Addressing Cybersecurity for Critical Energy Infrastructure through State Governing Bodies

Executive Summary

This paper reviews eight states that have made a concerted effort to address vulnerabilities facing the cybersecurity of the critical energy sector through a statewide governance body. These statewide governance bodies are tasked with developing recommendations for policymakers on a host of issues; identifying best practices; providing strategic direction on cybersecurity plans for state agencies; recommending training for state employees; and addressing cybersecurity workforce or professional development issues in the state. This paper addresses practices Governors can follow to establish effective cybersecurity governance bodies that support critical infrastructure cybersecurity, with a focus on the energy sector.

Overview

Governors often use governance bodies – also commonly referred to as councils, task forces, boards, working groups or commissions – to address important and complex subjects such as cybersecurity. These bodies can serve a variety of purposes – from making recommendations, advising the Governor on an issue, and crafting the state's strategic plan. As the cybersecurity threat landscape continues to evolve and our dependency on technology grows, Governors are sharpening their focus on addressing cybersecurity vulnerabilities in their states. With malicious actors continually attempting to access parts of our nation's critical infrastructure, some states have expanded the breadth of their statewide homeland security advisory council or cyber governance body to include critical infrastructure protection, specifically focusing on the energy sector. Others have created a statewide task force to engage specifically on energy sector cybersecurity.

NATIONAL GOVERNORS ASSOCIATION

Given this issue crosses many state entities, statewide coordination of public and private entities should be sponsored and driven by the Governor's office. This includes developing a whole-of-state approach for guiding practices to establish open communications and help officials work together effectively to identify, protect, and detect cyber threats, while responding to and recovering from cyberattacks on critical energy infrastructure. The components that make up the national power grid are among the most important assets within the nation's critical infrastructure. Without energy, everything from emergency services to residential lighting would not work. It is the "backbone of our nation's economy, security, and health."[i]

This paper reviews eight states that have made a concerted effort to address vulnerabilities facing the cybersecurity of the critical energy sector. These statewide governance bodies vary in how they were established, their lifespan, mission, authorities, size, and public reporting requirements. Overall, the bodies are tasked with developing recommendations for their Governor or legislature on a host of issues; identifying best practices; providing strategic direction on cybersecurity plans for state agencies; recommending training for state employees; and addressing cybersecurity workforce or professional development issues in the state.

This paper addresses practices Governors can follow to establish effective cybersecurity governance bodies that support critical infrastructure cybersecurity, with a focus on the energy sector.

Cybersecurity Governance Bodies: Common Approaches to Address Critical Energy Infrastructure

Governors have the authority to set their states' cybersecurity strategies and often delegate that responsibility to a central governance body. The type of body a Governor creates should account for state needs and typically include holistic representation from sectors that have a stake in the state's cybersecurity governance ecosystem. An examination of existing bodies indicates that Governors incorporate a mix of three approaches when creating a governance body, tasking them to:

1) Develop a strategic plan that either improves the state's cybersecurity posture generally or addresses specific cybersecurity challenges within the state;
2) Develop recommendations and continuously advise the Governor on cybersecurity issues.
3) Assess the cybersecurity preparedness of state agencies or industries within the state; or identifying and detecting threats and implementing recommendations.

Experts recommend a cross-functional approach to improve cybersecurity governance for a state's critical energy infrastructure, with representation from

pertinent agencies. Cyber governance bodies may include representatives from state information technology departments, homeland security offices, emergency management agencies, the National Guard, state fusion centers, state energy offices, utility companies, public utility commissions, state departments of transportation, the education community, commerce departments, tax commissioners, and others. In addition to state representatives, states may include members from the private sector, federal agencies (e.g., FBI, DHS), local governments, critical infrastructure owners and operators, and other experts.

Governors base their cyber governance bodies' roles and responsibilities on the needs of the state and may consider specific needs of critical energy infrastructure as they assign them. To improve critical infrastructure security, Governors typically task these bodies with:

- Incorporating utilities into state emergency response planning efforts;
- Recommending how to manage cyber risks to critical infrastructure assets and data;
- Formalizing strategic cybersecurity partnerships across the public and private sectors;
- Improving threat information sharing between private and public critical infrastructure owners and operators;
- Recommending and promoting cyber awareness training for the state's electric sector;
- Identifying best practices on trainings and cyber exercises; and
- Evaluating existing statutes – such as open records exemptions or cybercrime enforcement – for needed updates given cyber risks.

Addressing Critical Infrastructure through State Cybersecurity Governance Bodies

As of early 2021, at least eight states have a stand-alone governance body or subcommittee tasked with addressing the cybersecurity of critical infrastructure systems. Three of those bodies focus specifically on energy or electricity.

Indiana

Originally established in 2016, Indiana Governor Eric Holcomb continued the **Indiana Executive Council on Cybersecurity (IECC)**[ii] in 2017 via executive order 17-11 to formulate a statewide collaborative effort involving government, private sector, military and academia to enhance Indiana's cybersecurity posture. The IECC is composed of 20 committees and working groups tasked with "developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure."[ii] As of early 2021, the IECC has completed 80 percent of its outlined deliverables.

The Energy Committee, one of the 20 IECC subcommittees, is composed of Indiana energy utilities, the Midcontinent Independent System Operator (MISO), the Indiana Energy Association, and state entities with energy or environmental responsibilities. The Energy Committee executed a variety of tasks to improve the cybersecurity posture of the Indiana energy sector. One, the committee developed a critical contact database that identified energy companies in Indiana, their form of ownership, cybersecurity contacts, and how they manage cybersecurity. That information was turned over to the Indiana Utility Regulatory Commissions Emergency Support Function lead to ensure that the Indiana Public Utility Commission (PUC) has appropriate cybersecurity contact information in the event of a cyberattack. More than 85 percent of Indiana utilities were able to provide this valuable information. Second, the Energy Committee was able to use the information in the database to develop an annual survey for the utility energy industry to assess cybersecurity planning, preparedness, and recovery posture. Every Indiana utility had completed the survey by June 2018. The survey helps the Energy Committee assess the overall risk to the state of Indiana regarding energy utility operations[iii].

Third, the Energy Committee worked to formalize strategic cybersecurity partnerships across the public and private sectors. The Energy Committee began continuously sharing information and risks with the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The Energy Committee also recommended that all critical infrastructure sectors in Indiana utilize existing networks, like the E-SIAC and MS-ISAC, to advance cybersecurity throughout the state. Energy Committee members believe all participants will benefit from timely intelligence if coordination is done correctly.

The larger IECC also created a Cybersecurity Scorecard to help companies and businesses across the state assess their cybersecurity posture. It is meant to be approachable and does not require deep cybersecurity knowledge. The scorecard aligns with the 20 National Institute of Standards and Technology (NIST) Cybersecurity Framework controls. When companies complete the scorecard, they can receive follow-up guidance that lists simple steps they can take to improve their cybersecurity posture. The IECC tested the scorecard with several small municipal utilities, electric cooperatives, and MISO. Several of those entities were able to use the survey results to address deficiencies in their cybersecurity practices.

The IECC's Emergency Services and Exercise Working Group also works with the energy industry to assist in the event of a large-scale emergency. Their committee created a Cyber Response Toolkit used to help local emergency managers gauge the cyber preparedness of critical infrastructure in their jurisdiction. This survey is meant to begin conversations among an emergency manager and their local government partners as well as provide a collective overview of the emergency

manager's area through a risk profile using the information provided. This will help emergency managers be better informed as to what they should be focusing on when planning for a cyberattack.

Washington

The **Washington State Energy Coordinating Council (ECC)** formed in 2011, was active for several years and spurred a number of initiatives that continue to help Washington lead in energy-sector cybersecurity. The ECC was a part of the Infrastructure Protection Subcommittee of the Washington Committee on Homeland Security tasked with determining how to protect critical energy infrastructure in the state. The ECC was composed of representatives from electric and natural gas utilities and petroleum product suppliers as well as representatives from the Washington Utilities & Transportation Commission (UTC) and Department of Commerce. The ECC authored the *Washington State Sector Specific Plan for Critical Energy Infrastructure* which "establish[ed] a comprehensive plan that, when implemented, ensures that critical energy infrastructure in Washington state, or in nearby states and provinces that Washington depends on, is identified and appropriately protected." [1] One of the six goals identified in the plan is to "use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resilience."[iv]

One example initiative spurred by the ECC was a collaboration between the Cyber Team of the Washington National Guard and the Snohomish County Public Utility District (PUD) -- the second largest publicly owned utility in Washington -- conducting exercises to test for cyber vulnerabilities in 2015[v]. The Washington National Guard conducted penetration tests on the PUD network, which had dual value: PUD was able to assess the security of their networks (which supports critical infrastructure) and the Washington National Guard was able to exercise their cyber team/practice penetration testing. Those exercises led to a collaborative effort to create the *Cybersecurity Guide for the Critical Infrastructure of Washington State*, spearheaded by the National Guard, PUD, the UTC, the Washington State Emergency Management Division, State of Washington Office of the Chief Information Officer, and the Pacific Northwest National Laboratory. Efforts to identify cyber vulnerabilities through exercises continue today. In June 2020, PUD announced a new partnership with the Washington National Guard to pilot a critical infrastructure cybersecurity partnership program. The program aims to increase cybersecurity awareness in support of local government entities, including providing cybersecurity assessments and customized recommendations to remediate any vulnerabilities or risks identified.[vi]

Texas

While the **Texas Cybersecurity Council** does not have a critical infrastructure subcommittee, the Governor signed legislation creating the **Texas Electric Grid Security Council** and an **Energy Cybersecurity Monitor Program** in 2019 to mitigate the risk of cyber and physical attacks that may affect the reliability of electric systems in Texas. The Texas Electric Grid Security Council is composed of three members: the chairman of the public utility commission, president of ERCOT (Electric Reliability Council of Texas), and a representative appointed by the Governor. The council will create and disseminate grid security best practices, revise the state emergency plan to ensure coordinated restoration efforts, and prepare for grid-related security threats. The monitor will manage a comprehensive cybersecurity outreach program, and gather and disseminate best practices around electricity cybersecurity, review voluntary utility cybersecurity self-assessments, and report to the PUC about the cybersecurity preparedness level of the electric utility industry. Investor-owned, municipally owned, and electric cooperative utilities inside and outside of ERCOT may elect to participate in the Texas Cybersecurity Monitor Program. A total of 155 entities participated in the program in 2020.[vii]

The five remaining states formed governance bodies focused broadly on critical infrastructure, including the energy sector.

Missouri

The commissioner of the state of Missouri's Office of Administration, with support from then-Governor Jay Nixon, created a short-term governance body to study how to improve cybersecurity in Missouri. The **Missouri Cybersecurity Task Force**, formed in 2016, made recommendations focused around five pillars, with one dedicated to hardening critical infrastructure. The task force conducted an assessment using NIST 800-30, a guide from the National Institute of Standards and Technology created to help conduct risk assessments, to determine risk on four publicly and independently owned utility systems. The body identified that utilities were not able to quickly obtain critical threat reports. To resolve this shortcoming, the group encouraged state fusion centers to create public-private partnerships to facilitate faster information sharing[viii]. Timely communication enables utilities to execute meaningful action in the event of a cyberattack. After the task force issued its recommendations, Berkshire Hathaway Energy started an ongoing partnership with the Kansas City Regional Fusion Center to share threat information.

Iowa

The Iowa Legislature created the **Iowa Energy Center Board** to govern and provide direction concerning programs, policies, and procedures of the Iowa Energy Center (IEC). Board members are appointed by the Governor, and representation includes but is not limited to the economic development authority, the Iowa Association of Municipal Utilities, the Iowa Utilities Board, and representatives from investor-owned utilities. The Iowa Energy Center also supports cybersecurity preparedness at the state's rural utilities, among other objectives. Although the governing body does not address cybersecurity more broadly, it bolsters collaboration among state officials, higher education, and utility representatives to synchronize risk management activities, emergency response preparedness efforts, and cybersecurity. The IEC also provided competitive grant funds to the Iowa Association of Electric Cooperatives (IAEC) to strengthen cybersecurity preparedness. The IAEC used the funds to increase coordination between cooperatives and implement/facilitate two of the cybersecurity programs developed by the National Rural Electric Cooperative Association (NRECA). The first program was an online cybersecurity assessment of each participating individual Iowa rural electric cooperative (REC). The assessment was used to help identify cyber or physical critical electric infrastructure vulnerabilities. The second program involved executing a cybersecurity tabletop exercise at each participating Iowa REC. The cybersecurity tabletop exercise provided an opportunity to test an Iowa REC's ability to assess and respond to a potentially damaging cyber incident. Both programs were used to create remediation plans to improve a cooperative's cybersecurity posture.

Louisiana

The cyber governing bodies of Louisiana, Maryland and South Carolina are standing bodies meant to constantly assess state cybersecurity posture and recommend how to improve it. The **Louisiana Cybersecurity Commission**, established by Governor John Bel Edwards through Executive Order 17-31 in 2017,[ix] addresses critical infrastructure through its Cyber Risk, Assets, and Capabilities Assessment Subcommittee. The subcommittee developed a risk management plan to adequately protect the state's critical infrastructure. This framework has helped Louisiana to identify and characterize the cyber risk landscape of the 16 critical infrastructure sectors in the state. The creation of a risk profile for each sector enables the state to appropriately allocate resources to address the highest threats based upon potential impact.

Maryland

The **Maryland Cybersecurity Council**[x] was established in 2015 at the recommendation of a previous short-term cybersecurity commission, **the Maryland Commission on Cybersecurity Innovation and Excellence**. The council was subsequently reaffirmed by the Maryland General Assembly in 2018. The council has a Subcommittee on Critical Infrastructure and Cybersecurity, composed of members from the legislature, higher education, the National Guard, NIST, the Maryland Fusion Center and members of the private sector[xi]. The subcommittee created a repository of cybersecurity resources and has made several recommendations to be considered by the larger council[xi]. The council has plans for dedicated outreach to the utility sector but that has been delayed due to COVID-19.[xii]

South Carolina

South Carolina addresses critical infrastructure through an independent body called the South Carolina Critical Infrastructure Cybersecurity Executive Oversight Group. The group was established in 2017 via Executive Order 2017-08 and is tasked with preventing cyber threats, incidents or attacks affecting the state's critical infrastructure and key resources. The Executive Oversight Group is made up of six individuals from state government and the Governor's office and includes a private sector advisory panel of four individuals from rotating critical infrastructure sectors. One salient accomplishment of the formal working group was the construction of the South Carolina Critical Infrastructure Cybersecurity program which oversees the Cyber Liaison Officer program. The intent of the Cyber Liaison Officer program is to create multiple mechanisms for the rapid distribution of actionable cyber intelligence.[xiii] There are currently 105 cyber liaison officers representing all the critical infrastructure sectors in the state including the energy sector. The cyber liaisons keep in regular contact with critical infrastructure owners and operators and develop trusting relationships. These relationships make it easier to share information in steady state and during a cyberattack.

Additional State Examples

In addition to the eight states NGA studied that have a dedicated body or subcommittee focused on critical infrastructure, six states (DE, IA, IL, MA, NY and WV) referenced critical infrastructure in the mission of their cybersecurity governing body. For example, the Delaware Cyber Security Advisory Council's mission states that it will "facilitate cross-industry collaboration to share best practices and mitigate cyber security risks related to critical infrastructure and protected systems." Seven states (AZ, DE, KS, NH, NV, RI and VT) included critical infrastructure agencies or companies as members of the state's cybersecurity body. For example, the Rhode

Island Cybersecurity Commission includes two utility company representatives, the Rhode Island National Guard, and representatives from the Rhode Island Emergency Management Agency.

The table below highlights common characteristics of the eight state critical infrastructure cybersecurity governance bodies NGA has highlighted in this report.

Governors may want to consider the below practices when they are expanding or creating a governance body to focus on critical infrastructure cybersecurity:

- Include critical infrastructure agencies and owners/operators on the board;
- If the body is in perpetuity, regularly conduct environment surveys and analyze trends related to the cyber posture of the critical infrastructure landscape to stay abreast of the latest threats;
- Collect and share best practices with critical infrastructure owners and operators in the state;
- Consider reviewing emergency response or business continuity plans for utility companies;
- Consider interdependencies among critical infrastructure sectors; and
- Consider interdependencies between neighboring states or countries.

Table: Characteristics of Critical Infrastructure Bodies or Subcommittees

State	Body Type and Status	# of members	Task (report, recommendations)	Established via
Indiana	Council 2016 – present	250	Develop strategic plans and implement them to improve the state's cybersecurity posture, maintain a strategic framework, identify sources and methods for accomplishing recommendations	Executive Order
Iowa	Review Board 2017 – present	13	Recommends policy guidance for program implementation to the IEC	Legislation
Louisiana	Commission 2017 – present	17	Improve information sharing, encourage cyber assessments, improve critical infrastructure resiliency, create a strategic framework	Executive Order

State	Body Type and Status	# of members	Task (report, recommendations)	Established via
Maryland	Council 2015 – present	30	Report/recommend policy guidance and/or goals	Legislation
Missouri	Task Force 2016	27	Recommend policy guidance, and/or goals on improving the state's cybersecurity posture	Agency Action
South Carolina	Working Group 2015 – 2017	6[xiv]	Improve the ability to and/or identify and detect threats, improve information sharing	Executive Order[xv]
Texas	Security Council 2019 **-** present	3	Facilitate collaboration, identify/disseminate security best practices for the energy sector	Legislation
Washington	Council 2011 – 2015[xvi]	17	Report/recommend security best practices for the CIKR sector	

Authors

This publication was developed by Alyse Taylor-Anyikire and Khristal Thomas with the National Governors Association Center for Best Practices (NGA Center).

Acknowledgements

The NGA Center would like to thank the state officials who granted informational interviews, reviewed drafts of recommendations and promising practices and provided a sounding board for the authors:

- Chetrice L. Mosley-Romero, Indiana Department of Homeland Security
- Brian Sellinger, Iowa Economic Development Authority
- Bruce Smalley, South Carolina Law Enforcement Division
- Michael Furze, Washington State Department of Commerce

Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000817.

represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Unite d States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

---

[i] "What Is Critical Infrastructure?" Department of Homeland Security, accessed December 7, 2017, https://www.dhs.gov/what-critical-infrastructure.

[ii] Indiana's Executive Council on Cybersecurity, "Indiana Cybersecurity Strategic Plan," State of Indiana, 2018.

[iii] C. Mosley, Interviewee, *Cybersecurity Program Director - Indiana Office of Technology.* [Interview]. February 2021.

[iv] Washington State Energy Coordinating Council, "Washington State Sector Specific Plan for Critical Energy Infrastructure," State of Washington, 2011.

[v] Cybersecurity Insiders . "Snohomish County PUD and the Washington State National Guard." *Cybersecurity Excellence Awards*, 9 Aug. 2016, cybersecurity-excellence-awards.com/candidates/snohomish-county-pud-and-the-washington-state-national-guard/.

[vi] Snohomish County Public Utility District No. 1. "PUD Partners With the Washington National Guard." Latest Buzz | PR, Snohomish County Public Utility District No. 1, 30 June 2020, www.snopud.com/newsroom.ashx?p=1102&173_list=archived&173_na=412.

[vii] https://interchange.puc.texas.gov/Documents/49819_25_1088822.PDF

[viii] State of Missouri Cybersecurity Task Force, "Cybersecurity Task Force Action Plan," State of Missouri, 2016.

[ix] LA Executive Order 17-31, 2017. https://lacybercommission.la.gov/wp-content/uploads/2018/07/Governors-Louisiana-Cybersecurity-Commission-Executive-Order-17-31.pdf

[x] Updated Council Membership from 2018 Maryland Senate Bill 281 https://www.umgc.edu/documents/upload/senate-bill-281.pdf

[xi] Maryland Cybersecurity Council, "Maryland Cybersecurity Council Activities Report 2017-2019," The State of Maryland, 2019.

[xii] https://www.umgc.edu/documents/upload/draft-meeting-minutes-for-october-14-2020-2.pdf

[xiii] SC Executive Order 2017-09, https://www.scstatehouse.gov/Archives/ExecutiveOrders/exor2017-08.pdf

[xiv] Five members are specified in the EO but additional ad hoc members may be added at the discretion of the Cyber Executive https://www.scstatehouse.gov/Archives/ExecutiveOrders/exor2017-08.pdf

[xv] The South Carolina Working Group was intended to be a short-term body to "document a strategic framework to … develop, implement, and maintain a comprehensive program and operational effort to evaluate and enhance the State's [critical infrastructure and key resources] cybersecurity posture." The plan is being carried out by the South Carolina Office of Homeland Security and fusion center.

[xvi] The ECC is no longer active but efforts they spurred continue throughout the state of Washington such as the National Guard working with the utility sector to address cybersecurity vulnerabilities.