NATIONAL GOVERNORS ASSOCIATION

WHITE PAPER

Smart & Safe: State Strategies for Enhancing Cybersecurity in the Electric Sector

NATIONAL GOVERNORS ASSOCIATION
444 N. Capitol Street NW, Suite 267 | Washington, DC 20001 | 202.624.5300 | NGA.org

AUTHORS

Patricio Portillo
Policy Analyst

Dan Lauf
Program Director

Sue Gander
Division Director

NGA Solutions:
Energy, Infrastructure & Environment

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

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal li ability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or 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.

Executive Summary

Cyber-attacks have grown rapidly in the last few years and the energy sector has become a prime target for those attacks. In 2016, 20 percent of incidents reported to the U.S. Department of Homeland Security (DHS) targeted the energy sector.[1] Electricity is informally considered the most critical of the 16 critical infrastructure sectors designated by DHS; water, wastewater, communications, transportation and other parts of the energy sector all depend on reliable and secure electric power.[2] Because of these interdependencies, a successful cyber-attack on the electric system could have serious secondary effects: disrupting power or fuel supplies, damaging specialized equipment, and jeopardizing public welfare.

States are developing strategies for enhancing electric grid cybersecurity as they move toward a more modern, connected infrastructure. This white paper recommends seven actions for governors to consider in order to protect electricity infrastructure and personally identifiable information (PII):

- Define Roles and Responsibilities and Coordinate Efforts
- Incorporate Cybersecurity Roles and Responsibilities into Energy Assurance Planning
- Protect Sensitive Information
- Collaborate with Utility Regulators
- Participate in Cyber Response Exercises
- Leverage the National Guard and Civilian Workforce
- Conduct Risk Assessments

The paper also details roles and responsibilities for key state and industry stakeholders and catalogues important resources.

Introduction

Cyber-attacks have grown rapidly in the last few years and the energy sector has become a prime target for those attacks. Between 2010 and 2016, the number of incidents reported to the Department of Homeland Security Industrial Control Systems Cyber Emergency Respoonse Team (ICS-CERT) increased sixfold.[3] In 2016, the energy sector was the third-most targeted industry, accounting for 20 percent of reported incidents.[4] The consequences of a cyber-attack on the electricity system could be serious: disrupting power or fuel supplies, damaging specialized equipment, and jeopardizing public welfare.[5] As governors consider and implement policies to support grid modernization, strategies to enhance cybersecurity should be a primary concern.

Presidential Policy Directive 21 deems the energy sector and, by extension, electricity, "uniquely critical due to the enabling functions [it] provides across all critical infrastructure sectors."[6] Water, wastewater, communications, transportation and more rely on a reliable and secure supply of electric power. Because of these interdependencies, a successful cyber-attack on the electric system could have devastating cascading effects.

According to the Council of Economic Advisors (CEA) "a cyberattack on the electrical grid could have large-scale economic impacts as infrastructure damages, loss in output, delayed production, spoiled inventory, and loss of wages all decrease productivity and earnings for the duration of the blackout."[7] The CEA adds that expansive or sustained power outages likely would impact heating and cooling systems, slow emergency response times, overstretch police, disrupt clean water and sewage operations, impede the Department of Defense, and weaken trust in government.[8]

The National Governors Association recommends that governors consider the following seven strategies to inform the development of policies to protect electric infrastructure and PII from cyber incidents:

- Define State Agency Roles and Responsibilities and Coordinate Preparedness Efforts
- Incorporate Cybersecurity Roles and Responsibilities into Energy Security Planning
- Protect Sensitive Information to Encourage Strategic Information Sharing with the Private Sector
- Collaborate with Utility Regulators to Enhance their Cybersecurity Oversight
- Participate in Cyber Exercises to Practice Response, Strengthen Communication, and Identify Areas for Improvement
- Leverage and Expand the National Guard's and Civilian Workforce's Existing Cyber Expertise
- Conduct Risk Assessments of Electricity Infrastructure

Although the focus of this paper is on the electric system, some cybersecurity strategies and state examples also applicable to other aspects of the energy sector.

Cyber Strategies for Governors

Define State Agency Roles and Responsibilities and Coordinate Preparedness Efforts
Knowing who is responsible for what is paramount to effective planning and response. Governors are uniquely positioned to define roles and responsibilities and convene entities within their states to address the intergovernmental and cross-sector dimensions of electric grid security. The *Roles and Responsibilities of Key Parties* section below describes potential parties with whom governors should consider engaging. **Oregon** developed a comprehensive state energy assurance plan that coordinates nine state agencies and various federal and private partners to restore electricity, fuel and natural gas in the event of an emergency.[9] In this plan, responsibilities are clearly delineated -- for instance designating the Oregon Public Utilities Commission (PUC) as the lead agency during electric-system disruptions. Additional support agencies are enlisted as the risks and consequences increase.[10] With respect to cybersecurity, the Oregon PUC and the Office of Emergency Management are the primary agencies responsible for planning, preparedness, response and recovery from breaches.[11] In 2017, **Vermont** Governor Phil Scott issued an executive order that created a 10-member Governor's Cybersecurity Advisory Team to provide advice on the state's cybersecurity readiness, strategy and planning with members from the public and private sectors.[12] The cross-disciplinary team is charged with developing a strategic plan and enhancing the relationships and lines of communication across federal, state and local governments, as well as the private sector. The focus of this group is cybersecurity broadly, with members that include state information technology and homeland security leads alongside other state officials and academic experts. Underscoring the criticality of cybersecurity in the electric sector, Gov. Scott also appointed the CEO of the Vermont Electric Power Company to serve as an advisor.[13]

Governors also can facilitate private sector efforts by encouraging involvement in ongoing public sector information sharing and emergency response activities, such as those conducted through fusion centers. The nation's 79 fusion centers gather intelligence on threats, including cyber-attacks, and serve as conduits for information sharing among federal, state and local governments; private companies; and law enforcement.[14] Each state has at least one state-designated fusion center. The remaining 29 reside in major cities and three territories. These venues can serve as important forums for the secure sharing of threats and other information between utilities and states. Former **New Jersey** Governor Chris Christie, for example, established the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) to act as the state's clearinghouse for cybersecurity information sharing, threat intelligence, best practices and incident reporting.[15] The NJCCIC facilitates information sharing with public- and private-sector entities. Further, in accordance with a New Jersey Board of Public Utilities order, electric distribution companies are required to establish cybersecurity programs consistent with frameworks put forth by the National Institute of Standards and Technology (NIST), U.S. Department of Energy (DOE), and Information Systems Audit and Control Association and to report cybersecurity incidents to the NJCCIC.[16]

As governors delineate roles and work with the private sector, they also should be aware of changing federal authorities during a grid security emergency and the resulting impacts of potential emergency orders.[17] Under provisions of the Fixing America's Surface Transportation Act (FAST Act) of 2015, a presidential declaration of a Grid Security Emergency grants the Secretary of Energy emergency order authority to protect or restore the reliability of the electric grid from a physical or cyber-attack. This authority can include issuing waivers, obtaining special permits, providing access to classified information as needed, shielding entities from liability violations related to the Federal Power Act and FERC reliability standards, and other actions.[18] Presidential Policy Directive 8 (PPD-8) assigns the U.S. Department of Energy (DOE) as the lead to restore damaged energy systems from cyber incidents requiring a federal response[19] and PPD-41 directs DOE to assess business and operational impacts from a cyber incident on critical energy infrastructure.[20]

Governors should direct their staffs to integrate DOE's expanded authority in the event of a Grid Security Emergency into plans and documented roles and responsibilities. Further, governors should ensure that changing roles are tested through exercises (described later in this paper) so that the appropriate contacts are known and understood prior to an emergency occurring.

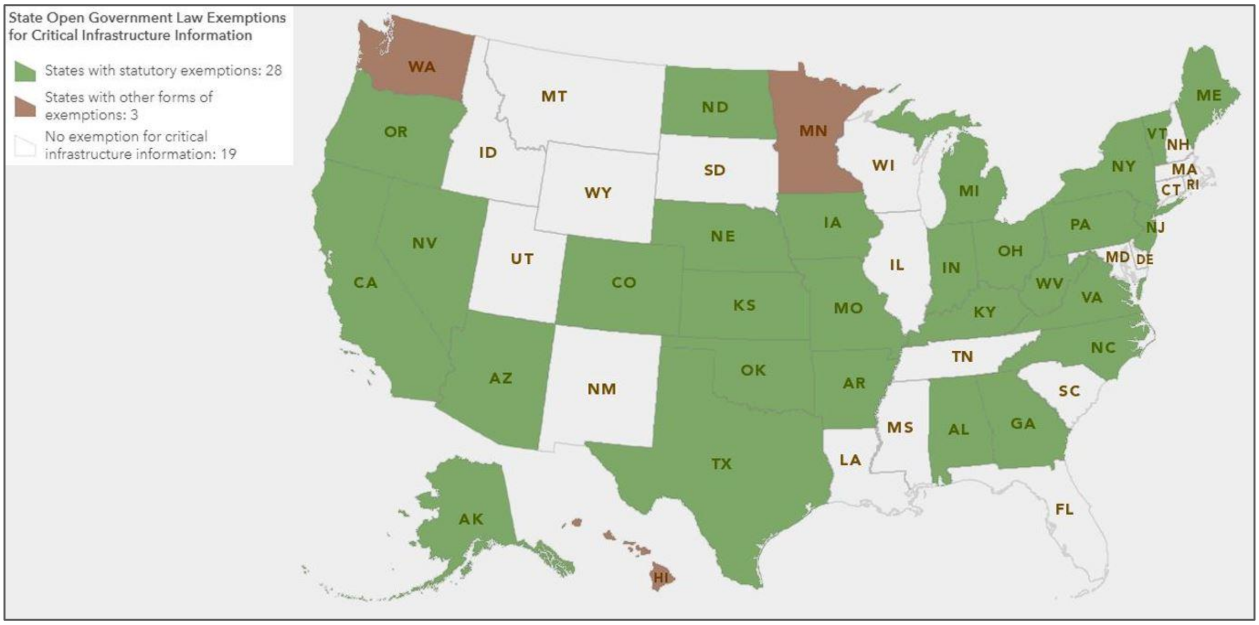
Incorporate Cybersecurity Roles and Responsibilities into Energy Assurance Planning

Energy assurance plans are important state resources that delineate how states can support a reliable, resilient energy supply. As governors seek to have their states develop or revise energy assurance plans, they should incorporate comprehensive strategies that address cybersecurity threats to energy supply and strategies to meet those threats.[21] This includes documenting and defining roles and responsibilities in coordination with utilities, other private and federal entities, and state agencies. In the past, most energy assurance plans did not address cybersecurity threats because they were not well understood. Recently, states have begun updating their plans to reflect this new threat. **Montana**, for example, has incorporated planning for cyber threats into its plan, whereby responsibility for responding to cyber threats is led by the utilities, with oversight and support from state and federal agencies.[22] In addition, the Montana Department of Justice operates the Montana All Threat Intelligence Center (MATIC) to facilitate cyber communication and threat response organization.[23] **Oklahoma**'s state energy assurance plan describes private-sector cybersecurity plans, activities and resources. Cybersecurity responsibilities are delineated, along with a discussion of response and communications strategies during and after a cyber event.[24] Other states that incorporate cybersecurity planning, practice and implementation into their energy assurance plans include **California, Louisiana** and **Connecticut**.[25]

Protect Sensitive Information -- Including Classified Threat Information – to Encourage Private Sector Information Sharing

Threat information sharing among public and private actors is critical to cyber threat detection, preparation and response. However, to facilitate information sharing, asset owners must be able to trust that sensitive information is securely managed, stored and protected from public disclosure. States may need to create additional protections or consider how to exempt sensitive electricity system data containing "engineering, vulnerability, or detailed design information" from public inquiry.[26] This "critical energy infrastructure information" (CEII),[1] includes locational data, security plans and vulnerability risk assessments. Often state regulators determine procedures for protecting CEII, including how to label and store data. While state public disclosure laws vary significantly, 30 states have various forms of open law protections for CEII, including **Connecticut**, **Florida**, **Idaho** and **Kansas** which include provisions to exempt sensitive cybersecurity-related information.[27] When determining how to exempt and secure CEII, states can evaluate industry best practices and federal CEII protection rules promulgated by DOE and FERC.[28] A forthcoming NGA white paper will provide more detail on this topic.

[1] Terminology can vary, however this paper will refer to this information as CEII.


State Open Government Law Exemptions for Critical Infrastructure Information
🟩 States with statutory exemptions: 28
🟫 States with other forms of exemptions: 3
□ No exemption for critical infrastructure information: 19
WA
OR
CA
NV
ID
MT
WY
UT
AZ
NM
CO
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
OH
KY
TN
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
NH
ME
MA
CT
RI
NJ
MD
DE
AK
HI

The map was developed with Esri's mapping software based on data from the National Conference of State Legislatures.[29]

Collaborate with Utility Regulators to Enhance their Cybersecurity Oversight

Public utility commissions (PUCs) are key to improving state utility cybersecurity postures, through their oversight of parts of the electric utility industry, ability to authorize cost recovery for investments, and their roles during restoration and response activities. Governors can support grid cybersecurity by directing or encouraging PUCs to examine the adoption and deployment of new technologies or processes by regulated utilities. Governors also encourage PUCs to direct regulated entities to conduct cybersecurity assessments and audits to better understand their cybersecurity posture. For example, in 2013, **Connecticut**'s Comprehensive Energy Strategy, signed by then-Governor Dan Malloy, directed the Public Utilities Regulatory Authority (PURA) to conduct a "cyber review" to assess the state's electric, natural gas and water utilities' cyber capabilities and recommend actions to strengthen deterrence.[30] Following the review, PURA held technical meetings with utilities to review how they manage cyber risk. Through voluntary standards and guidelines, industry adopted utility-wide cyber updates and procedures to improve expertise and help identify vulnerabilities.[31] The New York Public Service Commission's Office of Utility Security (OUS) conducts quarterly on-site security audits of utilities to evaluate the effectiveness of their cybersecurity systems.[32] The OUS typically evaluates utility cybersecurity measures by comparing them to the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection standards.

Given the complexity of the issue, utility regulators, who must evaluate utility investments for potential rate recovery, may find it difficult to accurately assess the cost of cybersecurity investments and evaluate them in the context of the "used and useful" criteria of traditional cost-of-service ratemaking.[33] It is therefore essential that PUCs understand the latest cybersecurity technologies, cybersecurity standards and the cost of investments, and continuously evaluate and refresh the knowledge of PUC staff. The resource section below includes guidance to that end.

Participate in Cyber Exercises to Practice Response, Strengthen Communication, and Identify Areas for Improvement

Exercises simulating cyber-attacks can help government and utilities practice coordinated responses, identify gaps or misalignments in plans, strengthen communication channels, and address areas for improvement.[34] They can be an efficient way to test security and response with limited resources.[35] Some utilities conduct internal cyber exercises or partner with other organizations including academia, technology companies, vendors and other utilities to identify vulnerabilities and response strategies where results may be reported back to state regulators.[36] Other exercises test coordination more broadly across industry, federal, state, local and international entities. One well-recognized cross-sector exercise, GridEx, convenes thousands of industry and government participants over multiple days every two years to test the electricity sector's ability to respond to cyber and physical attacks.[37] Another exercise to stress test the nation's energy infrastructure and strengthen regional cooperation is Liberty Eclipse, which consists of cyber-attack scenarios on critical energy infrastructure and convenes stakeholders from federal, state and local governments, the electricity and oil and natural gas industry, as well as other key partners.[38] Governors can ensure their states participate in regional and national exercises, direct state agencies to conduct collaborative local or regional exercises, and implementing recommendations described in after-action reports.[39] The 2014 **New York** State Critical Infrastructure Cybersecurity Exercise involved more than 120 participants from 13 utilities, industry organizations, federal, state, local and tribal governments.[40] The scenario tested incident response capabilities through a mock cyber-attack on critical infrastructure affecting energy delivery systems.

Leverage the National Guard's and Civilian Workforce's Existing Cyber Expertise

Governors may want to engage National Guard units that can provide valuable support and expertise in preparation for and during a grid emergency, particularly if they have a dedicated cyber unit. As of the beginning of 2019, the National Guard had close to 4,000 cyber service members in 59 cyber units in 38 states.[41] These units, which operate on a part-time basis in support of their respective states, are trained to joint standards established by the U.S. Cyber Command and are utilized in a variety of ways.[42] The U.S. Cyber Command also has new authority to defend critical infrastructure but its role has not yet been defined. Governors and states should stay abreast as those roles are defined. For example, in 2015, the **Washington** National Guard conducted a "red team" operation to expose cyber vulnerabilities at the Snohomish County Public Utility District (SnoPUD). The National Guard, SnoPUD and other government and private-sector members formed the Energy Sector Cybersecurity Working Group and published the Cybersecurity Guide for the Critical Infrastructure of Washington State.[43] The guide is based on the National Institute of Standards and Technology (NIST) cybersecurity framework and assists small and medium utilities, as well as municipal and cooperative electricity utilities that lack the capacity to invest in expensive cyber defenses. **Michigan's** National Guard is developing cyber units by leveraging individuals in the National Guard Reserve with experience in the cyber field.[44] They are augmenting this through the Cyber Civilian Corp (MiC3) consisting of trained expert volunteers to serve as a rapid response team that can "provide mutual aid to government, education, and business organizations" in the event of a cyber emergency.[45] NGA has a detailed case study of the MiC3 on its Cyber Resource Center website.[46]

Conduct Risk Assessments

Risk assessments of cyber threats and vulnerabilities across the electricity sector can help states protect critical infrastructure and make informed investment decisions.[47] Risk assessments help identify threats, gauge the likelihood of occurrence, identify the potential impacts, and inform the development of protection and mitigation plans. At the direction of the governor, governors' homeland security advisors and state chief information security officers – in partnership with state energy officials and utility regulators – should determine where risk assessments are needed, who should conduct the assessment, and what methodology should be used.[48] States can develop risk assessments internally, contract with the private sector, or leverage federal resources. For example, **West Virginia** passed the Secure WV Act, which includes a requirement that state agencies undergo cyber risk assessments and exempts cyber risk information from public disclosure. [49] States also encourage electric-sector participants to include risk management practices in their operations. For example, the **California** Public Utility Commission's Risk Assessment and Safety Advisory (RASA) Section develops risk assessments and informs commission proceedings to ensure "regulated entities integrate risk analysis and risk management practices into their current operations, future planning, and decision-making processes."[50] States also can use the Nationwide Cybersecurity Review, operated by the Center for Internet Security and the U.S. Department of Homeland Security, to identify gaps and capabilities of state cybersecurity programs.[51]

The DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is leading a State Energy Risk Assessment Initiative to increase states' understanding of energy infrastructure risk and inform investment decisions, resilience strategies and asset management. The initiative intends to instill a culture of energy risk management in state entities, integrate energy risk assessments into existing state energy assurance plans (EAPs), and promote transparent and defensible investment and mitigation decisions.[52] This initiative is a collaborative effort with the National Governors Association, the National Association of State Energy Officials, the National Association of Regulatory Utility Commissioners and the National Conference of State Legislatures.

Roles and Responsibilities of Key Parties

Because grid security is a multidisciplinary, multi-sector challenge, confronting sophisticated threats, it demands a strategic approach that leverages distinct expertise, resources and functions from across the public and private sectors. This section describes the responsibilities of key state, industry and federal entities for electric-sector cybersecurity planning and response.

Governors and State Officials

States are critical partners in identifying threats, enhancing cybersecurity, and coordinating response and recovery efforts. Securing the electric grid requires support and coordination from numerous state participants, including governors, emergency managers, law enforcement officers, homeland security officials, utility commissioners and energy officials.

As the chief executive officers of their states, governors implement state laws, oversee the operation of the state executive branch, and ensure their states are adequately prepared for all emergencies and disasters. As such, governors are uniquely positioned to convene state agencies and stakeholders as well as counterparts from neighboring states to enhance communication and align cybersecurity policies and plans.

Sharing cyber threat and vulnerability information between state, industry and federal partners is a core mitigation and response function.[53] Governors play an integral role by ensuring state agencies take advantage of information sharing opportunities between government and industry. Additionally, each state and three of the five territories operate state-designated fusion centers. Fusion centers are designed to encourage interagency and intergovernmental cooperation. They receive, integrate and analyze information and intelligence from federal, state and local authorities.[54]

Broadly, states have regulatory authority over retail sales of electricity, electric generation and distribution facilities, and are vital to ensuring their security. State public utility commissions (PUCs), whose commissioners are appointed by the governor in all but 14 states (where they are elected), independently regulate all investor-owned and some consumer-owned utilities (municipal utilities and rural electric cooperatives).[55] These regulated utilities must seek approval to recover investments, including for cybersecurity, through consumer rates.[56] Although PUCs are independent, opportunities exist for governors to appropriately support regulatory outcomes, for example by directing PUCs to evaluate the security of state-regulated utilities and offer recommendations to strengthen cyber defenses.

Industry

States should coordinate with the private sector to develop emergency response and risk communications plans for cyber incidents affecting privately owned systems or infrastructure.[57] Most of the nation's energy infrastructure is privately owned and operated, which tasks the private sector with vital responsibilities for managing cybersecurity risks.[58] Electric utilities are thus responsible for a number of crucial functions, including protecting assets and detecting, responding and recovering from cyber incidents.[59] To coordinate and manage these challenges, the electricity industry has coalesced around several entities to leverage collective knowledge and resources. Governors should understand these industry resources, groups and activities to identify how they align with state organizations and plans and to identify optimal forums for coordination and information sharing. Further, by working with industry, governors can better coordinate response and restoration efforts should an attack occur. A brief description of the relevant organizations and programs follows.

The Electricity Information Sharing and Analysis Center (E-ISAC) serves as the primary security communications channel, gathering, analyzing, and sharing security and threat information for the electric sector and coordinating with other industry and government partners.[60] The E-ISAC is operated by NERC but is organizationally isolated from NERC's enforcement processes. The E-ISAC manages the Cybersecurity Risk Information Sharing Program (CRISP) to enable "bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure."[61] CRISP enables energy-sector owners and operators to voluntarily share near-real-time network data with each other and government by installing passive sensors called Information Sharing Devices (ISDs). The ISDs share encrypted data for classified, intelligence-enriched analysis by DOE and non-classified analysis by the Pacific Northwest National Laboratory. This dual analysis is used to identify cyber threat patterns and attack indicators, which then sent as alerts and mitigation measures back to owners and operators through the E-ISAC.[62] CRISP's 26 participating utilities account for three-quarters of U.S. electricity customers.[63] Of note, the E-ISAC and Multi-State ISAC (MS-ISAC: the main cybersecurity resource for state, local, tribal and territorial governments, including chief information officers, Homeland Security advisors and fusion centers) recently agreed to improve information sharing between the two organizations and their members.[64] As discussed in the "strategies" section above, states need to ensure information obtained from the private sector is protected and stored properly.

The Electricity Subsector Coordinating Council (ESCC) consists of electric-sector industry executives and interacts closely with the Energy Government Coordinating Council (EGCC),which includes federal and state government participation, to serve as the principal liaison between the federal government and electric power sector leaders.[65] The ESCC supports industry-led initiatives to "facilitate coordination with the government and other critical infrastructure sectors; improve information sharing capabilities, tools and technologies; and enhance resilience, response and recovery efforts."[66] [2]

The Cyber Mutual Assistance (CMA) Program is a relatively new industry initiative composed of cyber experts that "provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems and/or IT infrastructure due to a cyber emergency."[67] Participants of the CMA Program cover approximately 80 percent of U.S. electricity customers.[68]

Energy Emergency Assurance Coordinators

The Energy Emergency Assurance Coordinators (EEAC) program is a cooperative effort between the National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), the National Governors Association (NGA), the National Emergency Management Association (NEMA), and the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), Infrastructure Security and Energy Restoration (ISER) Division to support timely communication and information sharing during energy emergencies.[1] Through the EEAC, each state assigns primary and secondary contacts for each energy source and provides DOE assessments of energy markets during an energy supply disruption or emergency. In turn, the states receive DOE assessments and situation reports, facilitating situational awareness across the states, federal government and industry.

[2] There is also an Oil and Gas Subsector Coordinating Council for those portions of the energy sector, which addresses similar and overlapping issues.

Federal Government

The federal government is a critical partner in electric-sector cybersecurity, including its role in sharing intelligence and best practices, developing standards, coordinating preparation activities, and responding to incidents. Additionally, federal authorities offer states a wealth of knowledge and resources to detect, prevent and investigate cyber-attacks.[69] Multiple agencies help perform these functions with various degrees of authority. These roles have changed over time and adjustments may continue as the cyber risk landscape evolves.

The Department of Homeland Security (DHS) manages the federal effort to promote critical infrastructure security and resilience. DHS operates the National Cybersecurity and Communications Integration Center (NCCIC), which acts as a national fusion center and provides federal, states, local officials cybersecurity information, analysis, training and exercise support. NCCIC focuses on cyber defense and incident response and coordinates with the E-ISAC.[70]

DOE is the lead agency (known as the Sector Specific Agency or SSA) for the energy sector and for cybersecurity in the energy sector.[71] In the event or imminent threat of a cyber-attack that disrupts grid reliability, the President can declare a grid security emergency.[72] This declaration enables the Secretary of Energy to, among other things, order electricity asset owners or operators to protect or restore critical electric infrastructure and share classified information.[73] DOE recently established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER)[74] to lead emergency preparedness and coordinated response to disruptions to the energy sector from cyber and physical attacks.[75]

In 2013, DHS developed the National Infrastructure Protection Plan (NIPP) 2013 to guide the national effort to manage risks to critical infrastructure. DHS also developed the National Cyber Incident Response Plan (NCIRP), in accordance with PPD-41, which articulates the roles and responsibilities, capabilities and coordinating structures that support response and recovery from significant cyber incidents.[76] The ESCC and its public-sector counterpart, the EGCC, are the backbone of the NIPP. The EGCC, led by DOE and co-chaired by DHS, coordinates interagency and cross-jurisdictional reliability and resiliency efforts.[77] It includes state, local and tribal governments and international partners from Canada and Mexico.[78]

As the SSA, DOE developed the Energy Sector-Specific Plan to "help guide and integrate the sector's continuous effort to improve the security and resilience of its critical infrastructure."[79] In 2018, DOE released the DOE Multiyear Plan for Energy Sector Cybersecurity to strengthen energy sector preparedness, coordinate incident response and recovery, and accelerate research, development and demonstration of resilient energy delivery systems.[80] Included in the plan is a goal to update DOE's 2014 Electricity Subsector Cybersecurity Capability Maturity Model (C2M2), which helps utilities and grid operators assess cybersecurity capabilities and coordinate investments.[81] DOE also tracks cyber events, requiring utilities to file a report if an incident interrupts electrical system operations.[82]

The Federal Energy Regulatory Commission (FERC) oversees the reliability of the bulk power system and approves mandatory cybersecurity reliability standards proposed by NERC.[83] Violators of the reliability standards are subject to civil fines of up to $1 million per violation per day. FERC's authority is largely limited to wholesale power sales and the transmission of electricity in interstate commerce. Consequently, local distribution systems do not have to follow the federal reliability standards.[84]

The North American Electric Reliability Corporation (NERC) is a nonprofit regulatory authority that is the officially delegated Electric Reliability Organization (ERO) for North America, subject to oversight by FERC in the United States.[85] It is responsible for developing and enforcing reliability standards of the bulk electric power system in North America, including cybersecurity standards.

Resources

State Resources

NGA Resource Center on State Cybersecurity, which includes numerous factsheets and resources on critical infrastructure including the electricity sector and materials from Governor Terry McAuliffe's 2016-2017 Chair's Initiative on cybersecurity: https://www.nga.org/bestpractices/divisions/hsps/statecyber/

NGA publication on the state's role in enhancing the cybersecurity of energy systems:
https://classic.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-eet-publications/col2-content/main-content-list/state-roles-in-enhancing-the-cyb.html

NGA publication offering actions governors can take to improve cybersecurity:
https://classic.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf

NGA memorandum comparing the 22 states that established governance bodies tasked with identifying the cyber threats facing their state and the avenues to mitigating those threats:
https://ci.nga.org/files/live/sites/ci/files/1617/docs/TaskForceMemoFinal.pdf

National Association of Regulatory Utility Commissioners (NARUC) comprehensive cybersecurity primer for state regulators:
https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F

NARUC Cybersecurity Strategy Development Guide to support state regulators in developing cybersecurity strategies. The document aims to guide PUC interactions with utilities on issues related to cybersecurity.
https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204

National Association of State Energy Officials (NASEO) guidelines on state energy assurance plans and specific guidance on smart grid and cybersecurity issues:
https://www.naseo.org/eaguidelines
https://www.naseo.org/data/sites/1/documents/publications/NASEO_Smart_Grid_and_Cyber_Security_for_Energy_Assurance_rev_November_2011.pdf

Cooperative agreement on the Energy Emergency Assurance Coordinators program and information on how to nominate individuals:
https://www.naseo.org/eeac

National Conference of State Legislators (NCSL) overview of State Efforts to Protect the Electric Grid:
http://www.ncsl.org/research/energy/state-efforts-to-protect-the-electric-grid.aspx#Cybersecurity

NCSL Budgeting for Cybersecurity:
http://www.ncsl.org/research/telecommunications-and-information-technology/budgeting-for-cybersecurity.aspx

NCSL State Cybersecurity Training for State Employees:
http://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx

NCSL Cyber Mutual Assistance (CMA) Program Information:
http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cyber%20Mutual%20Assistance%20Program.pdf

Federal Resources
Department of Homeland Security's Energy Specific Plan (2015):
https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (2014):
https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

National Institute of Standards and Technology's (NIST) framework for securing critical infrastructure:
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Department of Homeland Security's Cybersecurity Evaluation Tool (CSET) that helps users assess their cyber readiness:
https://ics-cert.us-cert.gov/Assessments

The National Cyber Incident Response Plan (NCIRP) articulates the roles and responsibilities, capabilities and coordinating structures that support response and recovery from significant cyber incidents:
https://grants.nhisac.org/BackgroundData/2016_NCIRP_National_Cyber_Incident_ResponsePlan.pdf

State-Specific Resources
Publication by the National Association of State Energy Officials on Michigan's Cyber Initiative:
http://www.naseo.org/data/sites/1/documents/publications/Michigan%20Cyber%20Profile%2012-29-15%20final%20draft%20copy.pdf

Washington State's plan for cyber emergencies, including the role of the National Guard:
https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

Washington State's Cybersecurity Guide for Critical Infrastructure:
https://www.snopud.com/Site/Content/Documents/cyber/Cybersecurity_WA_915.pdf

Connecticut's Public Utilities Regulatory Authority plan for cyber emergency and standards:
http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf

[1] Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Annual Vulnerability Coordination Report – Incident Response Pie Charts* (Washington, DC: United States Department of Homeland Security, 2016).

[2] Stanford.edu, "Critical Infrastructure Resilience," Stanford University, https://fsi.stanford.edu/research/critical-infrastructure-resilience (accessed May 1, 2019); and DHS.Gov, "Critical Infrastructure Sectors," Department of Homeland Security, https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed May 1, 2019).

[3] Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Incident Response Summary Report* (Washington, DC: United States Department of Homeland Security, 2011).

[4] Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Annual Vulnerability Coordination Report – Incident Response Pie Charts* (Washington, DC: United States Department of Homeland Security, 2016).

[5] Ibid.

[6] Ibid

[7] The Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Washington, DC: The Council of Economic Advisers, 2018).

[8] Ibid.

[9] Oregon Department of Energy and Public Utility Commission, *Oregon State Energy Assurance Plan* (August 2012), https://www.oregon.gov/energy/Data-and-Reports/Documents/2012%20Oregon%20State%20Energy%20Assurance%20Plan.pdf

[10] Ibid.

[11] Ibid.

[12] An Executive Order establishing the Governor's Cybersecurity Advisory Team, Vermont Legislature, 2nd Sess. (October 10, 2017).

[13] Office of Vermont Governor Phil Scott, "Governor Phil Scott Announces Appointments to Cybersecurity Advisory Team," Press Release, November 20, 2017, https://governor.vermont.gov/press-release/governor-phil-scott-announces-appointments-cybersecurity-advisory-team.

[14] DHS.gov, "State and Major Urban Area Fusion Centers" Department of Homeland Security, https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

[15] Executive Order No. 178, New Jersey Legislature (May 20, 2015).

[16] State of New Jersey Board of Public Utilities Docket No. AO16030196 (March 18, 2019), https://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf.

[17] United States Department of Energy, *Liberty Eclipse Energy – Energy Assurance Exercise & Event*, (Newport, RI: United States Department of Energy, 2016).

[18] *Grid Security Emergency Orders: Procedures for Issuance*, Federal Register Vol. 83, No. 7, *Rules and Regulations* (2018)

[19] Presidential Policy Directive 8, National Preparedness (March 30, 2011), https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

[20] Presidential Policy Directive 41, United States Cyber Incident Coordination (July 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[21] T. Simchak, D. Lauf, P. Portillo, S. Gander, *Governors Staying Ahead of the Energy Innovation Curve: A Policy Roadmap for States*. (Washington, DC: National Governors Association Center for Best Practices, July 2018).

[22] Montana Department of Environmental Quality, Montana Energy Assurance Plan, Montana Legislature, (January 2016).

[23] Ibid.

[24] United States Department of Energy, *Oklahoma Energy Assurance Plan* (Washington, DC: United States Department of Energy, 2013).

[25] T. Simchak, D. Lauf, P. Portillo, S. Gander, *Governors Staying Ahead of the Energy Innovation Curve: A Policy Roadmap for States*. (Washington, D.C.: National Governors Association Center for Best Practices, July 2018).

[26] FERC.gov, "Critical Energy/Electric Infrastructure Information (CEII)" Federal Energy Regulatory Commission, https://www.ferc.gov/legal/ceii-foia/ceii.asp

[27] Emily Dowd, *Open Government Laws and Critical Energy Infrastructure* (Washington, DC: National Conference of State Legislatures, 2018).

[28] J. Rackley, P. Portillo, *State Protection of Critical Energy Infrastructure Information (CEII)*. (Washington, D.C.: National Governors Association Center for Best Practices, 2019).

[29] Dowd, Emily, *Open Government Laws and Critical Energy Infrastructure*, National Conference of State Legislatures, January 2018 (http://www.ncsl.org/research/energy/open-government-laws-and-critical-energy-infrastructure.aspx)

[30] State of Connecticut Public Utilities Regulatory Authority, *Cybersecurity and Connecticut's Public Utilities,* (New Britain, CT: State of Connecticut Public Utilities Regulatory Authority, 2014).

[31] State of Connecticut, Public Utilities Regulatory Authority, *Connecticut Public Utilities Cybersecurity Action Plan,* (New Britain, CT: State of Connecticut Public Utilities Regulatory Authority, 2016).

[32] Chairman Todd A. Snitchler (2012) Written Testimony before the U.S. Senate Committee on Energy and Natural Resources, Full Committee Hearing on Cybersecurity, July 17, 2012.

[33] United States Department of Energy, *Liberty Eclipse Energy*.

[34] North American Electric Reliability Corporation, "GridEx V Frequently Asked Questions," Fact Sheet (Atlanta, GA: North American Electric Reliability Corporation)

[35] Indiana Executive Council on Cybersecurity, *Cyber Pre- Thru Post- Incident Working Group Strategic Plan* (Indianapolis, IN: Indiana Executive Council on Cybersecurity, September 2018).

[36] Mission Support Center Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* (June 19, 2017); and The Florida Public Service Commission Office of Auditing and Performance Analysis, *Review of Cyber and Physical Security Protection of Utility Substation and Control Centers,* (Tallahassee, FL: The Florida Public Service Commission Office of Auditing and Performance Analysis, April 2018).

[37] North American Electric Reliability Corporation, *Grid Security Exercise GridEx IV Lessons Learned,* (Atlanta, GA: North American Electric Reliability Corporation, March 2018).

[38] U.S. Department of Energy, *Liberty Eclipse Energy – Energy Assurance Exercise & Event, December 8–9, 2016 Exercise Summary Report,* https://www.energy.gov/oe/articles/liberty-eclipse-exercise-summary-report; and Blake Sobczak, “DOE to vet grid’s ability to reboot after a cyberattack,” *E&E News*, August 3, 2018, https://www.eenews.net/stories/1060092675.

[39] National Governors Association, *A Governor’s Guide to Homeland Security* (Washington, DC: National Governors Association Center for Best Practices, Homeland Security & Public Safety Division, November 2018).

[40] New York Senate Standing Committee on Veterans, Homeland Security and Military Affairs, *To Address New York State’s Cyber Security Infrastructure*, 2015

[41] Scott Maucione, “National Guard cyber units protect country’s interests, still face training issues,” *Federal News Network*, January 18, 2019, https://federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/.

[42] National Governors Association, *A Governor’s Guide to Homeland Security* (Washington, DC: National Governors Association Center for Best Practices, Homeland Security & Public Safety Division, November 2018).

[43] State of Washington Energy Sector Cybersecurity Working Group, *Cybersecurity Guide for Critical Infrastructure for the State of Washington* (Olympia, WA: State of Washington Energy Sector Cybersecurity Working Group).

[44] National Association of State Energy Officials, *NASEO State Energy Cybersecurity Models Analysis: Michigan Cybersecurity Structures and Programs Profile* (Arlington, VA: National Association of State Energy Officials, December 2015).

[45] State of Michigan, “Michigan Cyber Civilian Corps,” https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html.

[46] Michael Garcia, “Building a Civilian Cyber Corps,” *National Governors Association*, June 2017, https://ci.nga.org/files/live/sites/NGA/files/pdf/2018/HSPS/MiC3%20Memo%20(1).pdf

[47] United States Department of Energy Office of Electricity Delivery and Energy Reliability, “Creating a Risk Assessment Culture for State Energy Infrastructure Decision Making,” Fact Sheet (Washington, DC: United States Department of Energy Office of Electricity Delivery and Energy Reliability, April 2015).

[48] National Governors Association, *A Governor’s Guide to Homeland Security* (Washington, DC: National Governors Association Center for Best Practices, Homeland Security & Public Safety Division, November 2018).

[49] Secure WV Act, H.B. 2452, West Virginia Legislature 2019 Regular Session (passed March 7, 2019).

[50] Cpuc.ca.Gov, “Utility Risk Assessment and Safety Advisory,” California Public Utility Commission, http://www.cpuc.ca.gov/riskassessment/ (accessed May 5, 2019).

[51] CISecurity.org, “Nationwide Cybersecurity Review,” Center for Internet Security, https://www.cisecurity.org/ms-isac/services/ncsr/ (accessed May 1, 2019)

[52] Ibid.

[53] United States Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*

[54] National Governors Association, *A Governor’s Guide to Homeland Security* (Washington, DC: National Governors Association Center for Best Practices, Homeland Security & Public Safety Division, November 2018).

[55] T. Simchak, D. Lauf, P. Portillo, S. Gander, *Governors Staying Ahead of the Energy Innovation Curve: A Policy Roadmap for States* (Washington, DC: National Governors Association Center for Best Practices, July 2018).

[56] Jim Lazar, Electricity *Regulation in the US: A Guide. Second Edition*. (Montpelier, VT: The Regulatory Assistance Project, June 2016).

[57] National Governors Association, *A Governor’s Guide to Homeland Security* (Washington, DC: National Governors Association Center for Best Practices, Homeland Security & Public Safety Division, November 2018).

[58] United States Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*

[59] Ibid

[60] EISAC.com, “Governance,” Electricity Information Sharing and Analysis Center, https://www.eisac.com/governance (accessed May 1, 2019).

[61] Energy.gov, “Energy Sector Cybersecurity Preparedness,” Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER), https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity

[62] United States Department of Energy Office of Cybersecurity, Energy, Security, and Emergency Response, “Cybersecurity Risk Information Sharing Program (CRISP),” Fact Sheet (Washington, DC: United States Department of Energy Office of Cybersecurity, Energy, Security, and Emergency Response, September 2018).

[63] United States Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*

[64] North American Electric Reliability Corporation, “NERC, Community-Owned Utilities Group Launch Information Sharing Partnership to Strengthen Grid’s Cyber, Physical Security,” February 27, 2019, https://www.nerc.com/news/Headlines%20DL/MS-ISAC%20Announcement%2027FEB19%20final.pdf.

[65] ESCC: http://www.electricitysubsector.org/

[66] Electricity Subsector Coordinating Council, “ESCC Electricity Subsector Coordinating Council” Fact Sheet (Washington, DC: Electricity Subsector Coordinating Council, January 2018).

[67] Electricity Subsector Coordinating Council, “The ESCC’s Cyber Mutual Assistance Program,” Fact Sheet (Washington, DC: Electricity Subsector Coordinating Council, January 2018).

[68] EEI.org, “Cyber & Physical Security,” Edison Electric Institute, http://www.eei.org/issuesandpolicy/cybersecurity/Pages/default.aspx

[69] National Governors Association, *A Governor's Guide to Homeland Security* (Washington, DC: National Governors Association Center for Best Practices, Homeland Security & Public Safety Division, November 2018).

[70] DHS.gov, "National Cybersecurity and Communications Integration Center," Department of Homeland Security Information Sharing, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[71] The White House, *Presidential Policy Directive*

[72] Fixing America's Surface Transportation Act, 114th Congress (December 4, 2015).

[73] Ibid.

[74] United States Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response," Press Release, February 14, 2018. https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency

[75] Energy.gov, "CESER Mission," Office of Cybersecurity, Energy Security, and Emergency Response, https://www.energy.gov/ceser/ceser-mission

[76] United States Department of Homeland Security, *National Cyber Incident Response Plan*, (Washington, DC: Department of Homeland Security, December 2016

[77] DHS.gov, "Government Coordinating Councils," Department of Homeland Security Critical Infrastructure Sector Partnerships, https://www.dhs.gov/cisa/government-coordinating-councils

[78] Department of Homeland Security, "Energy Sector Government Coordinating Council Charter," Fact Sheet (Washington, DC: Department of Homeland Security, 2014).

[79] United States Department of Homeland Security, *Energy Sector-Specific Plan,* (Washington, DC: United States Department of Homeland Security, 2015).

[80] United States Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*

[81] United States Department of Energy, United States Department of Homeland Security, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)* (Washington, DC: United States Department of Energy, United States Department of Homeland Security, February 2014).

[82] Oe.netl.doe.gov, "Electric Disturbance Events," Office of Cybersecurity, Energy Security, & Emergency Response, https://www.oe.netl.doe.gov/oe417.aspx

[83] Energy Policy Act of 2005, 109th Congress (August 8, 2005).

[84] Congressional Research Service, *Electric Grid Cybersecurity* (Washington, DC: Congressional Research Service, September 2018).

[85] FERC Docket numbers RR06-1-000 & RR06-2-000, Washington, D.C., July 2006

Addendum

Smart And Safe: State Strategies for Enhancing Cybersecurity in the Electric Sector

The threat of malicious attacks on the electrical grid is ever present, and the vulnerability of energy infrastructure to cyberattacks grows as the grid becomes increasingly interconnected and modernized. In 2019, NGA released a resource titled "Smart and Safe: State Strategies for Enhancing Cybersecurity in the Electric Sector" outlining best practices for Governors to enhance electric grid cybersecurity. While the recommendations in the paper continue to remain relevant, new resources have been released and actions have been taken that can further inform or support Governors' efforts to protect the grid from malicious attacks.

Since NGA published the 2019 paper, the threat of cyberattacks on energy systems has only grown. In May 2021, a ransomware attack on the Colonial Pipeline infected the data and information technology (IT) systems of the pipeline, leading operators to preemptively shut down the pipeline for multiple days out of an abundance of caution, protecting operational systems but also leading to consumer panic buying that resulted in fuel supply concerns. In addition, the use of cyberattacks to critical infrastructure during the Russian war in Ukraine has raised concerns for the National Security Agency (NSA), and the vulnerability of U.S. critical infrastructure sectors to People's Republic of China state-sponsored cyber actors was highlighted in a February 2024 joint assessment by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the NSA.

New Federal Resources

On the federal level, many key actions have been taken in recent years to advance cybersecurity standards for energy systems. In 2021, the Infrastructure Investment and Jobs Act (IIJA) was passed into law with $1.9 billion in funding for cybersecurity across many programs such as those focused on energy, water, transportation, and state, local, tribal, and territorial governments. In addition, the IIJA includes a provision requiring states and territories to submit Energy Security Plans as a condition of eligibility to receive funding from the U.S. Department of Energy (DOE) State Energy Program. According to additional guidance states and territories have received from DOE, "delivery of applicable FY25 federal financial assistance to a state or territory may be delayed or withheld under Part D of Title III of EPCA, if a fully compliant SESP is not received and verified by DOE." State Energy Security Plans must incorporate cybersecurity, including assessments and mitigation strategies for cyberthreats. The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the U.S. DOE has many resources for states and territories, including this State Energy Security Plan Guide, as they work to complete energy security plans.

March 2024

In March 2023, President Biden released the National Cybersecurity Strategy (NCS) to establish a framework to protect critical infrastructure from cyberattacks, disrupt threat actors, shape market forces to promote security, make investments in cybersecurity research and development, and create international cybersecurity partnerships. The document establishes strategic objectives to advance cybersecurity across all missions, stakeholders and sectors. The NCS calls for a defensible and resilient digital ecosystem to protect our national security, public safety and economic prosperity.

This is a significant undertaking that will require industry, communities, and state, local, tribal, and territorial governments to share responsibility to create a more secure cyberspace. In July 2023, the White House released the National Cybersecurity Strategy Implementation Plan (NCSIP) to coordinate efforts with all relevant stakeholders across dozens of Federal initiatives.

The U.S. DOE, the North American Electricity Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC) and the U.S. Transportation Security Administration (TSA) have all taken actions to encourage or require cybersecurity standards and practices in the energy sector. In addition to the many energy cybersecurity programs from the IIJA that DOE is implementing, the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) released its National Cyber-Informed Engineering Strategy in 2023 to encourage cyber-resilient design, operation and maintenance of energy infrastructure. NERC governs mandatory cybersecurity standards for the bulk power system in the United States. Known as the NERC Critical Infrastructure Protection (CIP) Reliability Standards, these standards are the minimum level of cybersecurity practices grid operators can maintain. In 2022, NERC released a Distributed Energy Resource Strategy to encourage cybersecurity practices for distributed generation like rooftop solar, though distribution-level infrastructure is not subject to NERC CIP Standards. FERC is considering mandatory cybersecurity standards, and in 2022 proposed new incentives of an additional 2% return on equity for utilities to voluntarily invest in cybersecurity. Following the Colonial Pipeline cyberattack, the Transportation Secuiry Administration (TSA), which regulates owners and operators of pipelines, issued mandatory cybersecurity standards.

Recent State Actions

State and territory leaders have also been very active in encouraging or requiring the adoption of cybersecurity standards for critical energy infrastructure. In 2022, the **Virginia** Department of Emergency Management, Virginia Department of Information Technology, Dominion Energy, Virginia State Police and Virginia National Guard participated in an energy cybersecurity exercise referred to as "Cyber Fortress." This public-private collaboration allowed the commonwealth and its largest electric utility to test the commonwealth's emergency operations plan and associated cyber response annex to better prepare for a cyberattack. The exercise demonstrated the importance of simultaneously managing the downstream impacts of power outages and cyber recovery efforts.

In August 2023, **New York** Governor Kathy Hochul announced a Statewide Cybersecurity Strategy to safeguard critical infrastructure, personal information, and digital assets in New York from malicious actors. This strategy highlights AB 3904, a 2022 bill that was signed into law by Governor Hochul "requiring electric distribution utilities to prepare for cyberattacks in their annual emergency response plans" through new enhanced New York Public Service Commission Auditing Powers.

In response to heightened security concerns stemming from Russia's ongoing war in Ukraine, President Biden penned a letter to Governors on March 18, 2022, encouraging the adoption of state cybersecurity standards to protect critical energy infrastructure. On behalf of the Council of Governors, **Minnesota** Governor Tim Walz and **Ohio** Governor Mike DeWine reinforced the importance of cybersecure energy infrastructure and a whole-of-government approach to cybersecurity in a May 4, 2022, response to the President. The letter recommended a consistent, federally-coordinated approach to cyber standards for the energy sector. Recognizing the importance of a standardized approach to cybersecurity standards, DOE CESER is currently working with the National Association of Regulatory Utility Commissioners (NARUC) to "establish a set of cybersecurity baselines that states can consider and adopt for distribution systems and distributed energy resources." [1]

NGA Resources

NGA recently published an updated 2023 Energy Cybersecurity Resources for Governors' Advisors that provides an overview of federal and state cybersecurity standards for the energy sector as well as a collection of energy cybersecurity resources from NGA, the federal government and other state focused organizations.

This addendum was prepared by Fiona Forrester, Policy Analyst, NGA Center for Best Practices. For additional energy cybersecurity resources, please visit this online resource guide NGA has compiled, or reach out to the energy, cybersecurity, or homeland security leads at the NGA's center for best practices: Dan Lauf (dlauf@nga.org), Steve Fugelsang (sfugelsang@nga.org, and Jessica Davenport (jdavenport@nga.org).

This material is based upon work supported by the Department of Energy, Office of Cybersecurity, Energy Security, & Emergency Response under Award Number DE-CR0000011.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or 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 United 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.

[1] More information on this and related initiatives are described in a March 2023 blog post by DOE CESER Director Puesh Kumar: https://www.energy.gov/ceser/articles/national-cybersecurity-strategy-path-toward-more-secure-and-resilient-energy-sector.