CIS Center for Internet Security®

CTG UNIVERSITY AT ALBANY State University of New York

Managing Cyber Threats through Effective Governance

A *Call to Action* for Governors and State Legislatures

October 2020

This document was created in partnership with

NCSL NATIONAL CONFERENCE OF STATE LEGISLATURES

NGA NATIONAL GOVERNORS ASSOCIATION

Acknowledgments

The Center for Internet Security (CIS) and the Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany) would like to recognize the following individuals for their support in creating this *Call to Action*. Their time and experience were invaluable in completing this work.

Authors

John Gilligan, President and CEO, CIS
Theresa A. Pardo, Director, CTG UAlbany, Special Assistant to the President, University at Albany

Contributing Authors

Meghan Cook, Program Director, CTG UAlbany
Mike Garcia, Senior Advisor for Elections, CIS
Stephanie Gass, Cybersecurity Governance Project Lead, Senior Information Security Auditor, CIS
Jackson Koutsos, Cybersecurity Governance Intern, University of Maryland
Autum Pylant, Senior Communications Specialist, CIS

State Government Officials

Sincere thanks to the 13 state government officials who spoke with us about cybersecurity governance. Their frank and practical insights and deep experiences were critical to the development of this *Call to Action*.

Curtis Clan, CISO, Tennessee
Chris DeRusha, former CSO, Michigan
Daniel Dister, CISO, New Hampshire
Adam Ford, CISO, Illinois
Michael Geraghty, CISO, New Jersey
Vincent Hoang, CISO, Hawaii
Nancy Rainosek, CISO, Texas
Dan Sluga, Deputy CISO, Illinois
Maria S. Thompson, CRO, North Carolina
Thomas Vaughn, CISO, Florida
Michael Watson, CISO, Virginia
Jay White, CISO, Mississippi
Sean Wiese, former Cyber Operations Lead, North Dakota

Project Advisory Board and Expert Advisers

Sincere thanks to the members of the project Advisory Board and our esteemed colleagues who provided expert advice to ensure this *Call to Action* resonates with governors and members of state legislatures.

Advisory Board

Sean Atkinson, CIS
Peter Bloniarz, NYS Cyber Security Advisory Board
Brian de Vallance, CIS
Curtis Dukes, CIS
Mike Garcia, CIS
John Gilligan, CIS
Theresa A. Pardo, CTG UAlbany
Douglas Robinson, National Association of State Chief Information Officers (NASCIO)

Expert Advisors

Margaret Brunner, National Governors Association (NGA)
Susan Frederick, National Conference of State Legislatures (NCSL)
Pam Greenberg, NCSL
Abbie Gruwell, NCSL
Brian Nussbaum, College of Emergency Response, Homeland Security and Cybersecurity, University at Albany, SUNY
Matt Pincus, NASCIO

Contents

Executive Summary

Cybersecurity threats are an ever-present organizational risk on par with economic, legal, operational, financial, and political risks. They increasingly affect state assets. Managing these risks, and the threats from which they stem, must be part of a state's overall risk management portfolio. To do this, state leaders must have effective cybersecurity governance.

Cybersecurity governance is the processes by which decisions are made about cybersecurity risk. Effective cybersecurity governance provides the mix of control and influence necessary and appropriate for a state, and includes mechanisms for mitigating and responding to risk.

A *Call to Action*

This document is a *Call to Action* for governors and state legislatures to improve their cybersecurity risk management capabilities by creating or strengthening their cybersecurity governance. It presents four recommended action steps and a set of tools to guide the decisions states must make and execute to respond to an ever-increasing and evolving threat to state assets and operations.

While every state has implemented cybersecurity programs, few have cybersecurity governance that effectively ensures that a state's risk is managed to a level and in ways that have been determined to be, through formalized governance processes, acceptable to the governor and legislature. An effective cybersecurity governance framework answers important questions such as:

- What decisions need to be made about cybersecurity threats?
- Who makes those decisions?
- How are those decisions made?
- What mechanisms exist to inform those decisions?
- Who has responsibility for translating decisions made by cybersecurity governance into effective cybersecurity programs?
- What processes exist to make sure that the cybersecurity programs are effective?

This *Call to Action* presents four steps to be taken by governors and state legislatures to establish or strengthen their cybersecurity governance:

1. Establish Authorities through Executive Order and Legislation
2. Formalize Key Processes
3. Assign Roles and Responsibilities
4. Monitor Indicators for Decision-Making and Adaptation

It also includes eight tools that states have found useful in strengthening their cybersecurity governance, as well as questions that governors and state legislatures can ask to help determine whether their cybersecurity governance is effective in addressing and minimizing the threats their states face.

Fighting with One Army

...we're fighting with many armies and we need to be fighting with one. ... There has to be an army of one to improve our effectiveness in cybersecurity in the government. That only happens with governance.

Texas

Once established, cybersecurity governance must be agile, allowing cybersecurity programs to evolve as new threats that require adaptations in risk management strategies emerge. As smaller organizations become increasingly aware of their limits in understanding threats and managing their risk, they are looking to state partners for assistance. Expanding scope beyond executive level agency assets, to a "whole of state" perspective that engages stakeholders across multiple sectors and levels of government in a coordinated and collaborative process of risk management, is increasingly recognized as an important step in managing a state's cybersecurity risks.

An Increasing Threat to State Assets

The Frontier of Cybersecurity

"The frontier of cybersecurity today is ensuring that time-tested, risk-based techniques for hardening systems, training users, and sharing information are implemented, sustained, and coordinated. Organizations accomplish these objectives through governance, the 'formal and informal institutions that [influence how] a group of people determine what to decide, how to decide, and who shall decide.'"

Garcia, Forscey, and Blute

Beyond the Network: A Holistic Perspective on State Cybersecurity Governance. (96 Neb. L. Rev. 252 (2017); https://digitalcommons.unl.edu/nlr/vol96/iss2/3)

Cyber threats pose an increasingly significant risk to state governments and to the services that the public depend on. The information technology infrastructure that states have grown to rely on over the past half century poses as much risk to their operations as the lead water pipes and rusting bridges that more visibly demand our attention. Managing these risks must be part of a state's overall risk management portfolio. To do this, state leaders must have effective cybersecurity governance.

In some states, governance structures are defined through executive orders and administrative code. Other states use legislation to formally establish governance. Some states have found that while their governors and other top elected officials have attempted to increase cybersecurity capability and capacity, efforts have fallen short due to the lack of a formally established governance structure. Without an overarching governance structure, it is difficult to sustain coherent and consistent cybersecurity programs and practices.

This document is a *Call to Action* for governors and state legislatures to strengthen their cybersecurity risk management capability through creating or strengthening their cybersecurity governance. It presents four recommended action steps and a set of tools to guide the decisions that must be made and executed if states are to be prepared to respond to ever-increasing and evolving threats to state assets.

What is Cybersecurity Governance?

Cybersecurity governance is the processes by which decisions are made about cybersecurity risk, and effective programs established that manage that risk to a degree that is acceptable to the governor and legislature. If done well, cybersecurity governance defines priorities, processes, metrics, tolerances, and implementation methods. It is codified in legislation and executive orders that provide a framework for written policies and procedures. It integrates with and reflects the structure of the state's overall IT governance. And, most importantly, cybersecurity governance establishes a state-specific structure to be followed by the state's cybersecurity operational teams when identifying, quantifying, and managing cybersecurity risks on a statewide level.

Every state has cybersecurity programs—offices, standards, guidebooks, procedures, and incident response plans—that protect the state from cyber threats and enable it to respond quickly when that protection fails. Cybersecurity governance, on the other hand, is the framework that guides these programs and links them to the state's risk management processes. Cybersecurity governance:

- Consists of the executive level decision-making processes and the policies and procedures for overseeing the cybersecurity programs
- Provides the necessary control and influence a state's elected leaders need to have over their state's cybersecurity programs
- Establishes clear definitions and assigns roles and responsibilities
- Defines processes, tolerances, metrics, priorities, and implementation methods
- Links the state's cybersecurity programs into decision-making processes that enable the state's elected leaders to understand and minimize the cybersecurity risks that their state faces

If done well, a cybersecurity governance framework answers important questions, such as:

- What decisions need to be made about cybersecurity threats?
- Who makes those decisions?
- How are those decisions made?
- What mechanisms exist to inform those decisions?
- Who has responsibility for translating decisions made by cybersecurity governance into effective cybersecurity programs?
- What processes exist to make sure that the cybersecurity programs are effective?

Reducing Risk by Reducing Waivers

One of the biggest threats I've seen to our cybersecurity programs is the granting of waivers. If we had effective cyber governance, waivers could be limited to very specific conditions.

New Hampshire

While every state has cybersecurity programs, not all states have effective cybersecurity governance that ensures the state's risk is managed at an appropriate level and to a sufficient degree. As a governor and legislature, understanding the risk the state faces and the programs to mitigate those risks provides an impetus for improving the state's cybersecurity. In today's cyber risk environment—where essential services depend on technology working and where our cyber adversaries get smarter and more sophisticated every day—it is essential that states establish effective cyber governance so that they can adapt quickly and keep up with the increasing and changing threats to state assets.

Agility: A Critical Cybersecurity Governance Design Priority

As governors and state legislatures commit to taking action to manage their risk, they must also recognize that creating and strengthening cybersecurity governance requires a continuous process of understanding cyber threats and translating that knowledge into appropriate cybersecurity actions. A cyclic "risk-based" approach ensures that a state has the agility necessary to successfully evolve its cybersecurity risk management capability. Cybersecurity governance must be tailored to keep up with current risks and agile enough to adapt to future risks.

Establishing Cybersecurity Governance within a Specific State Context

State government leaders must manage risk within a context where authority is distributed across sectors and levels and branches of government. Regardless of the structures and local culture that a governor and state legislature must operate within, they must establish cybersecurity governance that provides the mix of control and influence necessary and appropriate for their state, and that includes mechanisms for mitigating and responding to risk.

Most states have already established some form of cybersecurity governance. Some have the "centralized structure" recommended by many experts, essentially placing decision-making authority on cybersecurity in one or more central organizations and, in many cases, embedding cybersecurity governance within the state's centralized information technology services organization. Others have a more decentralized approach to establishing the desired control and influence, while still others have implemented hybrid models with a mix of centralized and decentralized authorities, roles, and responsibilities.

Cybersecurity Governance Approaches

Centralized. Authority and decision-making vested within a central body.

Decentralized. Authority and decision-making distributed to individual organizations.

Hybrid. Authority and decision-making distributed between a central body and individual sub-organizations.

Many organizations, including the National Association of State Chief Information Officers, strongly recommend a centralized approach to cybersecurity governance. While full centralization may be out of reach for many states given their current culture and structures, evolving away from fully decentralized toward centralization is highly recommended. Ultimately, of course, day-to-day responsibility for managing cyber risk falls to the governor, like it does for all of the state's risks. Regardless of where a state starts with cyber governance, what is in place must support a tolerance for risk that reflects the intentions of the governor and legislature. It must put in place policies and processes that enable the elected officials to understand the state's risks and act effectively to manage those risks.

Four Actions Steps for Governors and State Legislatures

When establishing cybersecurity governance, whether through executive order, legislation, or administrative code, governors and state legislatures must ensure that their cybersecurity governance has the elements necessary to effectively manage their risks. The governance structure must designate specific units with both responsibility for cybersecurity and the authority to carry out those responsibilities. It must spell out how authority should be exercised and where collaboration with other stakeholders should take place in preparing for and responding to cybersecurity threats.

Four action steps are being used across the United States by governors and state legislatures as they work to establish cybersecurity governance (See also Appendix A):

1. **Establish Authorities through Executive Order and Legislation.** Executive orders and legislation are being used by governors to formally establish the entities and authorities required to govern cybersecurity. Such authorities are being designed to overcome existing fragmentation in cyber governance and, where possible, are leveraging strong existing governance structures.

2 **Formalize Key Processes.** An effective governance framework formalizes key processes, including financial, procurement, technical standards, and risk assessment, necessary to effectively identify and manage cyber risks.

3 **Assign Roles and Responsibilities.** An effective governance framework includes an assignment of roles and responsibilities for designing and implementing the state's cybersecurity program as directed by the governor and/or legislature.

4 **Monitor Indicators for Decision-Making and Adaptation.** An effective governance framework requires the use of relevant indicators, beyond incident reporting, in decision-making processes to guide cybersecurity governance strategies and execution (See Appendix B for the recommended indicators).

Tools for Cybersecurity Governance

Eight tools are being used by states to execute the authorities established in their governance frameworks (See Appendix C for the detailed description of the tools).

1 Enterprise Architecture

2 Cyber Risk Assessments

3 Control over IT Procurement and Acquisition

4 Control over Network Connectivity

5 Councils and Advisory Boards

6 Complementary Legislation

7 Collaboration and Shared Services Agreements

8 Monitor Workforce Requirements and Close Gaps

These tools are critical to states' efforts to gain compliance, even within executive agencies, with the standard policies and procedures required to systematically manage risk. Critical to the success of cybersecurity governance, and to the use of these tools, is the existence of some level of effective information technology governance. Governance tools such as the use of formal risk assessments and standards are more well-known and used. Where there is a recognized need for organizations to work together, and authority to compel participation is limited or missing, other tools, such as agreements and collaborations are necessary. These tools are critical for addressing the often weak or missing authority that executive agencies have to establish the interagency, intergovernmental, and inter-sectoral agreements that are necessary to formalize collaborations.

Tool Example: Control over Network Connectivity

State Cybersecurity Official. We're our own service provider, and we also serve as a service provider to the other elected constitutional offices. That gives us the ability to funnel network traffic through a shared set of security appliances that we manage and maintain and provide to them.

North Dakota. We've got network connectivity covering all seven branches of government, enabling visibility into the traffic at a network layer across the whole state. This provides us with a leg up in evaluating activity, looking for threat related traffic/ information to make sure that we are being protected.

Expanding Scope: Building a Whole of State Risk Management Program

Ready for Next Order Problems

Because of the things [we've done] like being centralized, having staff, having budget, we've been able to start focusing on those next order problems. Like, what do you do to protect and help the locals? How do you partner with industry?

State Cybersecurity Official

Critical Success Factors

You have to find those willing participants, and you have to find that champion that can effectively message the ultimate effects of a cyber-attack. We have a moral responsibility to protect the citizens of our state, so it's going to take a collective approach to protecting the infrastructure, the people, the data, and everything that goes with it on a day-to-day basis. You need to first and foremost understand what your current state is in order to determine what you need to do for the future.

North Dakota

This document provides a recommended set of actions for governors and state legislatures to take today to create or strengthen their cybersecurity governance. Cybersecurity governance can't be static; strategies must evolve if states are going to effectively protect state government assets. States must improve their governance to ensure they are ready to adapt as new threats emerge and require new risk management strategies.

Increasingly, success will correlate with the extent to which states are able to expand the scope of their cybersecurity governance across all of a state's public and private critical infrastructures. This implies incremental expansion from executive level agency assets to a "whole of state" perspective that engages stakeholders across all branches, jurisdictions, and sectors in a collaborative process of risk management.

As smaller organizations become increasingly aware of the limits to their ability to locally manage risk, expansion will become increasingly acceptable and expected. Cybersecurity governance is key to navigating this expansion and to ensuring that funding is commensurate with a state's position with respect to actual measured risk.

In some states, such adaptation is achieved by expanding authority from solely controlling network connections to controlling IT procurement and other functions in order to ensure cybersecurity is addressed consistently and efficiently. In other states, it may mean expanding the scope of authority beyond state government or building collaborations that lead to joint agreements about how cybersecurity threats will be managed across multiple levels of government, including local government. Ideally, evolution of cyber governance will lead to both. What is critical, regardless of the maturity of any single state's cybersecurity governance, is an ongoing commitment to champion governance that is forward-thinking, adaptable, and responsive. A commitment to governance ensures that states, and not just state governments, are ready to adapt as threats evolve.

Expanding Scope

New Hampshire. The state education department in New Hampshire, for example, is required by law to establish minimum standards for security and privacy of student data. This is being accomplished through a collaboration between the state education department staff and the state CISO.

Texas. School districts are required by law to follow a cyber-framework and are required to report incidents to the state education department.

North Dakota. Legislation passed in the 2019 session set forth the ability and intended direction of cybersecurity strategic alignment across all seven branches of government in North Dakota.

Appendix A

Four Action Steps

Action	Action Description
Establish Authorities through Executive Order and Legislation	• Issue executive orders and enact legislation to formally establish the entities and authorities required to govern cybersecurity in your state. • Leverage the strengths of existing governance structures. • Design authorities to overcome fragmentation in cybersecurity governance and programs within the state.

Formalize Key Processes	• Ensure the governance framework includes formalization of key processes necessary to manage risk.
	• This can take the form of the definition, ongoing review, and implementation of processes designed to effectively identify and manage cyber risks (financial, procurement, technical standards, risk assessment processes) including responding to questions such as:
	  ◦ How are cybersecurity threats, vulnerabilities, and risks determined?
	  ◦ What level of cyber risk is acceptable to our governor and state legislature?
	  ◦ Who determines what controls to put in place to mitigate risk to an acceptable level?
	  ◦ How will controls be monitored on an ongoing basis and revised to respond to changing conditions?
	• Of particular importance are the processes required for ensuring predictable and stable funding to those charged with the ongoing responsibility for cybersecurity governance and those authorized through that governance to assess cybersecurity threats, design and execute responses, develop technical architectures/standards, and help to conceive and implement required processes.

Assign Roles and Responsibilities	• Ensure the governance framework includes processes for assigning the roles and responsibilities each of the state's units will take in designing and implementing the state's cybersecurity program. ◦ This includes state government program units, its IT units and any dedicated cybersecurity units, and external entities including the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) and federal and private sector cybersecurity units. • Ensure the governance framework includes processes for assigning the roles and responsibilities each of the state's units will take in establishing and managing collaborative approaches to cybersecurity.
Monitor Indicators for Decision-making and Adaptation	• Ensure your state's cybersecurity governance requires the use of robust and relevant indicators in decision-making, and establish policies and procedures for guiding their management and use. • Ensure cybersecurity governance requires the creation and ongoing review of robust and relevant indicators that go beyond the reporting of incidents, and that guide cybersecurity governance strategy and execution.

Center for Internet Security®

CTG UNIVERSITY AT ALBANY
State University of New York

Appendix B

Recommended Cybersecurity Governance Indicators

There are many metrics for assessing the adequacy of cybersecurity programs, but few for assessing cyber governance programs. A state's cybersecurity governance is effective if it reduces the state's risk. However, because there are few commonly-accepted metrics for measuring risk, measuring the effectiveness of governance is difficult. Furthermore, no states publish measurements of their cyber risk, so there are few benchmarks from other states for comparative purposes. Below we list some questions that governors and state legislatures should have answers to if their cybersecurity governance is effective in addressing and minimizing the threats their states face.

Category	Cybersecurity Governance Indicator
Preparedness	1 Do we know what the three biggest cyber risks are to our state? What are we doing about them?
	2 Have we been told how we are protecting our state's most important assets from the cyber threats they face?
	3 Do we know what the roles of central IT authorities (e.g., the State Chief Information Officer/State Chief Information Security Officer), agencies, and the IT departments are for protecting each agency's information assets?
	4 Do we get briefed on the annual Nationwide Cyber Security Review (NCSR)?
	5 Do we have an annual cyber risk assessment conducted by a reputable third party?
	6 Do we conduct regular employee cybersecurity training and perform regular email phishing exercises for our employees?
Incident Response	1 Do we have an annual tabletop exercise to test out our ability to respond quickly to a significant disruptive cyber incident?
	2 Do we know who is in charge when we have such an incident? Do we have clear guidance on the role of the governor, legislative leadership, and other elected officials when incidents occur?
	3 Do we have pre-prepared templates for communicating with our employees and the public if an incident occurs?
	4 What do we do if the incident is so severe that our resources can't handle it? What is our backup plan? If we are depending on cyber responders from other organizations, what if they are occupied dealing with their own incidents?
	5 If the incident is accompanied by or causes kinetic effects and other physical disruptions, how are our emergency management and cyber responses going to work together? Have we done tabletop exercises to shake down how well our cyber processes integrate with our physical disruption processes?
	6 Do we have an annual tabletop exercise with our agencies and IT units to test out our ability to recover from a cyber incident that causes significant and long-lasting disruptions to operations?
	7 Do we have a formal communication process for agencies to report cyber incidents, including cyber incidents in progress?
	8 Do we have a mutual aid plan and/or an Appendix to the State Emergency Plan to address relationships and communication pathways during large scale cybersecurity incidents?
Overall	1 Do we perform an annual review of the incidents we have experienced? What does it tell us, and how is it informing our state's protective measures?
	2 Are the state's Chief Risk Officer, the governor's Homeland Security Advisor, the governor's emergency management director, and the Chief Information Officer synchronized? Do they all give the same answers to the above questions?

Appendix C

Eight Cybersecurity Governance Tools

Tool	Tool Description
1 Enterprise Architecture	**An Enterprise Architecture (EA) is a critical tool for identifying and documenting the structure and operation of an organization, and the business processes, data, applications, and information technology infrastructure that supports it.** Within the EA Framework, business, technical, and performance reference models and standards for an enterprise are established. EA provides a touchstone for all technical investments. It is also a critical tool for modeling the potential negative consequences of investments that fall outside of the established standards.
2 Cyber Risk Assessments	**Many states require cyber risk assessments as part of regular reporting cycles, procurement decisions, and connecting to various networks.** Such assessments create visibility of risks and reinforce adoption of security best practices and products. They make it possible for information about the threat potential related to any one action or group of actions to be available for use in decision-making.
3 Control over IT Procurement and Acquisitions	**Many states place the Chief Information Officer and/or the Chief Information Security Officer (CIO and CISO) on the critical path to IT procurement.** Authority over IT procurement in executive agencies makes it possible for these officials to require that IT procurements meet state security standards and that selected procurements include an assessment of cyber risk. Establishing this level of authority over IT procurement in non-executive branch agencies (e.g., constitutional offices, judicial branch, legislative branch, exempt agencies like the state lotteries or the public institutions of higher education) is a long-term goal of cybersecurity governance bodies in many states.
4 Control over Network Connectivity	**Some states are able to manage risk because they have authority to control what connects to their networks.** In these states, CIOs and CISOs have been granted authority to require those seeking to connect to state networks to comply with the rules as established through governance processes. This authority provides the CIO and CISO indirect authority over IT procurement (i.e., if the item you want to purchase doesn't meet our standards, we can't stop you from buying it, but you may not connect it to the state's network).
5 Councils and Advisory Boards	**Many states are using Governance Councils and Advisory Boards as vehicles to execute cybersecurity governance put forward in executive orders and legislation.** These bodies are often used to interpret executive orders and legislation, establish operational policies and procedures for cybersecurity programs, and to monitor their performance.
6 Complementary Legislation	**Some states are passing laws, administrative rules, and statewide policies that complement existing cybersecurity governance legislation to focus on specific priority domains, such as school districts and student data.**
7 Collaboration and Shared Services Agreements	**Interagency.** Many state CIOs and CISOs only have authority over executive agencies under the control of the governor, and not those of separately-elected officials. Interagency agreements, including joint decision-making bodies, are being used in many states to bridge these gaps to create coherent government-wide cybersecurity programs at the state level. **Intergovernmental.** In most states, the state CIO and CISO have no authority over local government cybersecurity. However, a few states are moving to formalize authority and responsibilities for non-state government assets from a cybersecurity perspective. Many states are investing in the development of intergovernmental agreements and other collaboration tools focused on cybersecurity and, in particular, joint governance and shared operational capability. For instance, some states have highly centralized elections operations where the state, often through a state board of elections, directs procurements and standards for local election systems.
8 Monitor Workforce Requirements and Close Gaps	**Many states are struggling to fill cybersecurity positions.** One strategy for filling those positions and providing the continuous training required to stay current is to ensure your state's cybersecurity governance has policies and procedures for regularly identifying necessary cybersecurity skills and making provisions for buying and/or building those skills. These skills should include the ability to create and use indicators of program effectiveness, to perform risk assessments, and to effectively communicate risk to key stakeholders.

CIS

The Center for Internet Security, Inc. (CIS®) is a community-driven nonprofit, responsible for globally recognized best practices for securing IT systems and data including the CIS Benchmarks™ and CIS Controls®. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS-ISAC® and EI-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities and U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

CTG UAlbany

The Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany), is an award-winning research institute, world-renowned for transforming public service through innovations in technology, policy, and management. Established in 1993, CTG UAlbany has led applied research and problem-solving projects at all levels of government and around the world. These projects focus on making connections between critical questions about the potential of emerging technologies to create public value and the policy and management innovations needed to ensure sustainable value-creation. CTG UAlbany experts work to create, and then translate to practice, new knowledge about public service transformation and serve as advisors and facilitators for local, state, federal, and international government bodies, focusing on management and policy decisions. The Institute partners with governments and other organizations to address the critical interplay among policy, management, and technology innovations. CTG UAlbany works to leverage new and emerging technologies to transform public service and solve pressing public policy problems. Learn more at https://www.ctg.albany.edu/.

NCSL

The National Conference of State Legislatures (NCSL), founded in 1975, represents the legislatures in the states, territories, and commonwealths of the U.S. Its mission is to advance the effectiveness, independence, and integrity of legislatures, and to foster interstate cooperation and facilitate the exchange of information among legislatures. NCSL also represents legislatures in dealing with the federal government, especially in support of state sovereignty and state flexibility and protection from unfunded federal mandates and unwarranted federal preemption. The conference promotes cooperation between state legislatures in the U.S. and those in other countries. In addition, NCSL is committed to improving the operations and management of state legislatures, and the effectiveness of legislators and legislative staff. NCSL also encourages the practice of high standards of conduct by legislators and legislative staff.

NGA

Founded in 1908, the National Governors Association is the voice of the leaders of 55 states, territories, and commonwealths. Our nation's Governors are dedicated to leading bipartisan solutions that improve citizens' lives through state government. Through NGA, Governors identify priority issues and deal with matters of public policy and governance at the state, national, and global levels. NGA is the premier resource for not only Governors but also for their cabinet members, state policy experts, the U.S. Congress, and private enterprise. NGA offers an array of services to help collaboratively tell the states' story. Thanks to decades of broad expertise, NGA teams are able to work side-by-side with state leaders to identify challenges, help Governors stay ahead of the curve, and offer solutions before challenges become problems.

Center for Internet Security®

CTG
UNIVERSITY AT ALBANY
State University of New York

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity