NASCIO
Representing Chief Information
Officers of the States

September 9, 2016
Submitted electronically via cybercommission@nist.gov

Mr. Kevin Stine
National Institute of Standards and Technology
100 Bureau drive
Gaithersburg, MD 20899

Dear Mr. Stine,

On behalf of the National Association of State Chief Information Officers (NASCIO), thank you for the opportunity to comment on "Information on Current and Future States of Cybersecurity in the Digital Economy" and provide recommendations to the Commission on Enhancing National Cybersecurity (hereinafter, Commission). NASCIO makes several recommendations for the Commission's consideration, including:

- Establish a federal working group to harmonize disparate federal security regulations
- Encourage state government development of a cyber disruption response plan and adoption of advanced cyber analytics capabilities
- Continue and expand successful workforce programs like CyberCorps: Scholarship for Service
- Reduce redundant investment in common IT technologies by recognizing benefits of exceptions to OMB's cost allocation principles

NASCIO represents the state chief information officers (CIO) and information technology executives and managers from the states, territories and D.C. State CIOs are leaders of state information technology policy and implementation and continually look for opportunities to improve the operations, bring innovation and transform state government through technological solutions. Naturally, cybersecurity has been a top priority for state CIOs for the past several years (See, NASCIO Top Ten Policy and Technology Priorities Survey, 2013-2016).

State governments are responsible for securing public networks, the state's digital assets, and citizen data. Within state government, state CIOs bear the responsibility for the aforementioned tasks and understand that cybersecurity is a shared responsibility. State CIOs work closely with federal, state, and local government partners and the private sector to ensure that the common goal of cybersecurity is achieved.

Since 2010 and every two years thereafter, NASCIO and Deloitte have partnered to survey state chief information security officers (CISO) to better understand the cybersecurity landscape within state government. In every iteration of the NASCIO-Deloitte study, insufficient budgets, the increasing sophistication of threats, and recruiting and retaining cybersecurity talent were cited as top barriers to cybersecurity. However, findings from the soon-to-be-released 2016 NASCIO-Deloitte Cybersecurity Study show that significant progress has been made:

- **Cyber risks now have Governor-level attention; elevated on the Governor's agenda**
    - Cybersecurity communication to the Governor has increased and is more frequent
    - Cybersecurity is becoming a key topic and more frequent in state executive leadership meetings
    - Continuing challenge of "confidence-gap" between state officials and CISOs in protecting the state's assets; officials continue to believe that states are in much better shape.
- **Cybersecurity has been weaved into the fabric of government operations/sustainability**
    - Role of the CISO has become more clearly delineated and states are seeing new roles emerge to protect citizen data
    - Functions included in the role are those areas CISOs can control
- **Most states indicate an increase in budget. However, funding remains the biggest challenge**
    - More than 50 percent of the respondents reported cybersecurity being just 0-2 percent of the overall IT budget
    - States with an approved strategy are more likely to obtain additional funding from the technology and business stakeholders
- **Finding talent is still a challenge but states are trying to win their hearts and minds**
    - Finding talent is the second biggest challenge
    - CISOs continue to use staff augmentation and outsourcing to bridge the talent gap

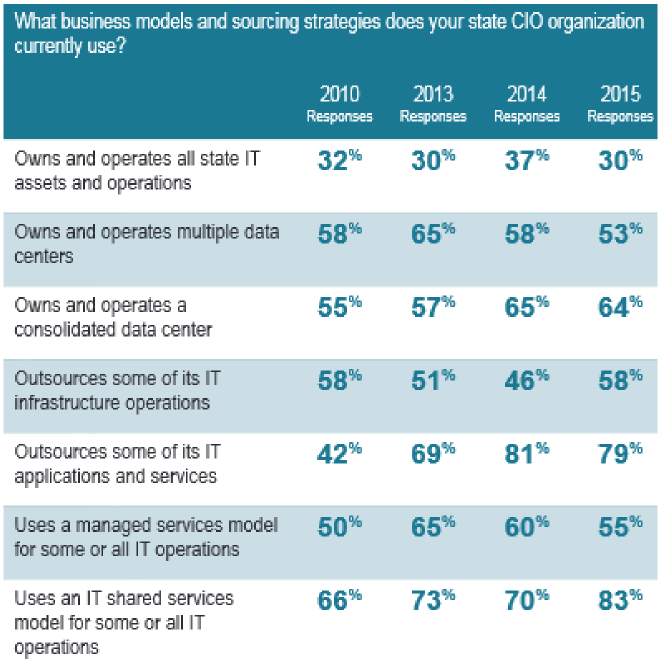
Federal Governance

The cybersecurity posture within state governments continues to improve but, much work remains. One issue that is particularly relevant for the Commission to address is inconsistent federal security regulations. The increasing number of and the lack of consistency among security regulations promulgated by federal government agencies pose an unnecessary burden on state governments.

Many federal regulations map to NIST guidance like the NIST Special Publication 800-53 and the NIST Cybersecurity Framework. Both documents are structured similarly and are organized by functional categories. While both documents recommend implementation of access controls under the "protect" function, federal agencies interpret this control differently and impose varying interpretations of the NIST specified requirement.

Consider this example: the FBI's Criminal Justice Information System (CJIS) Security Policy (v 5.5) requires a session lock (Section 5.5.5 Session Lock) after 30 minutes of inactivity, IRS Publication 1075 requires a session lock after 15 minutes of inactivity (9.3.1.9 Session Lock) and HIPAA does not specifically address session lock (See, Administrative Safeguards 45 CFR 164.308(a)(4)(ii)(B) "Access authorization: Implement policies and procedures for granting access to electronic protected health information, for example, though access to a workstation, transaction, program, process, or other mechanism"). To the casual observer, these details may seem insignificant but they have considerable implications for state CIOs who provide IT services to all state executive branch agencies.

State CIOs are bound by the same security requirements as their state agency customers. The list of federal security regulations with which state CIOs must comply include: Federal Information Security Management Act, Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), IRS Publication 1075, FBI Criminal Justice Information Services (CJIS) Security Policy, Office of Child Support Enforcement (OCSE) security requirements, among others. Complicating matters, business models are changing and state governments are moving away from the traditional owner/operator model and moving towards a broker of services model. This presents new opportunities for savings but again, varying interpretations of security controls embedded in federal regulations pose an unnecessary burden to state governments that are adapting to new business models.



What business models and sourcing strategies does your state CIO organization currently use?

	2010 Responses	2013 Responses	2014 Responses	2015 Responses
Owns and operates all state IT assets and operations	32%	30%	37%	30%
Owns and operates multiple data centers	58%	65%	58%	53%
Owns and operates a consolidated data center	55%	57%	65%	64%
Outsources some of its IT infrastructure operations	58%	51%	46%	58%
Outsources some of its IT applications and services	42%	69%	81%	79%
Uses a managed services model for some or all IT operations	50%	65%	60%	55%
Uses an IT shared services model for some or all IT operations	66%	73%	70%	83%

Source: NASCIO 2015 State CIO Survey

NASCIO recommends establishing a federal working group composed of representatives from federal agencies and state government to harmonize disparate federal agency interpretations of common security controls.

Critical Infrastructure Cybersecurity

State CIOs understand the need to work collaboratively with their federal, state, and local partners including private sector partners in the critical infrastructure space. In April 2016, NASCIO published the "Cyber Disruption Response Planning Guide" to help states build resiliency and prepare for large magnitude events caused by a cyber event. NASCIO recommends state governments take these steps to begin cyber disruption response planning:

- **Organization and Governance**: determining roles and responsibilities and decision rights and rules
- **Mitigation and Risk Assessment:** the intention is to identify what is at risk and the probability and magnitude of such risks. Mitigation strategies are designed based on identified risks. Mitigation is response focused on the thing being defended. Mitigation efforts are intended to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of the effects of a cyber disruption event. Mitigation measures may be implemented prior to, during, or after an event.
- **Communication:** communications includes internal communication for properly orchestrating resources, communicating known or anticipated threats, external communication to regional partners and status updates to citizens and the press.

- **Response:** Formulating a specific response based on the type of disruption, its magnitude and severity in order to prevent disruption if possible, to recover and restore operations.
- **Training:** Training strategy must provide the appropriate training for the various roles of the cyber disruption response as well as every employee.

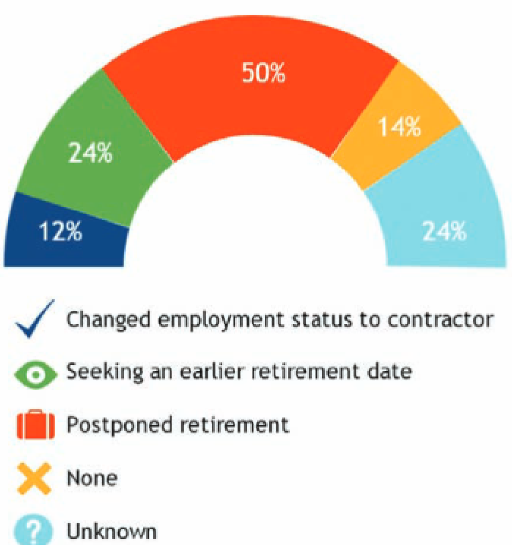
In addition to developing a cyber disruption response plan, state governments can enhance their cybersecurity posture by investing in advanced cyber analytics capabilities. With the increasing sophistication of cyber threats, NASCIO has called on states to develop and maintain response capabilities that keep pace with an ever changing threat landscape; one such method is by investing in cyber threat analytics. In "Advanced Cyber Analytics: Risk Intelligence for State Government," NASCIO highlights the benefits of cyber analytics:

- Detecting malicious activity earlier
- Stopping and reducing the impact of cyber attacks
- Preventing data loss and malicious data modification
- Protecting data assets, physical assets, workforce and citizens
- Assisting in the identification of the attackers
- Assisting in forensic investigations in the event an attacker gets though security defense
- Assisting in the prosecution of attackers
- Identifying a data breach sooner
- Detecting previously unknown attacks, new malicious behavior and insider threats through behavioral analytics
- Providing evidence based approaches through data driven results
- Increasing ability to analyze all cyber-centric data and identify statistically relevant data elements[1]

[1] NASCIO, Advanced Cyber Analytics: Risk Intelligence for State Government, April 2016.

States need to continue to build resiliency through planning and periodically update established cyber disruption guides to ensure that plans continue to be viable. The federal government has been a great partner to states by offering assistance through various cyber programs like US-CERT. Additionally, the U.S. Department of Homeland Security (DHS) has assisted state governments keep pace with advanced cyber threats by partnering with private sector security companies and making cyber intelligence products available, currently at no cost, to state governments.[2] Recognizing the intergovernmental partnerships are critical to secure state governments and the nation, **NASCIO recommends that the federal government work in partnership with states to encourage development of cyber disruption guidance and adoption of advanced cyber analytics capabilities to enhance state government resilience.**

In the past few years, some state workers have begun to rethink their retirement strategy. What change, if any, have your retirement-eligible IT employees made regarding their retirement?



Source: NASCIO State IT Workforce: Facing Reality with Innovation

Cybersecurity Workforce

Recruiting and retaining security professionals continues to be a challenge for state governments. NASCIO's 2015 study, "State IT Workforce: Facing Reality with Innovation,"[3] describes the state IT workforce environment where the majority of states are having difficulty recruiting new employees to fill vacant positions.[4] State salary rates and pay grade structures present the biggest challenge to attracting and retaining IT talent (91.8 percent).[5] 46 percent of states report that it is taking 3-5 moths to fill senior level IT positions.[6]

State governments are responding to the workforce challenge by implementing innovative strategies. In Washington, state CIO Michael Cockrill has "experimented with self-management, piloted physical work space changes, reclassified state government technology positions, and started hiring for value alignment instead of skills" to meet workforce demands.[7] State governments are also utilizing federal

[2] http://www.nlc.org/Documents/Influence%20Federal%20Policy/Policy%20Committees/ITC/DHS_iSIGHT%20FAQs.pdf

[3] http://www.nascio.org/Portals/0/Publications/Documents/NASCIO_StateITWorkforceSurvey2015_WEB.pdf

[4] NASCIO, State IT Workforce: Facing Reality with Innovation, April 2015 available at: http://www.nascio.org/Portals/0/Publications/Documents/NASCIO_StateITWorkforceSurvey2015_WEB.pdf.

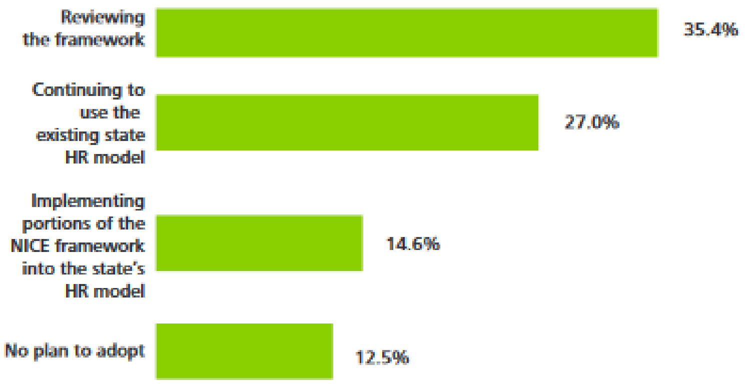
[5] Id.

[6] Id.

[7] http://www.nascio.org/Portals/0/Documents/CIOs2016/NASCIO%20-%20Fact%20Sheet%20-%20Washington.pdf

resources like NIST's National Initiative for Cybersecurity Education (NICE) Framework which provides a common language for that "categorizes and describes cybersecurity work."[8] Additionally, state governments are tapping federal programs like CyberCorps: Scholarship for Service where participants receive stipends for higher education in exchange for cybersecurity related work performed on behalf of a state, local, tribal, or federal government entity.[9]

Figure 20: States' adoption of NICE framework



Source: 2014 NASCIO-Deloitte Cybersecurity Study

NASCIO recommends continuation and expansion of successful federal workforce programs like CyberCorps: Scholarship for Service to assist state governments respond to the dearth of security professionals in state government IT.

Identity and Access Management (IAM)

Identity and access management (IAM) has appeared on the NASCIO top ten list for priority technologies, applications, and tools four times in the past five years.[10] State CIOs aspire to implement enterprise wide IAM solutions understanding that trusted digital identities and their authentication enables state government's digital ecosystem. In fact, several states are participating in NIST pilot studies on the issue.[11] Government participants like the Commonwealth of Pennsylvania and the Ohio Department of Administrative Services, are currently exploring methods for identity proofing and multi-factor authentication, respectively.

State CIOs understand the value of IAM within the state government enterprise and its value to state citizens. State citizens come to expect of government what they already experience in the private sector and IAM is key to offering that convenience. States like Michigan have made the citizen's online experience more convenient and user friendly by bringing access to state resources and services to a single app, MiPage.[12] The success of MiPage is due in part to the foundational IAM work put into place by Michigan's Department of Technology, Management, and Budget and the Department of Health and Human Services. The MiLogin initiative, an enterprise-wise identity, credential, and access management solution provides user account and access management, desktop and mobile single sign-on, password

[8] http://csrc.nist.gov/nice/framework/

[9] U.S. Office of Personnel Management (OPM), CyberCorps: Scholarship for Service, Frequently Asked Questions available at: https://www.sfs.opm.gov/StudFAQ.aspx?#num8

[10] NASCIO, Top Ten Priorities 2016, 2014, 2013, and 2012.

[11] https://www.nist.gov/itl/nstic/pilot-projects#summaries

[12] http://www.nascio.org/portals/0/awards/nominations2014/2014/2014MI11-2014%20NASCIO%20MI%20State%20CIO%20Recognition%20Nomination.pdf

management, and multifactor authentication services for state staff, citizens, third party/business partners, other states and local units of government.[13]

The federal government has and can continue to be a partner to states working to optimize IT components that benefit the administration of federal programs and also contribute to the operation of others. In 2011, the Centers for Medicare and Medicaid Services increased the level of federal support for eligibility and enrollment system modernization from 50 percent to 90 percent for new system builds and from 50 percent to 75 percent for maintenance and operations. Additionally, the Office of Management and Budget (OMB) offered a waiver of Circular A-87's[14] cost allocation rules which allowed human service programs other than Medicaid to share common IT components at little or no additional cost.[15] Identity management qualified as a business component under the A-87 exception which allowed multiple programs to share its use without being required to allocate costs based on proportional use; this was required prior to the A-87 exception.[16] **The Commission should consider cost allocation principles like the A-87 exception as a method by which the federal government can encourage states to adopt technology solutions that can enhance the security posture across lines of business.**

Cybersecurity Insurance

State CIOs operate and manage state IT with the understanding that cybersecurity is a business risk and some have chosen to manage that risk by purchasing cybersecurity insurance. State governments are increasingly obtaining cybersecurity insurance and NASCIO research indicates that twelve (12) states have a cybersecurity insurance policy as of August 2016. Those that have not obtained a cybersecurity insurance policy will likely cite cost, the abundance of uninsurable risks, and sufficiency of existing property or casualty insurance[17] as key reasons for being without a policy.

The cybersecurity insurance landscape in 2015 was fairly immature and was characterized by little actuarial data, lack of standard policies, lack of understanding for the federated state government model, and carriers were reluctant to cover services hosted in a cloud environment.[18] Despite the nascent nature of the cyber insurance market, many state CIOs have decreased the risk profile for state governments by working with carriers and adopting policies that work for their IT environment. States that have activated their policies, realized benefits like: customer notification, crisis communications, credit monitoring, forensic investigation, and data restoration.[19]

[13] http://www.isaca.org/chapters2/Western-Michigan/events/Documents/SOM-MiLogin.pdf

[14] On December 26, 2013 OMB issued the Super Circular "Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards" which replaces A-87 and other cost principle circulars.

[15] American Public Human Services Association (APHSA), A-87 Exception Toolkit for Human Service Agencies: Description of the Exception and Recommendations for Action, January 2014.

[16] Id.

[17] Ponemon Institute, Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, August 2013.

[18] NASCIO, 2015 Midyear Presentation available at http://www.nascio.org/dnn/portals/17/2015MY/Cybersecurity%20Insurance.pdf.

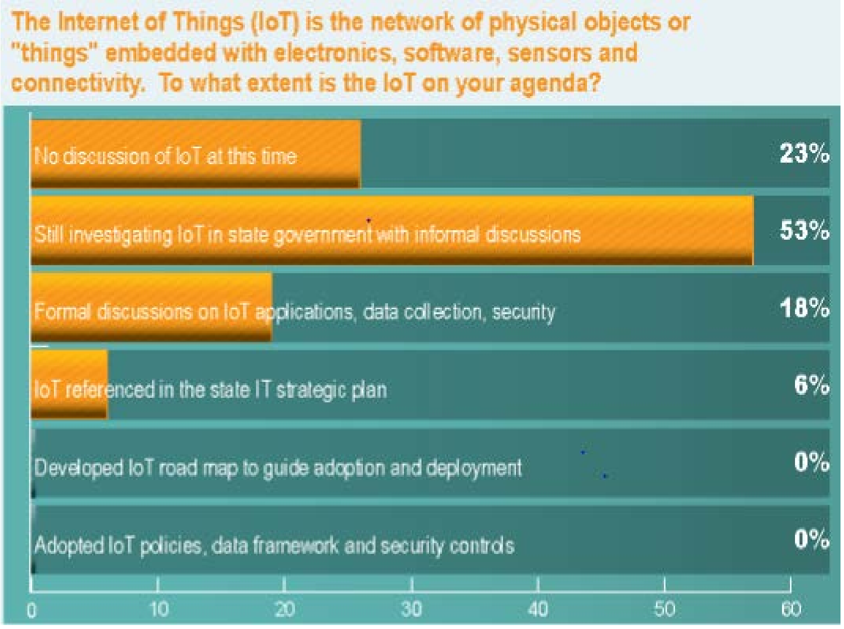
[19] Id.

Montana was an early adopter of cybersecurity insurance and activated their policy in May 2014 when they first discovered an incident within their networks. After initial discovery, Montana worked with their insurance carrier for forensic confirmation and public communication and began mailing notices by early July. Crisis communication and public relations professionals helped the state of Montana craft a message to inform and assure the public and press about the cyber incident.[20]

Internet of Things (IoT)

In 2015, the majority of state CIOs were still investigating IoT in state government with information discussions or were not discussing the topic at all.[21] Local governments have taken the lead on IoT implementation for government and states, too, are utilizing the technology in areas of transportation, health care, and public safety as noted in NASCIO's June 2016 publication, "Value and Vulnerability: The Internet of Things in a Connected State Government."

For states considering adoption of IoT, NASCIO recommends careful consideration of security, privacy, and data management policies.[22]



Conclusion

NASCIO looks forward to working with the Commission and our federal partners to enhance the security posture of state governments and the nation. For question or more information on anything in this comment, please contact NASCIO director of government affairs Yejin Cooke at ycooke@NASCIO.org or 202.624.8477.

Doug Robinson

Darryl Ackley
NASCIO President &
Secretary of Information Technology, State of New Mexico

Doug Robinson
Executive Director, NASCIO

[20] Id.

[21] NASCIO, 2015 State CIO Survey: The Value Equation, October 2015.

[22] NASCIO, Value and Vulnerabilities: The Internet of Things in a Connected State Government, June 2016.