NCSL | NATIONAL CONFERENCE of STATE LEGISLATURES

Cybersecurity Conversation Guide: Executive Branch, Legislative Branch and Higher Education

Dear Fellow State Legislators,

This Cybersecurity Conversation Guide has been developed for you to build on the efforts of the NCSL Executive Task Force on Cybersecurity and bring the conversation to your own state capitol. The task force was formed in 2016 to help state legislators understand and address the growing security risk posed by state and private computer networks. Task force members have learned from experts in computer science, information technology, law enforcement, emergency management and other fields.

While technology can be complicated, the task force has learned that technology policy does not have to be overly technical. The task force intends this guide to help break down misconceptions that cybersecurity is too sensitive or nuanced to be an appropriate topic for state legislatures to discuss. Legislatures in every state have a responsibility to provide oversight of executive and legislative branch cybersecurity actions, provide adequate funding for preventative and defensive measures, and encourage both public and private institutions to educate the necessary workforce to fill this critical sector.

We hope this guide will empower you to start asking the difficult, but necessary questions of our state governments. The guide includes an extensive, but not exhaustive, list of questions to help you gauge your state's cybersecurity readiness in the areas of risk assessment, cyber strategy, threat detection and remediation, budget, and cyber training and education. Ignorance can leave government systems weak against cyber-attacks, putting vital government services and infrastructure at risk. It is only with every state engaged that we will be able to reach our shared goal of a secure and safe future for our citizens.

Sincerely,

Jacqui V. Irwin
California State Assemblywoman
Co-Chair, NCSL Task Force on Cybersecurity

Thomas C. Alexander
South Carolina State Senator
Co-Chair, NCSL Task Force on Cybersecurity

The National Conference of State Legislatures (NCSL) is the bipartisan organization that serves the legislators and staffs of the states, commonwealths and territories.

NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues and is an effective and respected advocate for the interests of the states in the American federal system.

NCSL has three objectives:

- To improve the quality and effectiveness of state legislatures.
- To promote policy innovation and communication among state legislatures.
- To ensure state legislatures a strong, cohesive voice in the federal system.

NCSL Executive Task Force on Cybersecurity

Co-Chairs:

- Assemblywoman Jacqui V. Irwin, California
- Senator Thomas C. Alexander, South Carolina

Task Force Members by state:

- Katy Proctor, Director of Research, Majority Research Staff, House of Representatives, Arizona
- Brandon Bjerke, Legislative Aide, Office of Assemblymember Jacqui Irwin, California
- Representative Don L. Parsons, Georgia
- Diane Powers, Deputy Executive Director, Legislative Services Agency, Indiana
- Terri Clark, Director of Technical Services, Legislative Office of Information Services, Kansas
- Senator Whitney H. Westerfield, Kentucky
- Monique Appeaning, Fiscal Analyst/Special Projects Coordinator, Legislative Fiscal Office, Louisiana
- Senator Susan C. Lee, Maryland
- Representative Angelo J. Puppolo, Jr., Massachusetts
- Representative Pat Garofalo, Minnesota
- Representative Scott DeLano, Mississippi
- Representative Daniel Zolnikov, Montana
- Representative Kelly K. Fajardo, New Mexico
- Senator Louis P. DiPalma, Rhode Island
- Representative Stephen R. Ucci, Rhode Island
- Mark Humphrey, Director, Information Systems Division, Legislative Council, Texas
- Senator Wayne A. Harper, Utah
- Delegate Richard L. Anderson, Virginia
- Senator Frank Wagner, Virginia
- Lisa Wallmeyer, Executive Director, Joint Commission on Technology and Science, Virginia
- Senator Sharon R. Brown, Washington
- Representative Zack Hudgins, Washington
- Representative Cindy S. Ryu, Washington

NCSL Staff:

Susan Parnas Frederick,Washington, D.C.
Danielle Dean,Washington, D.C.

Pam Greenberg, Denver
Heather Morton, Denver

For their generous support of this task force, NCSL gratefully acknowledges these organizations:

- **AT&T**
- **Microsoft**
- **VMWare**
- Apollo Education Group, Inc.
- CompTIA
- CTIA-The Wireless Association
- Force Training Directorate, Office of the Assistant Secretary of Defense Readiness, Department of Defense
- MasterCard Worldwide
- Toyota Motor North America
- Walmart

NCSL thanks the National Association of State Information Officers (NASCIO) staff for assisting with this document.

STEP 1: COLLECT BACKGROUND INFORMATION

Familiarize yourself with the state personnel and legislative branch colleagues who handle or have an interest in cybersecurity for your state and any existing cybersecurity laws and legislation in your state.

- ☐ Determine through your leadership and policy staff which legislative committee(s) covers cybersecurity issues. Are there any special state commissions or task forces that examine cybersecurity issues? Who is in charge of IT services for the legislative branch?

- ☐ Identify through your governor and executive branch staff who your state chief information officer and state chief information security officer are. Find out who your state CIO is here.

The state chief information officer (CIO) is a governor-appointed position; every state has a state CIO. At a basic level, state CIOs provide information technology (IT) services to state executive branch agencies. As such, they are leaders well versed in delivering cost-effective IT solutions to their customer state agencies. Governance models for state CIOs differ by state. State CIOs in Mississippi and Texas report to a board, while 23 state CIOs report to an agency head and 25 state CIOs report directly to the governor.

The state chief information security officer (CISO) position exists in every state and all but one CISO (South Carolina) reports to the CIO. The CISO's main responsibility is to develop and maintain a cybersecurity plan and security policies throughout the executive branch.

For more on state laws and state CIO and CISO governance structures, see:

- State CIO Leadership in Government Innovation and Transformation, NASCIO.
- State Statutes Creating Chief Information Security Officer Positions in State Government, NCSL.
- State Data Security Laws | State Government, NCSL.

STEP 2: START THE CONVERSATION WITH THE EXECUTIVE BRANCH

The following general questions are best answered by your state CIO and/or CISO. They will build upon the background knowledge you collected and provide insight into your state's cybersecurity readiness through four key areas: risk assessment and cyber strategy, threat detection and remediation, cyber training and education, and budget and funding.

- ☐ Who are your executive branch customers? If there are parts of state government not under your control (i.e. constitutional officers), who are your counterparts in those offices? Does your authority extend to local jurisdictions such as cities, counties, parishes, or school districts?

- ☐ CIO question—What are the programmatic priorities for your office? Who sets the priorities for your office?

    - ☐ How often is the overall security strategy updated?

    - ☐ Are audits part of the overall security plan?

- □ CISO question—What are the cybersecurity priorities for your office?

- □ Is your department of emergency management involved in cybersecurity issues? Is your state National Guard? Law enforcement? What are each of their roles?

- □ What are your major areas of concern? (Possible areas include budget constraints and workforce development and retention).

    - □ If workforce development is a concern—Do you have a workforce development and retention strategy? If yes, please explain. If no, why not?

- □ How can I help promote a “culture of information security” with a governance structure including state leadership and all key stakeholders?

    - □ Who are the key stakeholders who should be included?

    - □ State CIO question—Do you have visibility over the entire enterprise (can you see what is going on in every agency)?

        - ▪ Would it help you to have legislation requiring all agency CIOs to report to you as the state CIO?

In some states, agency CIOs are independent from the state CIO so this may be a good policy area to consider—legislation can be drafted to require centrality, more structure, and oversight. For more on state CIO governance structures, see:

- Information Technology IT Governance and Structure, NCSL.

Risk Assessment and Cyber Strategy Questions

- □ Have you conducted a risk assessment?

    - □ What are the major components of the risk assessment?

    - □ Who actually conducts those and how frequently are they done?

    - □ Is data classified by risk?

    - □ Are security metrics available?

    - □ What are our current risks and how serious are they?

    - □ To whom are they available?

    - □ Can legislators who work on cyber issues receive periodic briefings from you and your staff on risk assessment?

- □ Have we implemented a statewide cybersecurity strategy that includes policies, control objectives, practices, standards, and compliance?
    - □ If no, why not?
    - □ If yes, what is our cybersecurity strategy based on?
    - □ What is the scope of the framework? Does it apply to executive, legislative and judicial branches? Regents and higher education institutions? Large agencies, e.g., Departments of Revenue and Transportation?
    - □ How is compliance enforced?

The National Institute of Standards and Technology (NIST) has created voluntary guidance to help organizations manage and reduce cybersecurity risk. Based on existing standards, guidelines and practices, the NIST Cybersecurity Framework can assist in increasing cybersecurity management communications, see:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework.

- □ Have you looked into the option of cyber insurance? Are vendors required to have cyber insurance? Please elaborate.

Threat Detection and Remediation Questions

- □ Have we invested in statewide solutions that provide continuous cyber threat detection, mitigation and vulnerability management?
    - □ Is this working? If not, what other tools or resources do you need? (Are you using any advanced cyber threat analytics?).
- □ Do you produce regular threat reports? How often are they produced? Can I see them?
    - □ Where are the specific threats that we can control coming from?
    - □ What percentage of the threats come from inside state government?
    - □ Can members of the legislature who work on cyber issues receive periodic briefings on threats to state systems?

Cyber Training and Education Questions

- □ What opportunities are available to you on updates to the best practices in the field?

□ Have state employees and contractors been trained for their roles and responsibilities in protecting the state's network and assets?

□ Is staff informed of the importance of updating software regularly? Is this being done? Please explain.

□ Are you alerting staff to phishing scams?

□ What are the authentication standards used in each agency?

□ Is there state-wide protocol for cyber hygiene in place for state employees?

Cyber hygiene is the establishment and maintenance of an individual's and an organization's online safety. Drawing on the concept of personal hygiene, cyber hygiene incorporates the behaviors and process to maintain a user's online security such as using a firewall, updating virus definitions and software, utilizing strong password protocols, and data backup systems, see:

- National Campaign for Cyber Hygiene, Center for Internet Security.

□ Are all state employees required to have cyber hygiene training? How often? How is this training verified?

  □ Are there consequences for state employees who don't undergo this training (e.g., restrictions of access to state systems)?

□ Does your state have a cyber disruption response plan or a crisis communication plan focused on cybersecurity incidents?

A cyber incident tends to be the more routine type of attack that is typically fully managed within the state CISO's purview, such as a data breach or a denial of service attack on a state website. In contrast, a cyber disruption is a much larger event, that requires a coordinated response from a whole host of organizations including state emergency management, law enforcement, homeland security, and other governmental organizations. A cyber disruption may cause or coincide with a man-made or natural disaster, with significant or catastrophic effects, such as cyber attacks on the power grid or water treatment plants. Recognizing the cross-jurisdictional impact of a cyber disruption, a cyber disruption response plan addresses events that have a wide scope and involve many different response stakeholders including other service areas or industries, see:

- Cyber-Disruption Response Planning Guide, NASCIO.

□ Do you prepare threat reports on a regular basis? How often? Who sees them? Can I?

□ How much of our statewide system is outdated? What plans are in place to address this problem?

Legacy systems refers to old or outdated technology, applications, or a computer system. Legacy systems tend to be more expensive to maintain and more difficult to secure.

□ Is there regular collaboration on cybersecurity issues and incidents between the three branches of government, local department of homeland security officers, state law enforcement agencies and the National Guard?

Budget and Funding Questions

□ How is your office funded? Do you operate on a chargeback basis or do you receive an appropriation?

The vast majority of state CIO organizations operate on a chargeback basis and do not receive general fund dollars. Chargeback means that the state CIO office provides IT services and directly bills customer agencies for services rendered. In most cases, overhead costs are embedded in service offerings but sometimes this cost is provided by the general fund. The budgets for Mississippi and Connecticut are provided via general fund.

□ What was your most recent appropriation and how is it allocated (e.g., between staff, software, hardware)?

□ How many funding sources support your state's cybersecurity needs? Have you partnered with any outside vendors to help offset the costs for cybersecurity support? Do you have federal funding to help support cybersecurity efforts?

□ Do you participate in budget hearings? If yes, did you have any communications with members of the legislature's appropriations committees prior to your budget hearing? If so, who did you meet with and what information about your budget request did you share?

□ Does your office, or your executive branch customers, report cybersecurity spending separately than other IT spending? Can that reporting be incorporated in the future to track spending on security efforts?

□ What level of appropriation do you need for this fiscal year? If you are requesting an increase in appropriation, what is the primary area which is the basis for your requests?

□ Do you have a five-year plan projection on the resources needs for the cybersecurity operations?

□ Have you fully and properly evaluated existing resources and are you actively looking into finding lower cost solutions? Please explain.

- □ Has the state homeland security or emergency management office reached out to you regarding the use of federal homeland security grant funds which include cyber as an allowable use?

- □ Are you using the free Multi-State Information Sharing and Analysis Center? To what extent?

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a cybersecurity operations center that provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response to the nation's state, local, tribal and territorial governments, see:

- MS-ISAC, Center for Internet Security.

- □ Aside from an appropriation, is there any legislation that would help with keeping our state systems safe?

STEP 3: START THE CONVERSATION WITH LEGISLATORS AND LEGISLATIVE STAFF.
The following questions may be used to begin a conversation with legislative leadership, legislative management or legislative technology committees, and/or key management and information technology staff.

Risk Assessment and Cyber Strategy Questions

- □ Has the legislature conducted a risk assessment of the legislative technology system?
  - □ Who actually conducts the risk assessments and how frequently are they done?
  - □ What are our current risks and how serious are they?
  - □ Is data classified by risk?
  - □ Are security metrics available?
  - □ Can legislators who work on cyber issues receive periodic briefings from you and your staff on risk assessment?

- □ Have we implemented a cybersecurity strategy for the legislature that includes policies, control objectives, practices, standards, and compliance?
  - □ If no, why not?
  - □ If yes, what is our cybersecurity strategy based on? (See e.g., NIST Cybersecurity Framework).

    - □ What is the scope of the framework?

    - □ How is compliance enforced?

- □ Is there regular conversation about cybersecurity issues and incidents between the three branches of government, local department of homeland security officers, statewide law enforcement agencies and the National Guard?

Threat Detection and Remediation Questions

- □ Is there a need to work or partner with the executive branch for solutions that provide continuous cyber threat detection, mitigation and vulnerability management?

- □ Do you produce regular threat reports? How often are they produced? Can I see them?

    - □ Where are the specific threats that we can control coming from?

    - □ What percentage of the threats come from inside state government?

    - □ Can members of the legislature who work on cyber issues receive periodic briefings on threats to legislative systems?

Cyber Training and Education Questions

- □ Have legislative employees and contractors been trained for their roles and responsibilities in protecting the legislature's network and assets?

- □ How are you informing yourself of best practices in the field?

- □ Does the legislature follow any protocol for cyber hygiene?

- □ Are all legislative employees required to have cyber hygiene training? How often? How is this training verified? Are there consequences for not undergoing this training? What are they?

- □ Does the legislature have a cyber disruption response plan or a crisis communication plan focused on cybersecurity incidents? (See e.g.,: NASCIO's Cyber-Disruption Response Planning Guide).

- □ How much of our legislature's IT system is outdated? What plans are in place to address this problem?

Budget Questions for Members and Staff of Legislative Budget/Appropriations Committees

- □ How is cybersecurity funded for the legislature?

- □ Does the budget process allow for a discussion of cybersecurity spending? Can more opportunities be created to allow department IT staff to inform the members and staff throughout the legislative session?

- □ How do you evaluate an appropriation request for cybersecurity? What justifications do you look for?

- □ Has the state homeland security or emergency management office reached out to you regarding the use of federal homeland security grant funds which include cyber as an allowable use?

STEP 4: START THE CONVERSATION WITH HIGHER EDUCATION INSTITUTIONS.

The following questions should be addressed to higher education administrators and faculty to assess the status of the cybersecurity and IT workforce in your state. These questions can be used as you familiarize yourself with the higher education institutions in your state offering computer science education, identifying key administrators and faculty representatives in charge of workforce development.

- □ What metrics do you have on current enrollment in computer science and engineering programs?

- □ What metrics do you have on the employment rate of your computer science and engineering graduates and other job market indicators?

- □ What are your current program offerings for computer science that focus on cybersecurity? Do you plan to expand your offerings or target your curriculum to train for specific cybersecurity roles?

- □ Do you currently have any partnerships with technology companies for curriculum development, internships, or job placement? Any partnerships with certification programs in IT or cybersecurity fields?

- □ Is there anything the state legislature can do, other than more funding, to make computer science and cybersecurity education more efficient in our state?

- □ If more funding was available, what programs or initiatives hold the most promise in creating new cybersecurity professionals in the near term?

CONCLUSION

We hope this Cybersecurity Conversation Guide will help you ask the difficult, but necessary, questions as you seek information from the various government entities in your state regarding their cybersecurity readiness. Although this guide contains an extensive list of questions to help generate discussion and information-gathering, it is not an exhaustive list. The questions are designed to help you focus on risk assessment, cyber strategy, threat detection and remediation, budget and cyber training and workforce issues. As you start conversations with the key cybersecurity and technology stakeholders, you may find yourself developing your own questions unique to your own state.