivery

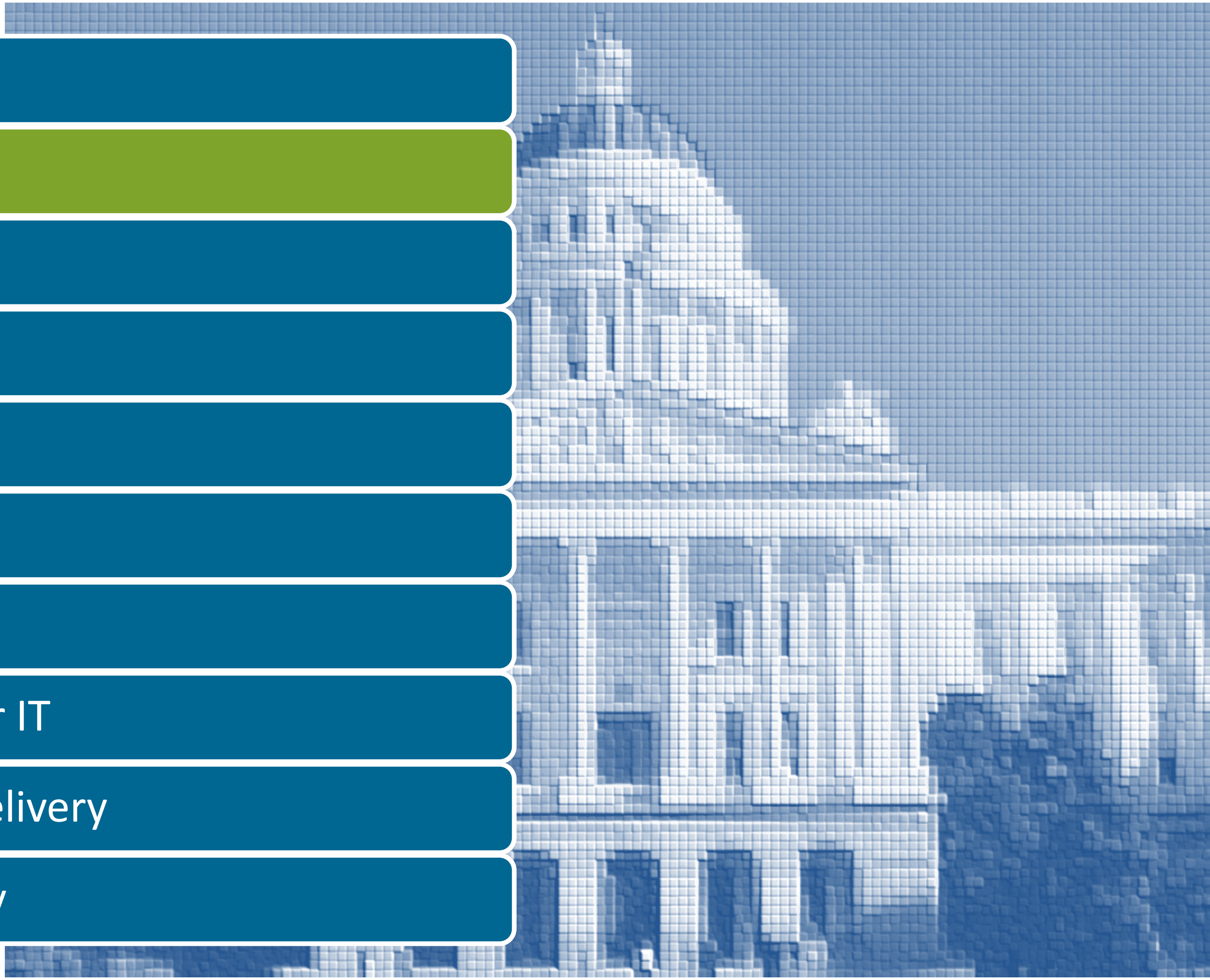
Cybersecurity as a **business risk.** Ransomware, hacktivism and evolving threats. Enterprise strategy, communication and talent

Growing investments in **cloud services**, data analytics, mobile

Advocating for IT **modernization**, agile approaches, procurement reform

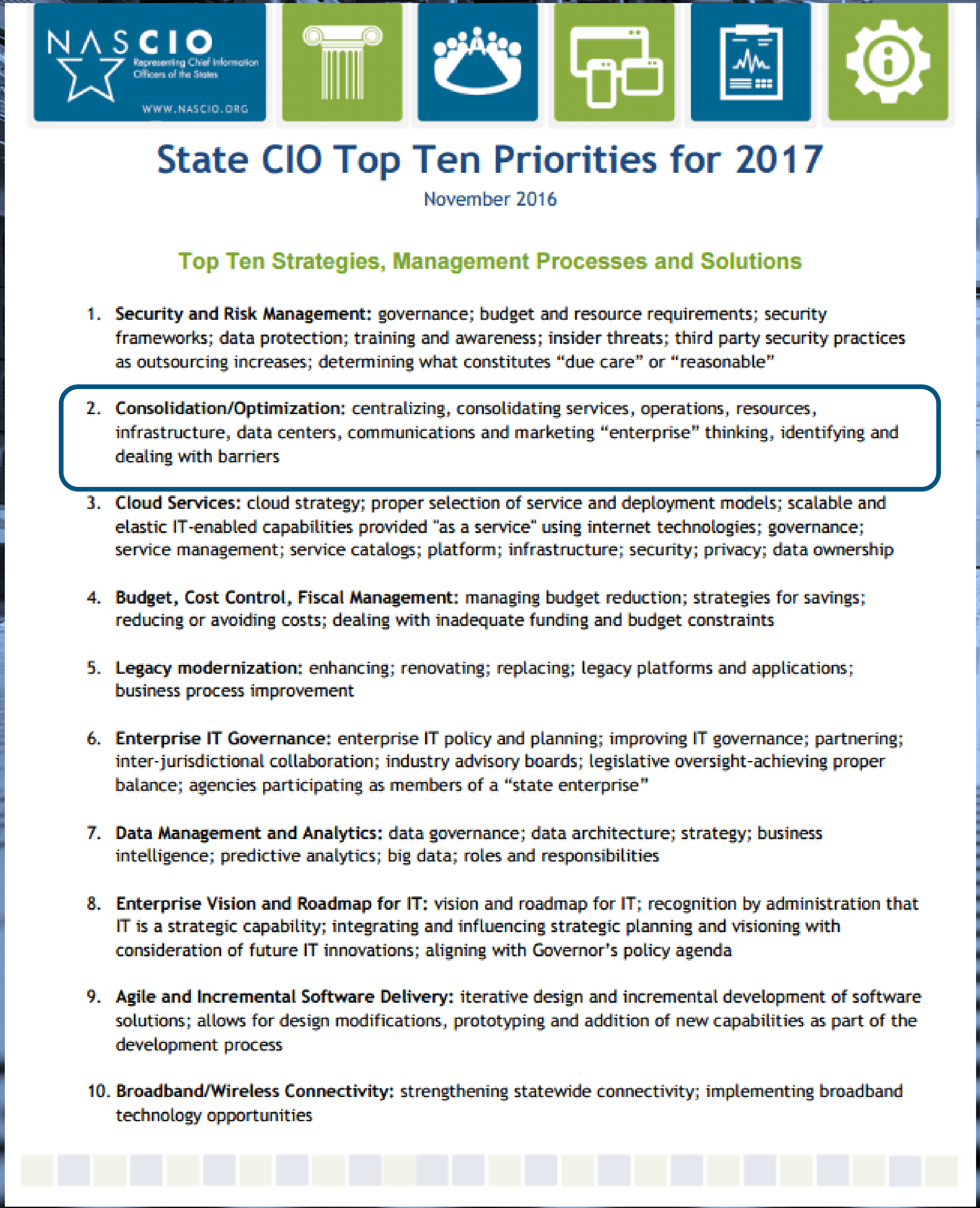
Continuing IT **workforce challenges:** retirements, skills gap, recruiting, talent management, workplace innovation

Top Ten: State CIO Priorities for 2017



1. Security
2. Consolidation/Optimization
3. Cloud Services
4. Budget and Cost Control
5. Legacy Modernization
6. Enterprise IT Governance
7. Data Management and Analytics
8. Enterprise Vision and Roadmap for IT
9. Agile and Incremental Software Delivery
10. Broadband/Wireless Connectivity

Source: NASCIO State CIO ranking, November 2016



NASCIO Representing Chief Information Officers of the States WWW.NASCIO.ORG

State CIO Top Ten Priorities for 2017

November 2016

Top Ten Strategies, Management Processes and Solutions

1. **Security and Risk Management:** 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"
2. **Consolidation/Optimization:** centralizing, consolidating services, operations, resources, infrastructure, data centers, communications and marketing "enterprise" thinking, identifying and dealing with barriers
3. **Cloud Services:** cloud strategy; proper selection of service and deployment models; scalable and elastic IT-enabled capabilities provided "as a service" using internet technologies; governance; service management; service catalogs; platform; infrastructure; security; privacy; data ownership
4. **Budget, Cost Control, Fiscal Management:** managing budget reduction; strategies for savings; reducing or avoiding costs; dealing with inadequate funding and budget constraints
5. **Legacy modernization:** enhancing; renovating; replacing; legacy platforms and applications; business process improvement
6. **Enterprise IT Governance:** enterprise IT policy and planning; improving IT governance; partnering; inter-jurisdictional collaboration; industry advisory boards; legislative oversight-achieving proper balance; agencies participating as members of a "state enterprise"
7. **Data Management and Analytics:** data governance; data architecture; strategy; business intelligence; predictive analytics; big data; roles and responsibilities
8. **Enterprise Vision and Roadmap for IT:** vision and roadmap for IT; recognition by administration that IT is a strategic capability; integrating and influencing strategic planning and visioning with consideration of future IT innovations; aligning with Governor's policy agenda
9. **Agile and Incremental Software Delivery:** iterative design and incremental development of software solutions; allows for design modifications, prototyping and addition of new capabilities as part of the development process
10. **Broadband/Wireless Connectivity:** strengthening statewide connectivity; implementing broadband technology opportunities

Consolidation has been on the State CIO Top Ten Priorities list consistently since 2006

Rationale for IT Consolidation

- Reduce diversity and complexity of environment – cost savings
- Economies of scale – reduce operational costs
- Strengthen IT security
- Promote enterprise integration and applications
- Introduce process standards: ITIL and ITSM
- Improved support for legacy systems
- Centralize infrastructure maintenance and upgrades
- Improve disaster recovery/business continuity
- Reinvestment of spend to services

Targets of Enterprise Consolidation

- Data Centers
- E-mail/Collaboration
- Telecom/Networks
- Servers
- Storage
- Desktops
- Content Management
- Security
- Help Desk
- Software Licenses

- Disaster Recovery/Back Up
- Automation Tools
- Application Development
- Business Intelligence/Analytics
- Project Management
- Imaging/Archiving
- Mobile Device Management
- Identity Management
- Contracts
- IT Staff

Challenges to Consolidation Initiatives

- Agency/workforce resistance to change
- Lack of funding/investment to prepare for consolidation
- Agencies desire to remain autonomous
- Problems moving infrastructure from the agencies
- Backlash when consolidation doesn’t meet agency business needs
- Higher than projected costs
- Seeking exemptions from federal statutory and regulatory requirements

State of Oklahoma Story: Consolidation & Savings

Consolidated 68 of 78 mandated agencies & 50 voluntary agencies

Before: 1,000 employees with 400 titles

Now: 750 staff assigned with 13 job families, 10 services team, 100 titles

$283 million: reduced spending and projected savings

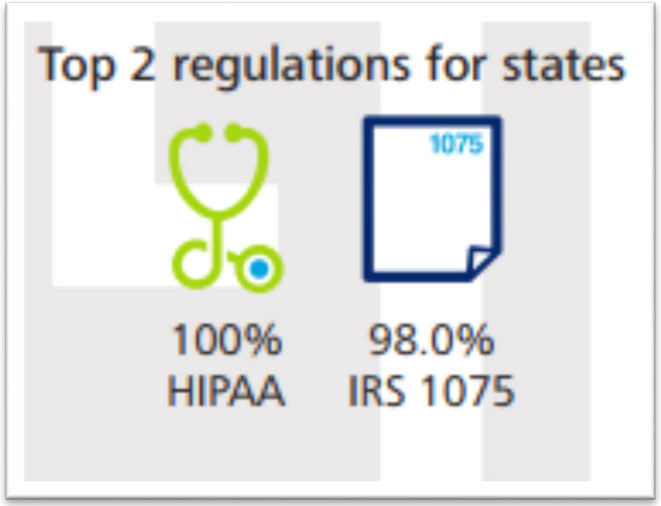
Partners: Okla. and Texas agree to share preferred technology provider list

Project Savings		FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
Total Annual Savings		$4,403,597	$10,528,325	$23,454,338	$23,794,798	$24,596,066	$36,010,600
Savings Over 6 years[1]	$107,988,240						

Project Cost Avoidance		FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
Total Annual Savings		$1,867,961	$4,829,530	$4,444,620	$618,928	$618,928	$618,928
Savings Over 6 years[1]	$12,209,040						

Purchasing Cost Avoidance		FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
Total Annual IT Contract Savings		$18,746,985	$26,463,196	$35,146,666	$36,736,079	$45,762,620	In Progress
Savings Over 5 years[1]	$162,855,546						

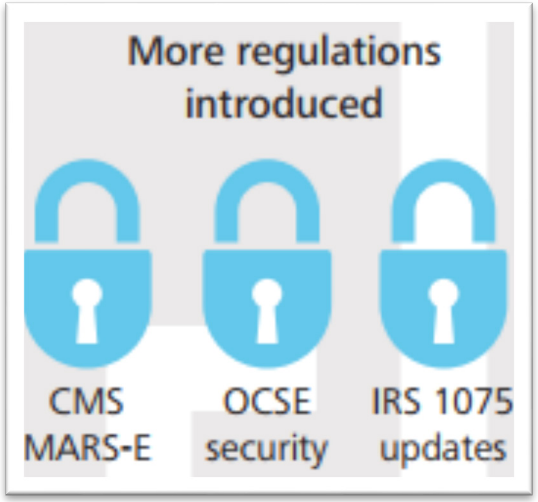
Federal Compliance Requirements



Top 2 regulations for states

100% HIPAA

98.0% IRS 1075

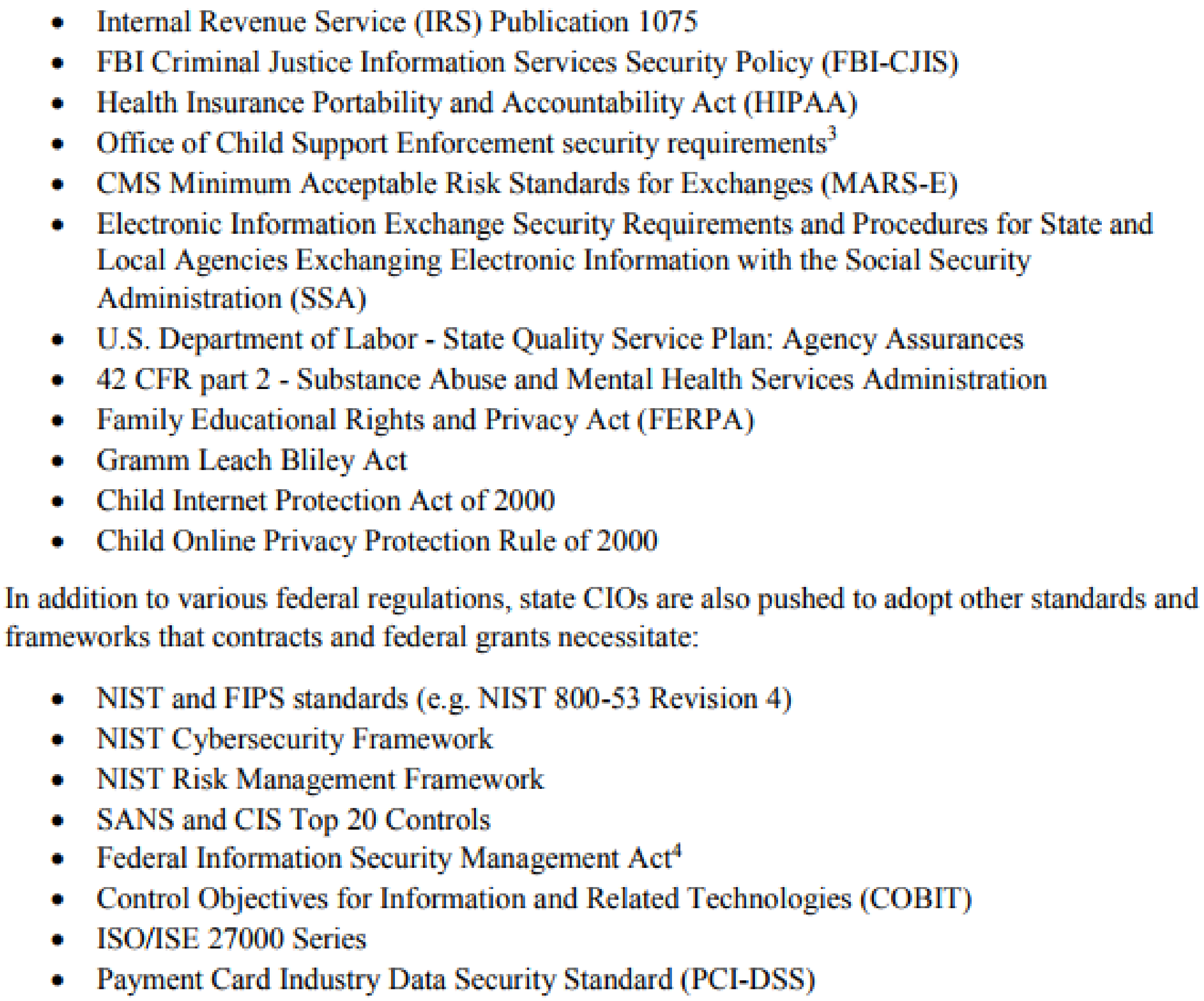


More regulations introduced

CMS MARS-E

OCSE security

IRS 1075 updates



- Internal Revenue Service (IRS) Publication 1075
- FBI Criminal Justice Information Services Security Policy (FBI-CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Office of Child Support Enforcement security requirements[3]
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA)
- U.S. Department of Labor - State Quality Service Plan: Agency Assurances
- 42 CFR part 2 - Substance Abuse and Mental Health Services Administration
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act
- Child Internet Protection Act of 2000
- Child Online Privacy Protection Rule of 2000

In addition to various federal regulations, state CIOs are also pushed to adopt other standards and frameworks that contracts and federal grants necessitate:

- NIST and FIPS standards (e.g. NIST 800-53 Revision 4)
- NIST Cybersecurity Framework
- NIST Risk Management Framework
- SANS and CIS Top 20 Controls
- Federal Information Security Management Act[4]
- Control Objectives for Information and Related Technologies (COBIT)
- ISO/ISE 27000 Series
- Payment Card Industry Data Security Standard (PCI-DSS)

Examples of Inconsistency

IRS 1075	FBI-CJIS
Unsuccessful logins (9.3.1.7) Information system must enforce a limit of 3 consecutive invalid login attempts by a user during a 120 min period, and automatically lock account for at least 15 mins.	**Unsuccessful Logins** (5.5.3) Where technically feasible, system shall enforce limit of no more than 5 consecutive invalid attempts, otherwise locking system for 10 mins
Password Requirements a. Enforce minimum password complexity of: 1. Eight characters 2. At least one numeric and at least one special character 3. A mixture of at least one uppercase and at least one lowercase letter 4. Storing and transmitting only encrypted representations of passwords b. Enforce password minimum lifetime restriction of one day c. Enforce non-privileged account passwords to be changed at least every 90 days d. Enforce privileged account passwords to be changed at least every 60 days e. Prohibit password reuse for 24 generations f. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password g. Password-protect system initialization (boot) settings	**Password requirements (5.6.2.1.1)** Passwords shall: 1. Be a minimum length of eight (8) characters on all systems. 2. Not be a dictionary word or proper name. 3. Not be the same as the Userid. 4. Expire within a maximum of 90 calendar days. 5. Not be identical to the previous ten (10) passwords. 6. Not be transmitted in the clear outside the secure location. 7. Not be displayed when entered

Examples of Inconsistency

IRS 1075	FBI-CJIS
Security Training Records (9.3.2.4) The agency must: a. Document and monitor individual information system security training activities, including basic security awareness training and specific information system security training b. Retain individual training records for a period of **five years** **Updates for Security Training and Awareness (9.3.2.1)** 1. Security awareness and training policy **every three years** (or if there is a significant change) 2. Security awareness and training procedures **at least annually** **Security Awareness Training Requirements (9.3.2.2) -** The agency must: a. Provide basic security awareness training to information system users (including managers, senior executives, and contractors): 1. As part of initial training for new users; 2. When required by information system changes; 3. At least annually thereafter b. Include security awareness training on recognizing and reporting potential indicators of **insider threat**. **Additional Role-Based Training for Security Personnel (9.3.2.3)** The agency must provide role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties that require access to FTI b. When required by information system changes c. At least annually thereafter	**5.2.1.2 Level One (those with physical access)** - General responsibilities, implications of noncompliance, incident response, visitor security challenges **5.2.1.2 Level Two (those with logical access) -** Media protection, protecting confidential information, proper handling and marking of CJI, threats/vulns/risks to CJI, social engineering, dissemination and destruction **5.2.1.3 Level Three (those with physical and logical access) -** 1. Rules that describe responsibilities and expected behavior with regard to information system usage. 2. Password usage and management—including creation, frequency of changes, and protection. 3. Protection from viruses, worms, Trojan horses, and other malicious code. 4. Unknown e-mail/attachments. 5. Web usage—allowed versus prohibited; monitoring of user activity. 6. Spam. 7. Physical Security—increases in risks to systems and data. 8. Handheld device security issues—address both physical and wireless security issues. 9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance. 10. Laptop security—address both physical and information security issues. 11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights). 12. Access control issues—address least privilege and separation of duties. 13. Individual accountability—explain what this means in the agency. 14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain. 15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems. 16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. 17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services. **5.2.1.4 Level Four (IT personnel only) -** 1. Protection from viruses, worms, Trojan horses, and other malicious code--scanning, etc. 2. Data backup and storage--centralized or decentralized approach 3. Timely application of system patches--part of configuration management 4. Access control measures 5. Network infrastructure protection measures

Examples of Inconsistency

IRS 1075	FBI-CJIS
Audit Logs Agency must determine that they can, at a minimum audit the following: 1. Log onto system 2. Log off of system 3. Change of password 4. All system administrator commands, while logged on as system administrator 5. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS) 6. Creation or modification of super-user groups 7. Subset of security administrator commands, while logged on in the security administrator role 8. Subset of system administrator commands, while logged on in the user role 9. Clearing of the audit log file 10. Startup and shutdown of audit functions 11. Use of identification and authentication mechanisms (e.g., user ID and password) 12. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su) 13. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system 14. Changes made to an application or database by a batch file 15. Application-critical record changes 16. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility) 17. All system and data interactions concerning FTI 18. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website	**Audit Logs** Required Events to Log (5.4.1.1) 1. Successful and unsuccessful system log-on attempts. 2. Successful and unsuccessful attempts to use access/create/write/delete/change permission on a user account, file, directory, or other system resource 3. Successful and unsuccessful attempts to change account passwords. 4. Successful and unsuccessful actions by privileged accounts. 5. Successful and unsuccessful attempts for users to access/modify/destroy the audit log file.

Challenges Presented by Federal Regs & Audits

The IRS has onerous requirements that do not **contemplate cost and lack a policy justification**. The IRS decided that if someone is using a VoIP phone, any phone call containing a discussion of FTI must be recorded and kept for seven years. The storage requirements, alone for this, are huge.

- Arkansas

We encounter multiple IRS audits that ask the **same questions across five separate agencies**. There is also a lack of consistency on certain controls such as encryption rules, password rests, and now background checks. The continuous cycle of auditors focusing on different regulations creates an extreme burden on the states. Since each auditing unit requires testing by auditors, **weeks if not months of personnel hours are wasted** simply repeating the same tasks for each audit event.

- Illinois

We have 3 agencies that receive Social Security Administration (SSA) data and 4 that receive IRS data. This is for the most part all the same data, but is distributed under 7 unique need and use agreements. As such, **we have 7 agency level audits for each need and use agreement and 1 additional specific to IT as the state transmission center (STC) for a total of 8 audits for common data**, all operating under the same controls and infrastructure.

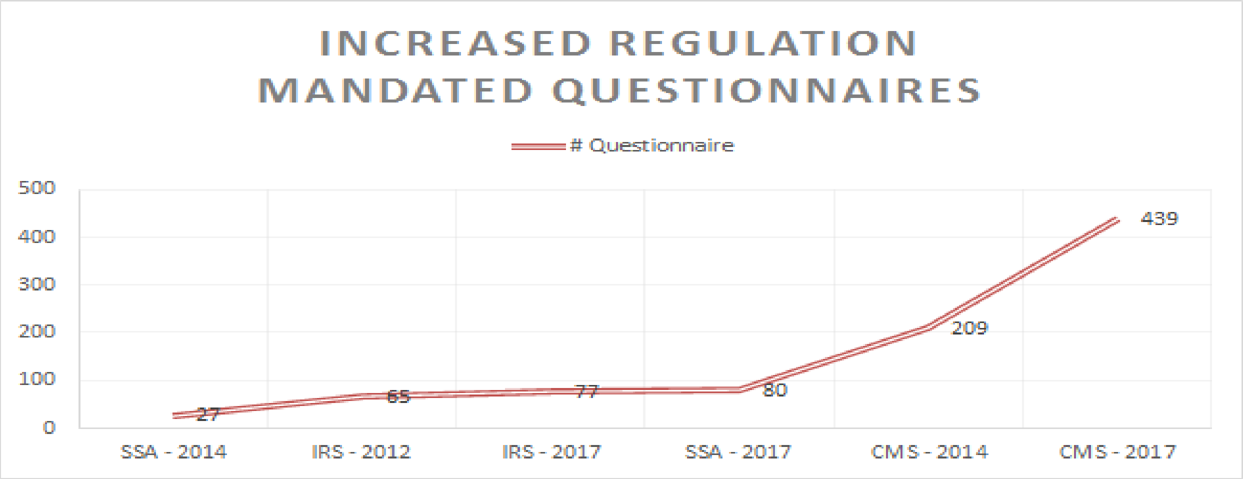
- Kentucky

Challenges Presented by Federal Regs & Audits

5 state agencies were assessed by five separate IRS assessors **all auditing the same exact statewide Information Security Policy** with the following breaking down of findings.
- Louisiana

Findings	
Agency #1	32
Agency #2	27
Agency #3	23
Agency #4	14
Agency #5	11

#	Regulatory Agency	State Resources	Total Hours
1	Internal Revenue Service (IRS)	12+	4,000
2	Social Security Administration (SSA)	4+	2,500
3	U.S. Treasury	1	60
4	Health Portability and Accountability Act (HIPAA)	6+	800
5	Criminal Justice Information Service (CJIS)	3+	800
6	Centers for Medicare and Medicaid Services (CMS)	12+	3,000
Total			11,160



Impact to State Cyber

- Investments based on compliance and not risk
- Inefficient use of state information security workforce

“We have to spend **scarce funding on services to map all federal regulations** and requirements together to make them somewhat manageable. We spend valuable human capital and scarce funding to process multiple audits for the same federal regulation such as IRS Publication 1075. This creates **complications in drafting and managing local security policy with zero flexibility**. The **federal approach is not based on risk management but rather “checkbox security” which forces the state to expend funds on low risk issues** instead of a high-risk issue to maintain compliance.

I use human capital (i.e. Full Time Equivalents FTE) and scarce funding to manage multiple frameworks. If federal agencies were on the same page, those resources could be used more effectively to improve the state’s security posture.”

- West Virginia

Thank You!

Contact:
Yejin Cooke
Director of Govt Affairs

202.624.8477
ycooke@NASCIO.org
www.nascio.org