

# STRONGER TOGETHER

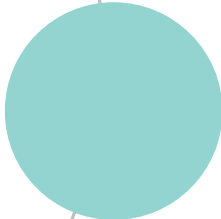
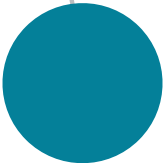
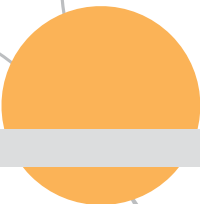
## State and Local Cybersecurity Collaboration



**NASCIO**<sup>®</sup>  
Representing Chief Information  
Officers of the States

---

**NGA**  
NATIONAL GOVERNORS ASSOCIATION



# STRONGER TOGETHER:

## State and Local Cybersecurity Collaboration

### Executive Summary

With a dramatic uptick in ransomware attacks across the country, governors, state chief information officers (CIOs) and state government executives are designing and implementing programs to strengthen local partnerships in cybersecurity. State governments are increasingly providing services to county and municipal governments, including endpoint protection, shared service agreements for cyber defensive tools, incident response and statewide cybersecurity awareness and training. This publication outlines promising programs that states have initiated to enhance collaboration with their local government counterparts for cyber resilience. It also provides high-level recommendations for state officials looking to strengthen partnerships with local government officials on cybersecurity. At a minimum, increased engagement can provide a more accurate threat picture to enhance state and local governments' cyber posture. However, there is a need to move beyond information sharing to leverage limited resources for enhanced cyber capabilities.

### Introduction

The majority of all publicized ransomware attacks in the United States have targeted local governments, according to 2019 estimates.<sup>1</sup> Some, like the August 2019 [Texas Cyber Incident](#), the [attack on Louisiana public schools](#) and the [Baltimore cyber disruption](#), have been well publicized. However, one can assume that many other incidents are publicly unknown. Additionally, in the 2018 Deloitte-NASCIO Cybersecurity Study, more than 70 percent of state chief information security officers (CISOs) identified ransomware as a very high or somewhat higher threat than other cyber threats. Ransomware is just one example demonstrating the need for broader engagement between states and locals.

Some states have little to no engagement with their local counterparts, especially where 100 percent of state resources are exclusively directed toward state agencies. Other states do provide a limited amount of services or have advanced engagement with local agencies. In the [2019 State CIO Survey](#), 65 percent of states reported providing security infrastructure and services to local governments. But, as the old adage goes, if you've seen one state, then ... you've seen one state; the scope of services provided varies widely. How are state CIOs, homeland security advisors (HSAs) and other state offices doing this? All states have a business relationship with local governments who are agents of state services (much like states are for the federal government). Still, some have jurisdiction or an executive directive and some because they feel it is the right thing to do.

Many CISOs believe that increased engagement with locals has strengthened the state's overall cyber posture, and they have made it a top cybersecurity priority. For example, in NGA's *Workshops to Advance State Cybersecurity* in 2019, several states focused their efforts on enhancing state and local partnerships.<sup>2</sup>

So, which cyber services are states providing to their local counterparts? Anecdotally, we know that states are providing security-as-a-service programs to local governments—for example, managed security services, election security, phishing training, cyber response teams and ransomware response.

However, CIOs and CISOs are not the only state officials who need to be dedicated to enhancing local government cybersecurity. NASCIO and NGA have advocated for a whole-of-state approach to effectively enhance statewide cybersecurity for many years. Cybersecurity is not just an “IT problem” anymore. It is a critical business risk, homeland security and public safety threat, voter confidence issue and economic development opportunity. Cybersecurity requires commitment from state executives and officials to use all levers of state government to move forward. And as such, it is essential that states take a multi-disciplinary approach.

Let’s take a look at specific state examples.

### **Colorado**

Colorado created the Colorado Threat Information Sharing (CTIS) network which provides a way to be able to quickly share threat information, indicators and other pertinent information among state agencies and local governments, industry and other nongovernment entities. In October 2019, the Office of Information Technology released a [cybersecurity guide for local government](#) to assist with cyber preparedness across the state.

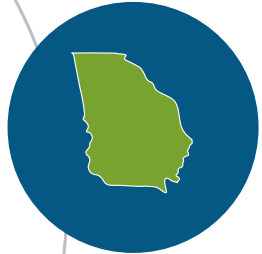
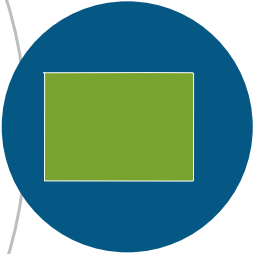
### **Georgia**

In 2018, the Georgia Cyber Center opened in Augusta with a core mission to develop the next generation cybersecurity workforce by delivering affordable and relevant cybersecurity training and education. It seeks to achieve its mission through collaboration among multiple sectors, including government, academia, law enforcement, the military, nonprofit organizations and the private sector. Through its partnership with Augusta University and Augusta Technical College, the Cyber Center is linked to certificate programs and undergraduate and graduate-level programs in cybersecurity and cyber sciences. Georgia recently announced its second year of partnership with the SANS Institute. This partnership will provide high school girls with the opportunity to develop their skills and explore careers in the cyber industry through Girls Go CyberStart.

The Cyber Center also includes the Cyber Range, which is available to students, companies and government professionals to test the stability, security and performance of cyber infrastructures and IT systems. The Georgia Bureau of Investigation’s (GBI) cybercrime unit is headquartered at the Cyber Center, which includes the GBI Cyber Crime Training Center. The Center offers classroom and laboratory training that covers a full range of cyber-related topics to assist law enforcement agencies and prepares first responders, investigators, forensic analysts and administrators with the skills necessary to address and contain cyber-related incidents.

### **Illinois**

Illinois created a “Cyber Navigator Program” in 2018 as a partnership between the Department of Innovation Technology and State Board of Elections. Using funding from the Help America Vote Act (HAVA), Illinois hired a cohort of dedicated personnel whose mission is to assist local election officials in improving their cybersecurity posture, mitigating



risks to elections infrastructure and building their resilience. The Cyber Navigators conduct risk assessments, connect local election officials to resources, and seek to demystify cybersecurity by converting jargon into business-friendly terms.

### **Indiana**

Understanding the critical role emergency management plays in responding to events, the Indiana Cybersecurity Council created a toolkit for local emergency managers in line with its statewide cybersecurity strategic plan.<sup>34</sup> Among the resources available through the toolkit are:

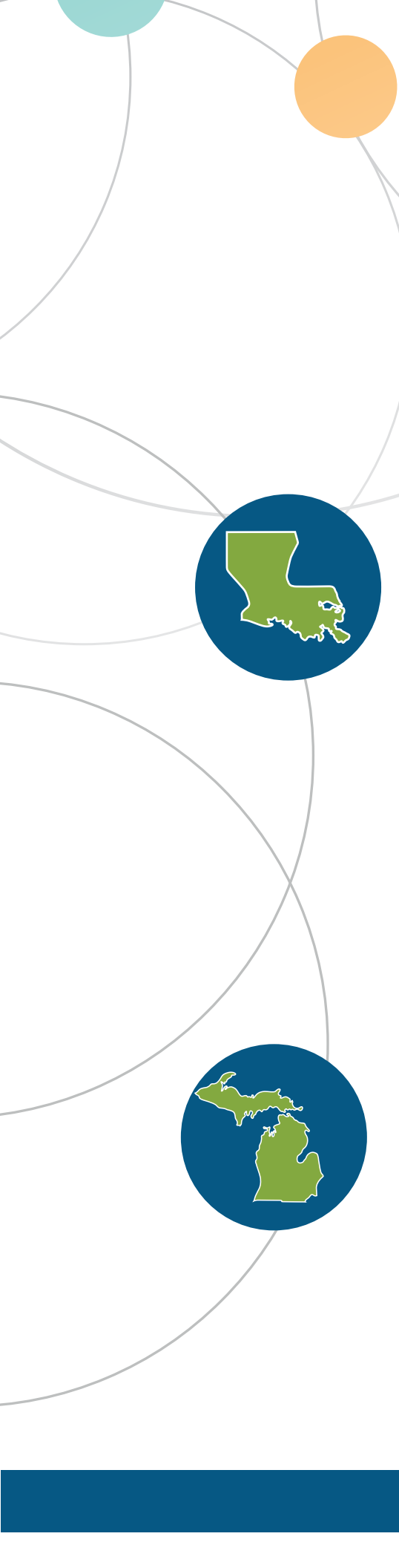
- A Cyber Situational Awareness Survey, designed to facilitate conversations between local emergency management offices and critical infrastructure on cybersecurity;
- A cybersecurity incident response template for local government entities;
- A cybersecurity training and exercise guide, to enhance emergency preparedness for cyber incidents; and
- Additional resources for local emergency managers.

### **Iowa**

In 2012, the state of Iowa began assisting counties with cybersecurity. The Office of the CIO Information Security Division was helping secure state agencies for a while but realized that resources for counties were (and are) so limited that it was helpful for counties to leverage state resources. To start expanding services to counties, the state first went to in-state conferences and workshops to discuss the importance of cybersecurity and then they marketed their services to counties and educated on state capabilities. In the beginning, 50 out of 99 counties took advantage of state cybersecurity services and that number has grown today to all 99 counties participating in at least 1 of the state's offerings.

The state was able to leverage the State Homeland Security Grant Program—from the 80 percent of grant funds designated for locals—to fund licensing, appliances/hardware and tools. One such example is vulnerability scanning to give counties an area of focus for patch management. The state also offers online security awareness training, incident response (including anti-malware tools) and an intrusion detection service which continuously monitors networks for malicious activity. Everything that is offered to counties is something the state itself uses as well.

Iowa is piloting other services to test their viability and plans to extend them to all counties who would like cybersecurity assistance. They are also piloting a few projects with local schools, cities and county hospitals with the hope of expanding those programs. The Information Security Division also partnered with the Secretary of State's Office on enhancing the cybersecurity resilience of election infrastructure. The SOS office has been instrumental in helping reach out to counties to get them involved with E-ISAC and EI-ISAC.



As far as advice for other states who may want to expand services to local governments, Iowa Cybersecurity Services Coordinator Jesse Martinez says that educating and outreach are very important and there is always room for improvement. Martinez also stresses the importance of relationship building and collaboration. If a county does not want to participate, he recommends still building a relationship with the county as a partner—in keeping with the mindset that cybersecurity is a team sport. Martinez also advises that communication alone is a win for all involved. For example, the state reports to counties when grant dollars have been used to provide hardware or services to a county. This transparency can help with securing future grant funding and/or assists counties with future budgeting should grant funding no longer be available. Finally, Martinez says some Iowa initiatives have succeeded and some have not met expectations, but it is important to always be adjusting and find what works.

### **Louisiana**



Louisiana has adopted the philosophy that assisting local government entities (LGEs) is an important aspect of their overall approach to statewide risk management. The statewide Information Security Team serves as an escalation point for Incident Response (via 1-800 hotline) for LGEs that can range from providing direction via phone call and remote assistance, to full onsite incident response. Louisiana's current focus is to find ways to engage with all the LGEs from a preparedness standpoint to improve prevention or, at a minimum, improve detection and ensure critical audit log data is being captured and maintained.

Governor John Bel Edwards established the Louisiana Cybersecurity Commission by executive order to address a range of cyber threats in the state. In 2016, the Commission began working on an Emergency Support Function for cybersecurity responses ("ESF-17") that would integrate a cyber response into the larger emergency management framework. The state activated ESF-17 through a gubernatorial emergency declaration in July 2019 to respond to a multi-targeted ransomware attack on local school districts. Local entities promptly reported the incident, which allowed the state to conduct a forensic investigation and stop the spread of attack to seven additional targeted entities.<sup>5</sup>

### **Michigan**



Michigan is looking to reboot the "CISO as a service Program," piloted in 2017 and 2018, and enhance it with partnerships, networking and organized incident response. The highly successful pilot reached 13 communities with a business plan for reaching up to 50 or more. The new model seeks statewide reach and envisions potential participation from all public-sector agencies. Supporting the CISO as a Service Program will be a statewide networking and best practice sharing group of "Cyber Partners." Partners will meet bi-monthly online and in-person to share current threats and best practices and to enhance both statewide and regional networks of public-sector cyber practitioners. Cyber incident response capabilities are provided by the Michigan State Police Cyber Command Center and a group of highly trained and organized volunteer incident responders, the Michigan Cyber Civilian Corps (MiC3).



### **New Hampshire**

New Hampshire is focusing on building relationships with local governments. New Hampshire is connected with local governments and school districts on cyber incidents to provide minimum cybersecurity standards and provide other general cybersecurity guidance. New Hampshire has conducted a series of tabletop exercises and functional exercises on cyber incident response, and the state invited local government and multiple private sectors to participate. The state also recently held a statewide cybersecurity workshop focused on local government which helped build relationships with locals, offered briefings on common cyber threats and protections, and promoted state and federal cyber incident resources (to include the New Hampshire National Guard).



### **New Jersey**

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) provides direct and indirect services to local government organizations. The services include advice and counsel—best practices, limited incident response and select remediation services—and the state is starting to provide risk assessments. New Jersey also has held a cyber symposium on how to respond and recover from cyber incidents for local and county governments that have experienced them. Finally, New Jersey offers threat intelligence products and cybersecurity training to locals, and the state recently rolled out a statewide threat grid at the county level which includes funding MS-ISAC Albert Sensors for all 21 county networks.



### **North Carolina**

North Carolina's Department of Information Technology actively engages county and municipal governments to raise awareness of the state resources and services available to help them prevent and mitigate the effects of cyberattacks at the local level.

The department has developed a partnership with the North Carolina National Guard and North Carolina Emergency Management to help local governments – as well as school systems and community colleges – remediate and recover infrastructure and data compromised during a cyberattack and to provide training that can help prevent future cybersecurity incidents. NCDIT has also deployed tools to support monitoring of county infrastructure and local network traffic.

When incidents cannot be prevented, NCDIT works together with state partners and federal law enforcement entities to respond to local cyber incidents and deploy IT strike teams, together with local resources, to help rebuild environments and detect remaining threats.

A memo of understanding allows NCDIT to activate the National Guard for cybersecurity assessments and other cyber services on state duties. The MOU allows this without requiring a declaration from the governor.

Most recently, the North Carolina General Assembly, in August 2019, passed legislation requiring county and municipal agencies to report cybersecurity incidents to NCDIT and encouraging private sector entities to do the same.



## **Pennsylvania**

The Commonwealth of Pennsylvania has made significant progress on improving its overall security posture through partnerships and cross collaboration with local government.

In 2015, the commonwealth partnered with the County Commissioners Association of Pennsylvania through a collaborative workgroup (called PA Cybersafe), a group of county CIOs and IT directors that meet quarterly and focus on security education, collaboration with the state CISO, and standardization of security approaches. In addition, an election-specific workgroup with state and county election leaders was established. The partnerships have matured over the years and continued efforts have helped to foster trust and achieve measurable results and improvements across these external organizations.

Through this partnership, Pennsylvania has been able to:

- Work collaboratively across state and local government to improve the overall cyber security posture;
- Positively affect and impact legislation and election security;
- Implement regular communications and improve information sharing and collaboration across the state via strategy sessions;
- Create a pilot with a cyber-forensic provider to help counties identify and remedy security gaps; and
- Provide statewide access to social engineering (phishing) exercise services and computer-based security awareness training via a cloud-based learning management system.

The statewide phishing services and training is a primary example of Pennsylvania's cross collaboration and partnership efforts which have produced measurable outcomes. It includes efforts with the counties on partnering on security awareness training and phishing campaigns. In 2018, to further strengthen overall election security in Pennsylvania and to further its mission to continue to mature the commonwealth's overall cyber security posture, the Pennsylvania Office of Administration partnered with the County Commissioners Association of Pennsylvania to provide security awareness training and phishing exercises for all 150,000 county and state employees and contractors through a single service.

Pennsylvania CISO Erik Avakian has said, "overall, we have found partnering and cross collaboration with local governments to be a successful recipe to improving collectively as an overall team. This initiative has bolstered election security and best practices. It also helps achieve economies of scale from overall license costs, reduces overall costs of the service for everyone, maximizes efficiencies, enhances knowledge transfer, reduces duplication of work and streamlines processes and services for those in state and local government."

## **Texas**

In 2018, Texas launched a Managed Security Services program which provides security device management, incident response services and assessment services to local and K-12 entities. The services are pre-bid and contracted for through a multi-sourcing services integrator and require an interagency agreement with the Texas Department of Information Resources (DIR). Additionally, in August 2019, DIR led the response to a coordinated ransomware attack that has impacted at least 20 local government entities across Texas.





## Wisconsin

Wisconsin provides cyber support to local, tribal and private agencies similar to what occurs during physical emergencies and natural disasters via the state's Cyber Response Teams (CRT). The CRTs strive for a safer, stronger environment for users by responding to major incidents, analyzing threats and exchanging critical cybersecurity information with trusted partners. Through a grant provided by the U.S. Department of Homeland Security, this program provides a 75 percent reimbursement to train teams specifically to support local units of government in Wisconsin. Team members are made up of cybersecurity professionals from Wisconsin's Division of Enterprise Technology, the Wisconsin Army National Guard, other state agencies, local and county government and the private sector. The Cyber Response Teams use a whole-of-community approach to provide training, experience and mutual aid to Wisconsin's governmental organizations in a cyber incident. When the CRTs are not responding to a specific incident, annual, full-scale, inter-team cyber response exercises are conducted that include public and private entities.

### Action is Needed Now

Still, challenges remain in funding and with jurisdictional disagreements, generally the most cited reasons that states are not assisting locals. In the 2019 State CIO Survey, one CIO expressed frustration saying, "we are trying to market our security services to local government. It is a slow process." So, what *should* states be doing?

- 1) At the very minimum states should be building relationships with local governments.
  - Work through state municipal leagues and county associations, with emphasis on local information technology associations.
- 2) States should raise awareness of existing services being offered to local governments (according to the 2019 State CIO Survey, only 31% of states have a formal awareness and marketing campaign to promote state offerings to local governments).
  - Hold cyber summits; and
  - Educate stakeholders.
- 3) States should be exploring cost savings that can be achieved through including local governments in service contracts.
  - Consult local governments during the contract planning process solicitation (according to the 2019 State CIO Survey, 42% of states consult with local governments prior to issuing a solicitation); and
  - Provide a conduit for discussions about pooling resources among shared risk pools at the local level.



# Security Guidelines for Local Government Access of State Systems



## Division of Enterprise Technology

### Background

Securing state information systems is critical. Wisconsin residents rely on the state, counties, and municipalities to deliver services reliably and safely. Cyber attacks are a continuous threat to the delivery of those services. The state needs your help to protect state systems and residents' information.

Cyber threats focus on the weakest link within systems, primarily the people using those systems. This document provides basic guidelines to reduce risks and ensure fundamental cybersecurity standards.

### Basic Guidelines for Appropriate Access to and Use of State Systems

#### Authentication and Access Control

1. Prohibit employees from sharing passwords.
2. Passwords used to access state systems must meet or exceed the following minimum requirements:
  - a. Must have at least eight (8) characters;
  - b. Must not have user's name, organization, or user id in the password;
  - c. Must contain three of these four data types: upper case alphabetic, lower case alphabetic, numeric, special character;
  - d. Must not be constructed of a single word found in the dictionary – passphrases constructed of multiple words are acceptable as long as they meet the other criteria outlined in this section; and
  - e. Users shall not be permitted to construct passwords that are identical or substantially similar to passwords that they had previously used.
  - f. Require password changes at least every 60 days.
3. Enforce a limit of no more than four consecutive invalid access attempts by a user before they are locked out.
4. Consider 2 factor or 2 step login (something you know and something you have) for access to systems and data for those users with elevated privileges.
5. Maintain a formal, documented process for granting and revoking access to all state systems that process or store sensitive information.
6. Require segregation of duties and the principle of least privilege for employees (they can access only the information and resources necessary for their specific job responsibilities).
7. Immediately revoke access rights upon employee separation or if a change in job role eliminates the requirement for continued access.
8. Ensure all access rights are reviewed at least annually by appropriate supervisor(s). Consider conducting this review during annual employee performance evaluations.

## Media Protection and Information Transfer

9. Provide direction to employees for securely handling, transporting, storing, and disposing of electronic media such as USB flash drives, CDs, and DVDs, as well as printed media such as paper copies of information printed from state systems.
10. Comply with all applicable laws pertaining to the retention and disposition of public records, including sections 19.21-19.39, Wis. Stats., and chapter Adm 12, Wis. Admin. Code.
11. Only use encrypted communications to transfer controlled or sensitive information – for example, SSL (Secure Sockets Layer).
12. Restrict staff from forwarding sensitive information to personal email or social media.

## System Security and Vulnerability Management

13. Replace unsupported hardware and software on a timely basis.
14. Ensure all networked devices have up-to-date:
  - a. Patches / Firmware (no later than 30 days of release by vendor)
  - b. Antivirus software
  - c. Spam and spyware protections
  - d. Web filtering software to protect against malicious websites
15. Ensure employees lock desktops when they walk away.
16. Implement password-protected screensavers to activate after no longer than 15 minutes of non-use.
17. Employ appropriate physical safeguards and visitor access controls to prevent unauthorized access to all areas and systems used to process or store state data.
18. Consider cyber liability insurance; some insurance includes some compliance services with the insurance.
19. Retention of backups offsite is strongly recommended.
20. Retention of login records is strongly recommended.

Immediately notify all appropriate parties in the event of inappropriate/unauthorized disclosure/use of information is suspected or confirmed. Contact the State Chief Information Security Officer: Bill Nash, 608.224.3779, [Bill.Nash@wisconsin.gov](mailto:Bill.Nash@wisconsin.gov) for events involving state systems/data.

## Awareness and Training

21. Conduct annual cybersecurity awareness training for employees and contract staff.

###

Thank you to Wisconsin CIO David Cagigal and CISO Bill Nash for providing this document

## Resources

- 1 See, e.g., <https://statescoop.com/ransomware-attacks-map-state-local-government/>.
- 2 NGA competitively selected Arkansas, Massachusetts and Ohio to focus on projects related to state and local partnerships in cybersecurity. <https://www.nga.org/news/press-releases/nga-to-assist-7-states-on-cybersecurity-strategies/>
- 3 <https://www.in.gov/cybersecurity/files/Cybersecurity-Report-FINAL-Full-Report1.pdf>
- 4 [https://www.in.gov/cybersecurity/files/Indiana-Emergency-Management-Cybersecurity-Toolkit-FINAL\\_Oct%202019.pdf](https://www.in.gov/cybersecurity/files/Indiana-Emergency-Management-Cybersecurity-Toolkit-FINAL_Oct%202019.pdf)
- 5 <https://www.govtech.com/pcio/How-Louisiana-Responded-to-Its-Recent-Ransomware-Attacks.html>

## Principle Authors

### Meredith Ward

Director, Policy & Research

National Association of State Chief Information Officers

[mward@nascio.org](mailto:mward@nascio.org)

### Maggie Brunner, JD

Program Director, Homeland Security & Public Safety Division

NGA Center for Best Practices

National Governors Association

[mbrunner@nga.org](mailto:mbrunner@nga.org)



### About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state 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. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit [www.NASCIO.org](http://www.NASCIO.org).



### About NGA

Founded in 1908, the National Governors Association is the voice of the nation's governors and one of the most respected public policy organizations in the country. The association's members are the governors of the 55 states, territories and commonwealths. Members come to the association from across the political spectrum, but NGA itself is boldly bipartisan. Because of that, governors can share best practices, speak with an informed voice on national policy and develop innovative solutions that improve citizens' lives through state government and support the principles of federalism.