National Governors Association

NGA PAPER

State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure

Executive Summary

Protecting the nation's energy system and infrastructure from cyber threats is of vital importance to governors, and the risks appear to be growing. Those threats have joined long-standing ones from natural disasters and physical attacks.[1] Cyber threats to the energy sector include intrusions into utility business systems to obtain sensitive information and strikes on control systems that could damage physical energy infrastructure and cause a disruption in the electric, oil, or gas supply. An attack on energy infrastructure also is likely to affect other critical infrastructure sectors, such as water, transportation, emergency services, and government operations. Electric utilities and other energy providers have begun reporting more frequent attacks on business and operational control systems, and recent attacks and tests have shown that an attack from cyberspace could damage or disrupt energy infrastructure. Recent studies estimate that the electric power industry will need to spend more than $7 billion by 2020 to protect the grid from cyber attacks; the oil and natural gas industry will need to spend nearly $2 billion by 2018.

Governors face several challenges in protecting critical energy assets from cyber threats and adequately responding to disruptions caused by a cyber attack. They include limited state-level experience with cyber-related response and recovery activities in general, limited understanding of the threats and risks associated with cyber attacks on the energy system, and an energy system that is interstate and interdependent with other critical infrastructure networks. Governors can confront those challenges and enhance the cybersecurity of the energy infrastructure within their state through the following actions:

- ***Adapt existing response, recovery, and resilience measures for natural disasters to cybersecurity.*** Governors can extend current approaches for preparing for and responding to natural disasters to cover cyber attacks. For instance, governors can emphasize cybersecurity in state energy assurance planning and develop cybersecurity capabilities in their state National Guard units. **Colorado** incorporated cyber risks into its energy assurance plan with recommendations for further possible state action; **Washington** is one of several states whose National Guard created units specifically devoted to cyber threats.

- ***Set specific roles and responsibilities for agencies that interact with the energy sector.*** Governors can make sure energy assurance plans and other cybersecurity efforts reflect best practices, are understood by responsible state agencies, and include clearly defined roles and responsibilities for state agencies. **Oregon** has delineated clear roles for nine state agencies, along with federal and private partners, in its energy assurance plan, with the lead agency determined by the severity of the consequences.

- ***Promote a risk-based approach to cybersecurity among utilities that adapts to evolving threats.*** Governors can promote practices among their utilities that build on standards and guidelines to address unique threats and vulnerabilities. They also can ensure that state agencies, including

[1] This issue brief focuses on cyber threats but recognizes that physical attacks on energy systems and infrastructure continue to pose significant risks.

public utility commissions, have a thorough understanding of how utilities manage risks. **Connecticut** developed a report on the status of the cybersecurity of the state's utilities that recommends using a cyber audit program to increase the state's understanding of utility risk management practices and inform any potential regulatory action.

- ***Convene state and regional players for planning, exercises, and information sharing.*** Governors are uniquely positioned to bring together agencies and entities to address the interstate, state-federal, and public-private nature of energy sector cybersecurity. Governors can convene state agencies that oversee critical infrastructure sectors to ensure that cybersecurity policies and plans are aligned and convene states in their region to address potential multi-state solutions and responses. Governors also can ensure state agencies are taking advantage of existing government-industry opportunities for information sharing and response. For example, **Michigan** created a multi-agency, public-private group to address cyber risks in several infrastructure sectors. Since March 2013, **Pennsylvania** has convened utility regulators from neighboring states on a quarterly basis to discuss energy-specific cyber threats and solutions.

Cybersecurity is an emerging responsibility for governors, and they have several tools readily available they can adapt, expand, or emphasize to address cyber threats. By working closely with the private owners and operators of energy infrastructure, governors can ensure energy networks are adequately protected and can better lead the response and recovery should a cyber attack occur.

Introduction

Protecting the energy system from a variety of threats—natural disasters, physical attacks, and cyber attacks—is of vital importance to governors and crucial to the nation's economy, security, and way of life. The system includes electric generation facilities, the electric power grid, oil and gas pipelines, and refineries. Elements of the energy system are interdependent, and the system as a whole is interdependent with other critical infrastructure sectors such as transportation, water, government, and telecommunications. Other sectors, such as emergency response and financial services, depend on it to function.

As with any sector of the economy that relies on digital infrastructure, the energy sector faces threats from cyberspace. For some electric utilities, cyber attacks have risen to the level of frequent or constant.[2] Most of those attacks focus on business systems, where utilities hold large amounts of personally identifiable information—for example, names, addresses, and credit card numbers. Advanced digital electric meters—deployed in nearly 40 percent of U.S. households and expected to reach 50 percent penetration by 2015—pose potential entry points for an attack and have attracted attention for their vulnerability.[3]

Although business systems have been the target of most attacks, the greatest cybersecurity risk to the energy sector is an attack on energy generation or delivery systems that causes a disruption in energy supply. Industrial control systems in power plants and pipelines, when integrated with digital, Internet-connected devices, are possible vectors for such an attack. Although they did not affect energy systems in the United States, the Aurora Test and Stuxnet virus demonstrated that cyber attacks on control systems can cause system failure and physical destruction.[4]

[2] House.gov, *Electric Grid Vulnerability: Industry Responses Reveal Security Gaps* http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf (accessed July 18, 2014).

[3] Innovation Electricity Efficiency, *Utility-Scale Smart Meter Deployments: A Foundation for Expanded Grid Benefits* (Washington, DC: IEE August

[4] NARUC.org, *Cybersecurity for State Regulators 2.0,* http://www.naruc.org/Grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf, p. 7 (accessed July 18, 2014). The Aurora Test was a staged cyber attack conducted at the Idaho National Laboratory that showed the possibility that a cyber attack on control systems could cause an electric power generator to self-destruct. The Stuxnet virus, discovered in June 2010, affected the control software in Iranian uranium enrichment centrifuges, causing them to spin beyond their intended speed and eventually fail while reporting normal operating conditions.

Cyber attacks designed to disrupt physical infrastructure appear to be on the rise. The U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported that it responded to 81 attacks against the energy sector between October 2011 and September 2012, the most of any sector.[5] In the following eight months, it had already responded to 111 attacks on the energy sector; during all of 2013, it responded to 151 energy sector incidents. During those same periods, attacks on the industrial control systems of the energy sector grew from 41 percent to 53 percent to 59 percent of all attacks warranting ICS-CERT response, while the next-highest sector (critical manufacturing) reported at most 20 percent of attacks.[6] That increase is caused by both a rise in the numbers of attacks and more frequent reporting of attacks to ICS-CERT.

In response to the variety of threats and vulnerabilities, federal and state governments and the energy industry have taken steps to enhance the cybersecurity of critical energy infrastructure. Those include creating standards and guidelines for the protection of critical assets, implementing methods to better manage risks, establishing information sharing networks, and adapting existing recovery and response capabilities for natural disasters. Governors can look to complement those efforts as they build cybersecurity capacity at the state level.

Challenges to Enhancing Cybersecurity for Energy Systems

Cybersecurity is an emerging concern for governors. Ensuring the security of the energy system requires states to recognize and overcome several challenges: a lack of experience with response and recovery activities for any cyber event, regardless of the affected sector; unfamiliar roles and responsibilities for addressing a cyber attack against the energy sector specifically; a lack of understanding of how private-sector energy companies manage cyber risks; and the added complexity and coordination demands related to the interstate and interdependent nature of the energy system and other critical infrastructure networks.

- ***Lack of experience with cyber-related response:*** Response and restoration activities for a cyber attack can be similar to those for a storm-related outage, but there also are important differences. Similarities include the need for quick response and recovery, the importance of clear roles and responsibilities, and a need for trusted networks to share information. Hurricanes and blizzards can be forecasted with some level of certainty, but cyber-related disruptions are largely unpredictable and could be repetitive in nature, of unknown duration, or concurrent with another attack or disruption.[7] In addition, the source of threats to the energy system might not be apparent initially, requiring an additional role for law enforcement in determining the source of the attack. That underscores the need for planning and preparation specific to addressing cyber threats.

- ***Unclear roles and responsibilities:*** Addressing cyber threats in the energy sector requires the involvement of multiple participants across the state, including governors, emergency managers, law enforcement officers, homeland security of-

[5] ICS-CERT focuses on attacks specific to industrial control systems across a variety of critical infrastructure sectors. Other sectors include critical manufacturing, communications, commercial facilities, water, transportation, postal and shipping, nuclear, information technology, public health, and government facilities.

[6] *ICS-CERT Monitor April/May/June 2013*, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf (accessed July 18, 2014); and *ICS CERT Monitor October/November/December 2013,* https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf (accessed July 18, 2014).

[7] Cyber attacks are not the only threats that could damage or destroy physical energy infrastructure. The 2013 shooting at the Metcalf substation in California is an example of a physical attack (also referred to as a kinetic attack) on the energy system. Another possible threat is an intentional release of an electromagnetic pulse by a malicious actor. It is also possible that a cyber attack could take place during a hurricane or other natural disaster when the energy system is already more vulnerable to disruption and the source of the attack could be disguised.

ficials, utility commissioners, and energy officials. Because of the emerging nature of cyber threats, states might not have delineated the role for each participant.

- ***Lack of understanding of risks:*** Because the cost of some utility cybersecurity measures could be passed on to customers, states have a role in determining whether utility cybersecurity measures are adequate and cost-effective and sufficiently incorporate risk management. However, state officials have limited expertise to make those determinations, particularly for risk management.

- ***Interstate and interdependence of critical infrastructure:*** Many of the energy systems vulnerable to cyber threats extend beyond state borders and are linked to other critical infrastructure networks. Critical infrastructure owners and operators work within a regulatory authority split between state and federal government for both the electric power grid and oil and gas pipelines. In addition, owners and operators of energy infrastructure and state energy regulators need to collaborate and coordinate with owners and operators of other critical assets who depend on the energy sector or help keep energy systems functioning, such as water, transportation, and telecommunications.

State Strategies for Improving Energy Sector Cybersecurity

Governors have an important role in addressing disasters and disruptions to the energy system, including cyber threats. In 2012, the National Governors Association created a *Resource Center on State Cybersecurity* to examine the role of state policy in ensuring adequate cybersecurity and provide governors with recommendations to promote cybersecurity across different sectors, including energy.[8] In 2013, NGA released *Act and Adjust: A Call to Action for Governors for Cybersecurity.* The paper includes several short-term actions governors can take to improve the protection of state government-owned assets and networks.[9] Governors can build on the recommendations in the *Call to Action* to improve the cybersecurity of energy infrastructure in their state by leading planning and preparedness efforts, working with state utility commissions to ensure that the utilities that deliver energy are adequately protected (with or without specific regulations), and convene their colleagues in other states to address common challenges. Steps governors could take include:

- Adapt existing response, recovery, and resilience capacity for storms to cybersecurity;
- Set clear roles and responsibilities for agencies that interact with the energy sector;
- Promote a risk-based approach to cybersecurity by utilities that adapts to evolving threats; and
- Convene state and regional players for planning, exercises, and information sharing.

Adapt Existing Response, Recovery, and Resilience Capacity for Natural Disasters to Cybersecurity

States have considerable experience managing efforts to help the owners and operators of energy infrastructure restore service quickly and safely following natural disasters. As discussed above, several elements of the response to disruptions in energy supply would be the same regardless of the cause. Governors can use or adapt various resources already in place, including energy assurance plans and the National Guard, to respond to and recover from cyber incidents in the energy sector.

Further Incorporating Cybersecurity into Energy Assurance Planning

Planning for energy disruptions is critical for states and critical infrastructure operators to be able

[8] NGA.org, "Governors O'Malley and Snyder to Lead NGA Resource Center on Cybersecurity," http://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html (accessed July 18, 2014).

[9] NGA.org, *Act and Adjust: A Call to Action for Governors for Cybersecurity,* http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf (accessed July 18, 2014).

to respond and recover quickly. Under the 2009 American Recovery and Reinvestment Act, the U.S. Department of Energy (DOE) granted states funding to develop detailed energy assurance plans to prepare for energy emergencies. DOE required that states explore cybersecurity as an element of those plans. As a result, states have included sections or appendices within their plans that address cybersecurity vulnerabilities and risks. Governors, who oversee the executive branch agencies that have written most of those plans, can make sure that their state's energy assurance plans consider cybersecurity issues. The **Colorado** Energy Assurance Emergency Plan (developed by the Colorado Energy Office, Public Utilities Commission, and Division of Emergency Management, now the Division of Homeland Security and Emergency Management) assesses the risks and vulnerabilities associated with a cyber attack on the state's energy system. The plan explores the consequences of cyber crime targeting personal and billing information and a terrorist or similar malicious attack designed to disrupt energy supplies. It also identifies forums for information sharing in the energy sector that exist but may need expansion. It includes recommendations for state action, including monitoring federal legislation, participating in a cybersecurity working group with a focus on the energy sector, and building capacity through training.[10]

Having a plan in place is necessary but is not enough; a successful response requires that plans be tested through exercises. Governors can support participation in emergency exercises to improve response and recovery procedures. Taking part in the exercises helps ensure that state energy assurance plans align with other state, federal, and utility response plans and are understood by the agencies that carry them out. Those exercises should test the alignment between state plans and federal response strategies such as the National Infrastructure Protection Plan, National Cyber Incident Response Plan, and National Response Framework. They also should include coordinating with local utilities or other infrastructure operators so that state officials can build relationships prior to a disaster and better understand the steps utilities take in responding to disruptions, including activating the mutual assistance network (see box). Exercises help states test response and recovery plans for all types of

Utility Mutual Assistance Network

The electric utility industry has a formal but voluntary program to provide support during emergencies affecting the electric power grid. The mutual assistance network is a partnership among utilities in which crews from states or regions unaffected by a disaster provide relief to affected utilities in the form of line crews, damage assessors, and specialized equipment. The network is coordinated regionally, but crews may travel beyond their neighboring states. For example, during Superstorm Sandy in 2012 crews and equipment from across the country were mobilized to the Northeast to help. Utilities view the mutual assistance network as a vital tool in response and restoration that may also be used in case of a cyber attack, although they may need to deploy different resources and expertise for a cyber-related response.

[10] Colorado.gov, *Colorado Energy Assurance Emergency Plan,* http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22Energy+Assurance+Report.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251826394416&ssbinary=true (accessed July 22, 2014).

energy system disruptions; governors need to ensure that exercises test elements that cover a cyber incident.

Promoting and Developing Cyber Capabilities within the National Guard

The National Guard is an important part of states' efforts to respond to and recover from a variety of disasters. Guard units across the country are beginning to provide support for cyber-related threats and disasters. **Washington** developed a cybersecurity team within its National Guard force in 2012, taking advantage of the private-sector cybersecurity and information technology experience of its citizen-soldiers. The Washington Guard is partnering with state agencies to help with threat detection and prevention, in addition to its traditional recovery and response roles. Other states with National Guard units dedicated to cybersecurity include **Delaware, Maryland, Missouri, Rhode Island**, and **Utah**.[11] In July 2014, the Council of Governors and the U.S. Departments of Defense and Homeland Security agreed to a joint action plan for cybersecurity that commits the parties to work together to protect the U.S. from cyber threats and establishes a framework for the National Guard's role in cybersecurity.[12]

Set Roles and Responsibilities for Agencies that Interact with the Energy Sector

The state agencies that have a role in enhancing the cybersecurity of the energy sector should include those with expertise in homeland security and public safety, information technology, and energy policy. Governors have the executive authority to define the roles and responsibilities for each agency.

Governors can use their state energy assurance plan or a similar plan to designate lead and support agencies for dealing with a cyber incident. That should include naming a single point-of-contact agency for state-federal or government-industry communication. **Oregon's** state energy assurance plan outlines the roles and responsibilities of state agencies in responding to disruptions of increasing severity for both the electric and oil and gas sectors. Notably, the lead agency remains the same as the severity of the incident increases, but the agencies designated to provide support may change, taking into account the risks and consequences of more widespread or long-term disruptions. For example, the Oregon Public Utilities Commission is designated as the lead agency for both electric and natural gas disruptions, with support from the Oregon Department of Energy and Office of Emergency Management for basic outages. As the length or scale of the outage increases, agencies such as the state's department of transportation, military department, civil air patrol, and department of human resources are designated to support the response, and the governor's office is specifically identified as having responsibilities in an escalating or severe energy emergency.[13]

Governors also can galvanize efforts at state agencies to address cybersecurity issues in critical infrastructure sectors. **Maryland** Governor Martin O'Malley updated the state's Strategic Goals and Objectives for Homeland Security so that the critical infrastructure goal includes a framework for actions the state can take to protect critical infrastructure from cyber attacks. Governor O'Malley also designated a director of cybersecurity in 2013 to oversee statewide cybersecurity and ensure coordination of state agency planning.[14] As part of his 2013 State of the State address, **New York** Governor Andrew Cuomo launched a cybersecurity initiative that

---

[11] Pewtrusts.org, *Stateline,* "The National Guard Takes on Hackers," http://www.pewstates.org/projects/stateline/headlines/the-national-guard-takes-on-hackers-85899535957 (accessed July 18, 2014).

[12] Nga.org, "Cybersecurity a Top Priority for Governors," http://www.nga.org/cms/home/news-room/news-releases/2014--news-releases/col2-content/cybersecurity-a-top-priority-for.html (accessed July 22, 2014).
The Council of Governors is a bipartisan group of 10 governors, appointed by the President, that meet with the Secretaries of Defense and Homeland Security to address matters pertaining to the National Guard, homeland defense and defense support to civil authorities. (http://nga.org/cms/CoG)

[13] Oregon.gov, *Overview of Energy Sector-Specific Emergency Response Plans,* http://www.oregon.gov/energy/docs/Oregon%20State%20Energy%20Assurance%20Plan%202012-Ch6.pdf (accessed July 18, 2014).

[14] Gohs.Maryland.gov, "Cyber Security and Critical Infrastructure Protection," http://gohs.maryland.gov/va_accomplishments.html (accessed July 18, 2014).

created a governor's Cybersecurity Advisory Board and called for the physical co-location of the state's intelligence center with the Multi-State Information Sharing and Analysis Center (MS-ISAC).[15] That created a combined physical and cybersecurity operations center to more efficiently protect critical infrastructure networks, including energy systems.[16] The operations center allows state and federal agencies to more easily share threat information and work cooperatively to address threats to critical infrastructure.

Promote a Risk-Based Approach to Cybersecurity among Utilities that Adapts to Evolving Threats

State-level cybersecurity plans should combine standards-based and risk-based approaches. Standards help ensure that private entities are following industry best practices by providing a list of minimum protections or procedures (see box on page 8). In a risk-based approach to cybersecurity, security measures are adopted based on consideration of known and potential threats, vulnerabilities, and consequences.

Governors should promote a policy among their utilities that best addresses risks unique to each segment of the energy sector and builds on any new or existing standards. Governors also should ensure that state agencies that interact with the private sector understand the strategies companies use to manage risks.

The National Association of Regulatory Utility Commissioners released a cybersecurity primer in 2011, updated in 2013, which introduces state utility regulators to key topics in energy sector cybersecurity. That document synthesizes issues for state regulators and provides a list of questions they should ask utilities to help the state build capacity and understand utility investment, particularly involving risk management.[17] Those questions also can help governor's staff and other state officials become more familiar with utility risk management strategies.

Because governors and state utility commissions are still working to understand the risks and protections associated with energy sector cybersecurity, few states have taken regulatory action. States are beginning to explore regulatory actions that do not duplicate existing efforts or ignore the changing nature of cyber threats. Those actions are still being developed, and so their effectiveness and relative cost are not yet known. **Connecticut's** state Comprehensive Energy Strategy, which Governor Dannel Malloy signed in 2013, directed the Public Utilities Regulatory Authority (PURA) to report on the security of the state's regulated utilities and provide recommendations to the governor on how to increase defense against cyber attacks. PURA released its report in April 2014, after consultation with each of the state's utilities. Although the report discusses the possible adoption of state-based cybersecurity standards, the report's main recommendation calls for the state to set up a cyber audit program to determine if the utilities are not only meeting standards but also adequately assessing risks, addressing evolving threats, and incorporating best practices.[18]

State efforts to understand energy sector cyber risks also should be coordinated with ongoing federal plans to promote risk-based approaches to cybersecurity. DOE has created cybersecurity capability maturity models (C2M2) to help utilities assess their cyber capabilities and prioritize the actions needed to protect their networks using a risk-based approach. The C2M2 combines information from existing efforts to develop a common tool to be used across the industry. A C2M2 for the electric subsector was released in 2012, and DOE is currently working on a C2M2 for the oil and gas subsector. States should determine whether their utilities are using the C2M2 or another approach to cyber risk management.

---

[15] The ISACs are discussed in further detail on Page 9.

[16] Governor.NY.gov, *NY Rising*, http://www.governor.ny.gov/sites/default/themes/governor/sos2013/2013SOSBook.pdf (accessed July 18, 2014).

[17] Naruc.org, *Cybersecurity for State Regulators.*

[18] CT.gov, *Cybersecurity and Connecticut's Public Utilities,* http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf (accessed July 18, 2014).

Cybersecurity Standards in the Energy Sector

Although risk management strategies, which weigh threats, vulnerabilities, and consequences, are a critical component of energy sector cybersecurity, compliance-based standards have a role in protecting energy systems as well. Several such standards already exist, as described below.

Electric power grid: The electric power subsector is the only critical infrastructure sector with mandatory, enforceable standards for cybersecurity. The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards address cyber and physical security for utilities in the wholesale electricity market. The CIP standards include requirements for asset identification, systems security management, physical security of critical cyber assets, incident reporting and response, and recovery planning. NERC's first CIP standards covering cybersecurity became effective in 2006, and implementation of Version 5 is underway.

In the electric distribution system, the National Institute of Standards and Technology has developed guidelines for cybersecurity of "smart grid" devices such as advanced electric meters and electric distribution automation equipment.

Oil and natural gas: Federal and industry guidelines and voluntary standards have been adopted throughout the oil and gas industry. The Transportation Security Administration, the American Petroleum Institute, and the Interstate Natural Gas Association of America have guidelines for oil and gas utilities and pipeline operators.

Commercial nuclear reactors: The U.S. Nuclear Regulatory Commission requires companies operating nuclear power plants to have cybersecurity plans and protocols in place. Those requirements build off of a previous voluntary industry-led strategy to enhance cybersecurity that had been adopted across the industry.

In February 2014, the National Institute of Standards and Technology released the first version of *Framework for Improving Critical Infrastructure Cybersecurity* as a new tool for owners and operators of critical infrastructure, such as the energy sector, to manage cyber risks. The document was a collaboration between government and industry that compiles existing standards and practices.[19]

How utilities and other entities in the energy sector understand and manage risks is directly linked to the cost of cybersecurity. Recent estimates place the cost of protecting the electric power grid from cyber threats at more than $7 billion by 2020, with the price tag for oil and gas cybersecurity reaching nearly $2 billion by 2018.[20] For most electric and natural gas utilities,

[19] NIST.gov, *Framework for Improving Critical Infrastructure Cybersecurity,* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (accessed July 18, 2014).

[20] Bipartisan Policy Center, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,* http://bipartisanpolicy.org/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf (accessed July 22, 2014); and *Pipeline,* http://www.pipelineme.com/news/regional-news/2013/01/oil-and-gas-cyber-security-to-cost-$187bn-by-2018/ (accessed July 18, 2014).

state utility commissions determine if and how those costs are passed on to customers. For that reason, it is important that state utility regulators and others within the state understand the risks to their specific utilities and the energy system as a whole so that any measures adopted balance the direct cost to customers with the benefit of adequate cyber protection.

Convene State and Regional Players for Planning, Exercises, and Information Sharing

Events such as the 2003 Northeast blackout and Superstorm Sandy in 2012 showed how interruptions in energy supplies affect multiple states and cause serious disruptions in other critical infrastructure sectors. The effects of a cyber attack on the energy sector could be similar. Governors have an important role in creating a "line of sight" across state agencies, reaching out to private-sector companies at the executive level, and coordinating with their counterparts in neighboring states to align protection and response strategies.

Coordinating State Agencies across Infrastructure Sectors

Governors can bring together agencies with oversight of all critical infrastructure sectors within a state to coordinate protection and resiliency of interdependent sectors. As part of **Michigan** Governor Rick Snyder's Cybersecurity Initiative, the state developed the *Michigan Cyber Disruption Response Strategy*. The document was a collaboration by several state agencies and private-sector critical infrastructure owners and operators, including two energy companies.[21] Goals include improving the awareness of cyber threats among critical infrastructure sectors and generating coordinated plans, trainings, and risk assessments across sectors. The strategy also establishes a goal of conducting exercises on elements of the strategy at least once a year and regularly re-evaluating risk assessments so that each sector is similarly prepared for responding to a cyber-related disruption.

Supporting Government-Industry Collaboration

The owners and operators of energy infrastructure are communicating and sharing cyber threat information among themselves and with federal and state government. Governors should be aware of those channels, and use them to inform their efforts. Those forums include:

- ***Information sharing and analysis centers (ISACs)***: The U.S. Department of Homeland Security (DHS) has encouraged private owners of critical infrastructure to create and participate in ISACs to facilitate the receipt and analysis of threat information within their sector. NERC operates an ISAC for the electric sector, and the Nuclear Energy Institute functions as an ISAC for nuclear operators. DHS runs the Multi-State ISAC to facilitate federal-state and interstate information sharing.[22]

- ***Sector-specific coordinating councils****:* Related to the ISACs are sector coordinating councils, which serve as means for interaction between the federal government and sector-specific owners and operators of critical infrastructure. There are separate coordinating councils for the electric sector and oil and gas sector, and the electric sector council helps manage the electric sector ISAC. Both are supported by the U.S. Department of Energy in coordination with DHS.[23]

- ***Fusion centers****:* State-based fusion centers are centralized locations for the sharing of threat

---

[21] Michigan.gov, *Michigan Cyber Disruption Response Strategy,* http://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf (accessed July 18, 2014).

[22] ISACCouncil.org, http://www.isaccouncil.org/memberisacs.html (accessed July 18, 2014).

[23] DHS.gov, "Critical Infrastructure Sector Partnerships." http://www.dhs.gov/critical-infrastructure-sector-partnerships; andNERC.gov, http://www.nerc.com/pa/CI/Pages/ESCC.aspx (accessed July 18, 2014).

[24] DHS.gov, "State and Major Urban Area Fusion Centers," http://www.dhs.gov/state-and-major-urban-area-fusion-centers (accessed July 18, 2014).

information that bring together state and federal law enforcement and public- and private-sector partners. Fusion centers could be particularly helpful for utilities if a consequence of a cyber attack includes disruption to utility communication or situational awareness capabilities.[24]

- ***InfraGard****:* States also participate in InfraGard, regional public-private partnerships for information sharing and law enforcement activities involving cyber critical infrastructure, funded and managed nationally by the Federal Bureau of Investigation.[25]

Promoting Regional Coordination

Governors should encourage their state agencies to participate in multi-state discussions to address the interstate nature of energy sector cybersecurity and to create their own forum if a regional one does not exist. Public utility commissions in the mid-Atlantic (led by **Pennsylvania**, along with **Delaware**, **Maryland,** and **New Jersey**) regularly hold discussions on electric grid cybersecurity that included federal agencies, utilities, and the regional grid operator. They share unclassified threat information and discuss how they could jointly address a cyber attack with multi-state consequences.[26] The first discussion was held in March 2013, with meetings scheduled quarterly for the following year. The states are planning to gather again in September 2014 as part of a meeting of the Mid-Atlantic Conference of Regulatory Utilities Commissioners, where they hope to expand the discussion to include more states within the region.[27]

Conclusion

Although pipeline networks, power plants, and electric power lines are largely privately owned and operated, governors are at the forefront of addressing the consequences of a potential cyber attack on the energy system. Through proper risk management and coordination with the private sector, federal agencies, and neighboring states, governors can help ensure that the private energy networks are adequately protected from cyber threats while strengthening their ability to lead response and recovery planning.

Andrew Kambour
Senior Policy Analyst
Environment, Energy & Transportation Division
NGA Center for Best Practices
202-624-3628

August 2014

Recommended citation format: A.Kambour, *Enhancing the Cybersecurity of Energy Systems and Infrastructure* (Washington, D.C.: National Governors Association Center for Best Practices, August 4, 2014).

---

[24] DHS.gov, "State and Major Urban Area Fusion Centers," http://www.dhs.gov/state-and-major-urban-area-fusion-centers (accessed July 18, 2014).
[25] https://www.infragard.org/ (accessed July 18, 2014).
[26] PUC.PA.gov, "PUC Recognizes National Cybersecurity Awareness Month," http://www.puc.pa.gov/about_puc/press_releases.aspx?ShowPR=3248 (accessed July 18, 2014).
[27] Interview with Shelby A. Linton-Keddie, Counsel to Commissioner Pamela A. Witmer, Pennsylvania Public Utility Commission. May 27, 2014.