ADDRESSING CYBER AND PHYSICAL THREATS

Technologies and Key Policy Trends

TECHNOLOGIES AND THREATS OVERVIEW.

Cyberthreats have emerged as a major concern and have been growing rapidly over the past decade. Between 2010 and 2016, the number of incidents reported to the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team increased sixfold.[1] In 2016, the energy sector was the third most targeted industry, accounting for 20% of reported incidents.[2] The consequences of a cyberattack on the electricity system could be serious: disrupting power or fuel supplies, damaging specialized equipment and jeopardizing public welfare. Traditional generation and transmission that use internet-connected supervisory control and data acquisition systems (SCADAs) can be vulnerable to attack. Clean energy technology can also be vulnerable, given that many of those technologies are also internet connected or supported by internet-connected devices.[3,4]

Cyberattacks on U.S. energy infrastructure have had limited consequences so far because they have mainly targeted personal information rather than operating units,[5,6,7] but there have been significant cyberattacks globally. The most notable cyberattacks occurred in Ukraine in 2015 and 2016. In 2015, cyberattackers manipulated circuit breakers across multiple distribution operators to cause a 3.5-hour power outage for 225,000 people. In 2016, malicious hackers created and deployed modular malware specifically targeting industrial control systems and were able to take 200 megawatts (MW) offline.

The United States has thus far avoided cyberattacks of consequence, but major incidents of concern have occurred. In 2017, several nuclear power generation sites experienced cyberintrusions.[8] These intrusions did not extend beyond the business systems, did not affect power delivery or cause safety concerns, but targeting of U.S. nuclear power plants is cause for concern. In March 2019, a cyberattack in the Western Interconnection temporarily eliminated visibility into SCADAs. The affected utilities were able to maintain adequate electricity supply, but the attack did interrupt internal operations[9] and represented the first successful attack on U.S. grid operations.

New threats continue to emerge. According to statements made by the Director of National Intelligence during the Worldwide Threat Assessment to Congress in 2019, malicious actors and nation-states have the ability to disrupt U.S. electric and gas distribution systems "with the goal of being able to cause substantial damage."[10]

In addition, physical threats caused by nature have always been a concern for governors and the energy sector alike. Potential earthquakes along major fault lines like the San Andreas in **California**, Cascadia in the Pacific Northwest and New Madrid in the Midwest, have posed longstanding dangers, alongside hurricanes, heavy snow and other storms, wildfires and floods. These threats are in addition to longstanding grid incidents involving animals and drivers, vandalism and physical attacks on grid infrastructure by bad actors.

In the past decade, natural threats have grown more intense. The overall number of hurricanes has remained the same, but the storms have increased in intensity and caused record-breaking levels of damage.[11] Rising sea surface temperatures cause increased wind speeds during storms, and rising sea levels amplify storm surges. The 2017 hurricane season resulted in a historic $282 billion in damages.[12] Similarly, wildfires have increased in frequency and duration. In fact, 61% of all fires ever recorded in the West have occurred since 2000, and the number of fires that burn more than 100,000 acres has climbed steadily in the past 20 years.[13] The frequency of flooding is also expected to increase. A Federal Emergency Management Agency report on the National Flood Insurance Program estimated that U.S. floodplains will grow by 45% by the end of the century.[14] At the same time, deaths attributed to flooding have risen. Over the past 30 years, flooding had killed on average 86 people annually. In the past 10 years, this average increased to 95, and there were more than 100 deaths each year in 2015, 2016 and 2017.[15]

ADDRESSING CYBER AND PHYSICAL THREATS

On the bad actors front, in 2013, Pacific Gas and Electric's Metcalf transmission substation was attacked by snipers, causing an estimated $15 million in damages.[16] Although limited in scope, that incident highlighted the vulnerabilities of the system and led to increased calls for securing substations and making them less accessible to the public.

KEY POLICY TRENDS

Establishment of the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER). DOE established CESER in 2018 to elevate the importance of cybersecurity issues in the energy industry. The office focuses on increasing emergency preparedness and coordinated response to disruptions to the energy sector, including physical incursions and cyberattacks, natural disasters and human-made events.[17] The office works closely with states to share information and provide support during emergencies; provide technical assistance and research; and host emergency exercises, trainings and workshops.

Growth and development of energy industry information sharing and analysis centers (ISACs). The energy industry is represented by three ISACs; the Electricity ISAC, the Oil and Natural Gas ISAC and the Downstream Natural Gas ISAC. Each ISAC has been growing in membership, building trust within the industry and increasing information sharing.

Increased importance of cybersecurity in energy industry subsector coordinating councils. Energy industry coordinating councils have also increased their focus on cybersecurity. The industry is represented by two main councils: the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council. These councils have established cybersecurity work groups or initiatives to address industry cybersecurity concerns. Governors and states are represented through the Energy Sector Government Coordinating Council, which often meets jointly with the industry councils.

Establishment of state resilience officers. As the intensity of storms increases and the amount of damages paid out balloons, states have increased their efforts to enhance resilience. They are designating officers to consider resilience across multiple functions. Governors in **Colorado, Florida, New Jersey, North Carolina, Oregon** and **Virginia** have all either designated a resilience officer or created a statewide resilience office.

Updating energy assurance plans with resilience in mind. States are also revising and updating their energy assurance plans with resilience measures to counter the growing intensity of storms and increased damage. This work has taken the form of altering planning protocols to include resilience metrics, institutionalizing existing relationships between state agencies and the private sector, improving communication among state agencies and with the federal government, addressing fuel assurance issues and investigating how microgrids and combined heat and power could help increase resilience.[18] New Jersey, **Hawaii** and **Michigan** have begun working on a petroleum "annex" to their energy assurance plans to better plan for petroleum supply issues during and after emergencies.[19] Colorado created a resilience framework to "assess current risks, plans and practices, and to build resiliency into policies, actions and investments across multiple sectors."[20] The framework is intended to help communities better understand the stresses they face and create a plan to prepare for them appropriately. Oregon created an energy resilience guidebook for consumer-owned utilities intended to help local these utilities better prepare for emergencies, prioritize investments and understand their role in emergencies relative to the state and federal government.[21]

Increased deployment of distributed generation and distributed energy resources to enhance resiliency. Currently, 29 states have a renewable portfolio standard; three states have a clean energy standard and 10 other states have renewable or clean energy goals.[22] These standards and goals have led to increased deployment of distributed generation and distributed energy resources alongside utility-scale resources. Together, such resources can provide grid services during a physical or cyberincident and mitigate future outages by providing fuel diversity and self-generation.

ADDRESSING CYBER AND PHYSICAL THREATS

1 Industrial Control Systems Cyber Emergency Response Team. (2016). *ICS-CERT annual vulnerability coordination report.* Retrieved from https://www.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

2 Industrial Control Systems Cyber Emergency Response Team. (2016). *ICS-CERT annual vulnerability coordination report.* Retrieved from https://www.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

3 EY. (2015, March). *Cybersecurity and the Internet of Things.* Retrieved from www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

4 Electricity Information Sharing and Analysis Center. (2016). *E-ISAC end of year report.* Retrieved from www.eisac.com/cartella/Asset/00006271/E-ISAC%202016%20End%20of%20Year%20Report.pdf?parent=64137

5 U.S. Department of Energy, Office of Cybersecurity, Energy Security, & Emergency Response. (n.d.) Electric disturbance events (OE-417) annual summaries. Retrieved from https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

6 Mai, H. J. (2019, May 10). NERC to analyze first potential cyberattack on US grid. *Utility Dive.* Retrieved from www.utilitydive.com/news/nerc-to-analyze-first-potential-cyberattack-on-us-grid/554504

7 Sobczak, B. (2019, May 6). Experts assess damage after first cyberattack on U.S. grid. *E&E News.* Retrieved from www.eenews.net/stories/1060281821

8 Walton, R. (2017, July 7). Reports: Cyberattacks breached at least a dozen power plants, including nukes. *Utility Dive.* Retrieved from www.utilitydive.com/news/reports-cyberattacks-breached-at-least-a-dozen-power-plants-including-nuk/446581

9 Mai, H. J. (2019, May 13). US power sector recognizes cyber risks, but violations show enforcement issues. *Utility Dive.* Retrieved from www.utilitydive.com/news/us-power-sector-recognizes-cyber-risks-but-violations-show-enforcement-iss/552558

10 Coats, D. R. (2019, January 29). *Statement for the record: Worldwide threat assessment of the US intelligence community.* Retrieved from www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

11 Milman, O. (2019, May 20). Are hurricanes getting stronger—and is climate breakdown to blame? *The Guardian.* Retrieved from www.theguardian.com/world/2019/may/20/are-hurricanes-getting-stronger-and-is-the-climate-crisis-to-blame

12 Milman, O. (2019, May 20). Are hurricanes getting stronger—and is climate breakdown to blame? *The Guardian.* Retrieved from www.theguardian.com/world/2019/may/20/are-hurricanes-getting-stronger-and-is-the-climate-crisis-to-blame

13 Patel, K. (2018, December 5). Six trends to know about fire season in the western U.S. Retrieved from https://climate.nasa.gov/blog/2830/six-trends-to-know-about-fire-season-in-the-western-us

14 AECOM. (2013, June). *The impact of climate change and population growth on the National Flood Insurance Program through 2100.* Retrieved from www.aecom.com/content/wp-content/uploads/2016/06/Climate_Change_Report_AECOM_2013-06-11.pdf

15 National Oceanic and Atmospheric Administration, National Weather Service. (n.d.). Weather related fatality and injury statistics. Retrieved from www.weather.gov/hazstat

16 Pagliery, J. (2015, October 17). Sniper attack on California power grid may have been "an insider," DHS says. *CNNMoney.* Retrieved from money.cnn.com/2015/10/16/technology/sniper-power-grid

17 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. (n.d.). CESER mission. Retrieved from www.energy.gov/ceser/ceser-mission

18 Kambour, A. (2016, October 21). *Improving state coordination for energy assurance planning and response.* Retrieved from https://www.nga.org/center/publications/improving-state-coordination-for-energy-assurance-planning-and-response

19 Kambour, A. (2016, October 21). *Improving state coordination for energy assurance planning and response.* Retrieved from https://www.nga.org/center/publications/improving-state-coordination-for-energy-assurance-planning-and-response

20 Colorado Resilience Office. (2019). Resiliency frameworks. Retrieved from www.coresiliency.com/resiliency-frameworks

21 Oregon Department of Energy. (2019). *Oregon guidebook for local energy resilience for small and medium electric utilities.* Retrieved from https://www.oregon.gov/energy/safety-resiliency/Documents/Oregon-Resilience-Guidebook-COUs.pdf

22 DSIRE & North Carolina Clean Energy Technology Center. (2019, June). Renewable and clean energy standards. Retrieved from s3.amazonaws.com/ncsolarcen-prod/wp-content/uploads/2019/07/RPS-CES-June2019.pdf

ADDRESSING CYBER AND PHYSICAL THREATS

Opportunities, Challenges and State Solutions

OPPORTUNITIES. Clean energy and the technologies that accompany it, such as battery storage, present unique opportunities to increase resiliency and address the rising number of cyber and physical attacks. In the event that a storm or cyberattack takes a large-scale power generator offline, distributed generation in the community could be used to provide power to critical customers in the interim or help provide "black start" services (i.e., when a generator starts from a total or partial shutdown). Distributed energy resources can also be used in microgrids to enable communities or critical assets to operate apart from the larger grid during emergencies caused by cyber or physical events.

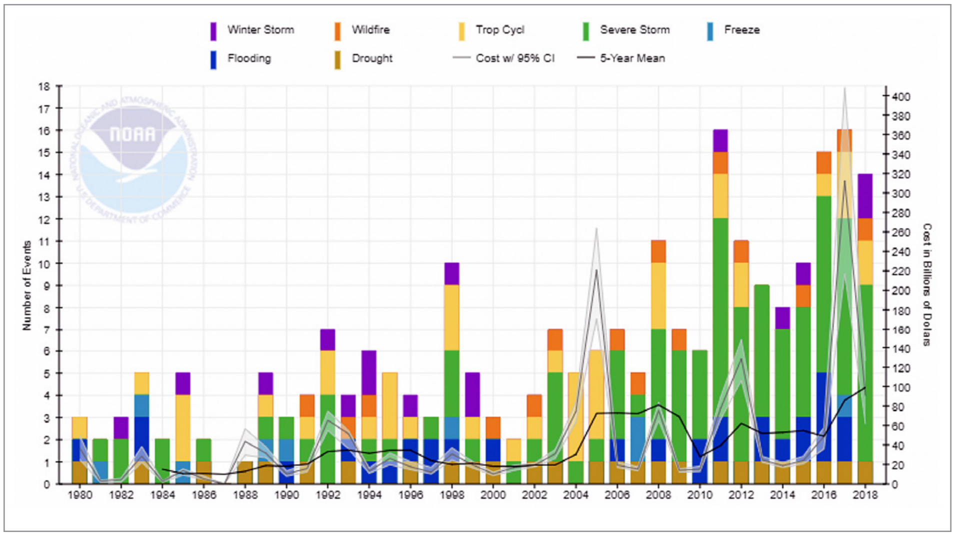


Figure 1: Consumer Price Index-adjusted billion-dollar disaster types by year

Smart and digitally connected grid technologies have been critical enablers of clean energy expansion. Everything from smart meters to new sensors to home monitoring systems make it easier to effectively integrate and optimize the use of clean energy. These elements can also be helpful in the event of a storm or cyberattack that disrupts grid operations (see Figure 1). Increased awareness and visibility from sensors and smart meters could facilitate dynamic system reconfiguration to route around comprised assets. Smart building and home energy management systems could be used for demand response to reduce the burden on the energy system during an incident, making recovery easier and faster.

CHALLENGES. Clean energy technologies present many opportunities to increase resiliency, but they also introduce vulnerabilities. Much clean energy technology is integrated with or enabled by smart technology. Most smart technology used to enable clean energy technology is internet connected. Every new connection to the internet presents a new access point for malicious hackers to infiltrate.

In addition to the internet connectivity issue, smart technology presents supply chain risks. Most smart devices are sourced and manufactured all over the world. It is often difficult to know where each component of a device originated. If the firmware or hardware in the device is compromised during manufacturing, it could make the device more vulnerable when deployed in the field. Threat actors may use this approach to gain access to energy infrastructure around the world.

The variable nature of some clean energy generation can also be a challenge if inverter technology becomes compromised. Inverters are used to convert direct current output of a clean resource into utility frequency alternating current output — a critical step in ensuring that grid frequency does not fluctuate outside the feasible range. When grid frequency deviates from its set range, it can cause grid outages. If an inverter is compromised and the current conversion is altered, those fluctuations in current can lead to outages.

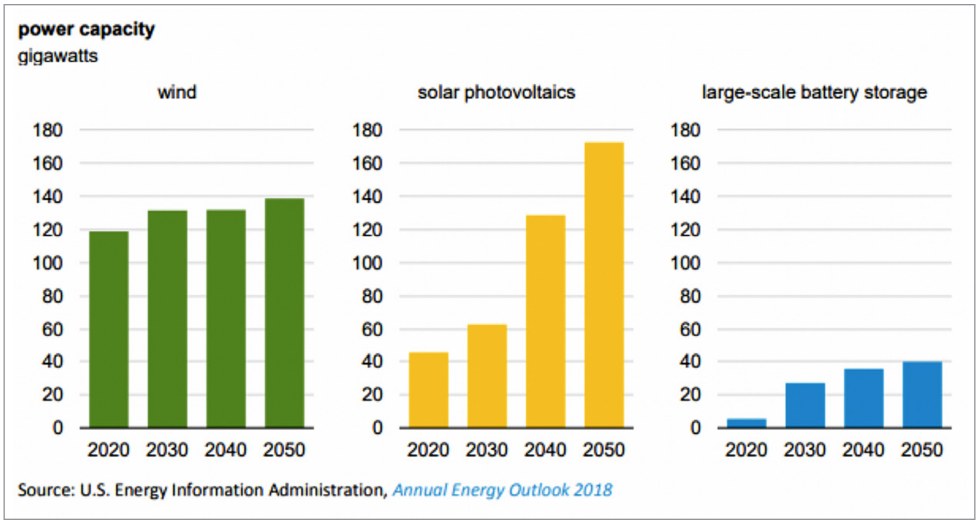
Compromised electric vehicles (EVs) and EV infrastructure can also create grid reliability problems. The introduction

ADDRESSING CYBER AND PHYSICAL THREATS

or removal of one EV and its charging demands from the electric grid is usually not a concern. However, if a network of EVs or charging infrastructure were to become compromised, that network could be used as a vector to spread malware throughout a system, transferring malware to chargers or buildings every time an EV charges. If a network of charging stations were compromised, the sudden introduction or removal of many charging EVs could cause wide power deviations, prompting a grid outage.

STATE SOLUTIONS. Governors are supporting a variety of policies to counter rising cyber and physical threats. State solutions include the following:

- ***Coordinate preparedness and planning efforts.*** Coordinating and planning state emergency efforts with the electricity sector are critical. Incorporating cybersecurity into those planning and preparedness efforts and identifying how new generation and distributed technologies can support those efforts are vital to addressing this threat.
- ***Establish cybersecurity governance bodies focused on energy industry issues.*** Governors use these bodies to accomplish a variety of goals, the most common of which are to assess the current cybersecurity preparedness level of the industry, establish roles and responsibilities, and monitor and improve cybersecurity preparedness.
- ***Protect sensitive information, including classified threat information and critical energy infrastructure information, to encourage private sector information sharing.*** Threat information sharing among public and private actors is critical to threat detection, preparation and response. Governors may need to create additional protections or consider how to securely store and exempt sensitive electricity system data from public inquiry.
- ***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; they can also direct regulated entities to conduct cybersecurity assessments and audits to better understand their cybersecurity posture.
- ***Participate in cyberexercises.*** Exercises that simulate cyberattacks can help governments and utilities practice coordinated responses, identify gaps or misalignments in plans, strengthen communication channels and address areas for improvement.
- ***Assess resiliency capabilities and gaps.*** Governors can support cross-agency collaboration to examine the status of resiliency in their state, assess gaps and prioritize action steps.
- ***Encourage the growth of microgrids and energy storage.*** Increasing the deployment of microgrids and energy storage can increase energy system resilience during or after a cyber or physical attack (see Figure 2). These technologies can be used to support critical assets such as hospitals and emergency shelters to ensure continuity of critical, life-saving functions.



Source: U.S. Energy Information Administration, *Annual Energy Outlook 2018*

Figure 2: U.S. large-scale wind, solar and battery storage capacity projections, 2020-2050

ADDRESSING CYBER AND PHYSICAL THREATS

State Solutions Spotlights

Governors have supported a range of state actions to counter growing cyber and physical threats:

- Coordinate preparedness and planning efforts.
- Establish cybersecurity governance bodies focused on energy industry issues.
- Protect sensitive information to encourage private sector information sharing.
- Collaborate with utility regulators to enhance their cybersecurity oversight.
- Participate in cyber exercises.
- Assess resiliency capabilities and gaps.
- Encourage the growth of microgrids and energy storage.

COORDINATE PREPAREDNESS AND PLANNING EFFORTS. All states conduct energy preparedness and planning efforts through their state energy assurance plans, generally created under the leadership of state energy offices. These plans are often coordinated with the electricity sector to ensure smooth operations during emergencies. As the threat of physical and cyberattacks rise, states should begin to incorporate a resilience mindset and cyberdisruption planning into their energy assurance plans. States will want to define roles and responsibilities, establish communication guidelines and coordinate response efforts to ensure that they are prepared for a cyberincident. Consider the following state spotlights:

State spotlight: Oregon. 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. In this plan, responsibilities are clearly delineated; for instance, designating the Oregon PUC as the lead agency during electrical system disruptions.[1] Additional support agencies are enlisted as the risks and consequences increase. The Oregon PUC and the Office of Emergency Management are the primary agencies responsible for cybersecurity planning, preparedness, response and recovery from breaches.

State spotlight: Montana. Montana incorporated planning for cyberthreats into its latest energy assurance plan, whereby responsibility for responding to cyberthreats is led by the utilities, with oversight and support from state and federal agencies.[2] In addition, the Montana Department of Justice operates the Montana All Threat Intelligence Center to facilitate cyber communication and threat response organization.[3]

State spotlight: Oklahoma. Oklahoma's state energy assurance plan describes private sector cybersecurity plans, activities and resources. Cybersecurity responsibilities are delineated, with a discussion of response and communication strategies during and after a cyberevent.[4]

ESTABLISH CYBERSECURITY GOVERNANCE BODIES FOCUSED ON ENERGY INDUSTRY ISSUES. Cybersecurity governance bodies take many forms, but their overall mission is to identify cyberthreats facing the state and develop solutions to mitigate those threats. As of 2017, 22 state cybersecurity governance bodies were in existence.[5] Some of those bodies established committees specifically to study critical infrastructure or the energy industry. In some cases, governance bodies have been established exclusively to study and develop solutions for cybersecurity in the energy industry. These bodies can be critical to supporting the industry and addressing growing cyberthreats. Consider the following state spotlights:

State spotlight: Texas. Texas enacted a pair of bills to strengthen the state's electric grid security. Senate Bill (S.B.) 475 establishes the Texas Electric Grid Security Council to "facilitate the creation, aggregation, coordination, and dissemination of best security practices for the electric industry." The three-member council has the ability to create and disseminate grid security best practices, revise the state emergency plan to ensure coordinated restoration efforts and prepare for grid-related security threats.[6] S.B. 936 creates a cybersecurity monitor program through the PUC. The

ADDRESSING CYBER AND PHYSICAL THREATS

monitor manages a comprehensive cybersecurity outreach program, gathers and disseminates best practices for electricity cybersecurity, reviews utility voluntary cybersecurity self-assessments and reports to the PUC about electrical utility industry cybersecurity preparedness level. The bill also directs the PUC to allow the recovery of reasonable and necessary costs related to findings/activities of the cybersecurity monitor.[7]

State spotlight: Vermont. In 2017, Gov. 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.[8] 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 and with the private sector. The focus of this group is cybersecurity broadly, with members including state information technology and homeland security leads alongside other state officials and academic experts. Underscoring the criticality of cybersecurity in the electricity sector, Gov. Scott also appointed the chief executive officer of the **Vermont** Electric Power Company to serve as an advisor.[9]

PROTECT SENSITIVE INFORMATION, INCLUDING CLASSIFIED THREAT INFORMATION AND CRITICAL ENERGY INFRASTRUCTURE INFORMATION, TO ENCOURAGE PRIVATE SECTOR INFORMATION SHARING. The federal government enacted the Cybersecurity Information Sharing Act (CISA) in 2015 to make it easier for private companies to share cyberthreat information with the federal government. CISA also introduced protections to exempt that information from being disclosed in response to a Freedom of Information Act request. Many states have similar laws to protect cyberthreat information and critical energy infrastructure information from being subject to disclosure. The National Governors Association issued a paper detailing how state laws and court rules have been protecting critical energy infrastructure information against public disclosure.[10] These protections help encourage private companies to share critical information with states and the federal government. Consider the following state spotlights:

State spotlight: Idaho. **Idaho**'s cybersecurity exemption covers records held by any public agency that are "related to proposed or existing critical infrastructure" if disclosure "is reasonably likely to jeopardize the safety of persons, property or the public safety."[11] For purposes of this exemption, "critical infrastructure" means any system, "whether physical or virtual," and including electrical, computer or telecommunications systems, whose disruption "would have a debilitating impact" on economic security, public health or safety or any combination of those matters.[12]

State spotlight: Louisiana. **Louisiana** enacted a state version of the federal CISA law in 2019.[13] The Louisiana law also addressed a gray area involving legal counsel and disclosure. S.B. 46 states, "sharing a cyberthreat indicator or defensive measure information does not constitute a waiver of any applicable privilege or protection provided in the Louisiana Code of Evidence."[14]

COLLABORATE WITH UTILITY REGULATORS TO ENHANCE THEIR CYBERSECURITY OVERSIGHT. PUCs are key to improving energy cybersecurity through their oversight of parts of the electrical utility industry, their ability to authorize cost recovery for investments and their roles during restoration and response activities. States can support grid cybersecurity by directing or encouraging PUCs to examine the adoption and deployment of new technologies or processes by regulated utilities and to direct regulated entities to conduct cybersecurity assessments and audits to better understand their cybersecurity efforts. Consider the following state spotlights:

State Spotlight: Connecticut. In 2013, then-Gov. Dannel Malloy signed the Compressive Energy Strategy, which 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.[15] Following the review, PURA held technical meetings with utilities to review how they manage cyber risk. Through voluntary standards and guidelines, the industry adopted utility-wide cyber updates and procedures to improve expertise and help identify vulnerabilities.[16]

ADDRESSING CYBER AND PHYSICAL THREATS

State spotlight: New Jersey. In 2011, the New Jersey Board of Public Utilities (BPU) passed an order requiring regulated utilities to report all cyberincidents involving their industrial control systems.[17] In 2016, the BPU built on that order by issuing a new order requiring regulated utilities to safeguard their computer systems, to join and share information with the New Jersey Cybersecurity and Communications Integration Cell and to implement BPU's Cyber Security Program.[18]

PARTICIPATE IN CYBER EXERCISES. Exercises simulating cyberattacks can help government and utilities practice coordinated responses, identify gaps or misalignments in plans, strengthen communication channels and address areas for improvement.[19] They can be an efficient way to test security and response with limited resources.[20] 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 can be reported to state regulators.[21] 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.[22] Consider the following state spotlights:

State spotlight: New York. In 2014, New York put on the State Critical Infrastructure Cybersecurity Exercise. The exercise tested incident response capabilities through a mock cyberattack on critical infrastructure that affected energy delivery systems. There were 120 participants from 13 utilities; industry organizations; and federal, state, local and tribal governments.[23]

Assess resiliency capabilities and gaps. Governors play a critical role in helping enhance resiliency in the wake of increasing physical threats: to withstand disasters better, respond and recover more quickly and excel under new conditions. Given the interdependency of the energy sector, such efforts, even if specific to electricity delivery only, call for a cross-agency effort to assess current capabilities and gaps. The National Governors Association has created the State Resiliency Assessment and Planning Tool (SRAP Tool) as the first-ever tool for state policy makers that uses a self-assessment rating scale encompassing a series of 41 questions across five categories. The tool is currently being revised based on feedback from states and is due to be released in Spring 2020. Governors can explore the use of that that tool or similar assessments.[24]

ENCOURAGE THE GROWTH OF MICROGRIDS AND ENERGY STORAGE. Microgrids and energy storage can increase resiliency during and after a cyberattack or a weather-related incident by giving communities the ability to provide their own power if electrical service is disabled. Many states are pursuing energy storage targets and deploying microgrids to increase overall system resiliency. Various approaches exist for implementing these targets. California established an energy storage target through legislation. **Connecticut** and **Massachusetts** are encouraging the growth of microgrids through grant programs. Other states, including Connecticut, Massachusetts, New Jersey and **New York**, are changing regulatory statues and using public-private partnerships to encourage and finance "public purpose" microgrids. Consider the following state spotlights:

State spotlight: California. In 2010, California enacted the first energy storage mandate in the United States.[25] The legislation required the three largest investor-owned utilities to deploy 1,325 MW of energy storage capacity by 2020. The state extended that target in 2016, requiring the utilities to procure an additional 500 MW of storage, bringing the total to 1,825 MW of energy storage.

State spotlight: Massachusetts. In 2014, the Massachusetts Department of Public Utilities issued an order requiring public utilities to develop a 10-year grid modernization program. In response, the Massachusetts Clean Energy Center (MassCEC), a state economic development agency, began offering a Community Microgrids Program to "catalyze the development of community microgrids… to lower customer energy costs, reduce greenhouse gas emissions, and provide increased energy resilience."[26] In 2018, MassCEC awarded $1.4 million in funding for feasibility studies for 14 projects located across the state.[27]

ADDRESSING CYBER AND PHYSICAL THREATS

State spotlight: Puerto Rico. Following the devastation of Hurricane Maria, **Puerto Rico** has been considering increased deployment of microgrids to increase resiliency and improve electricity service. The Comisión de Energía de Puerto Rico (Puerto Rico Energy Bureau) passed a new set of rules in 2018 to "promote and encourage the growth of microgrid systems" in Puerto Rico.[28] The new rules establish the legal and regulatory frameworks for microgrid operation on the island. The rules clarify three important directives: 1) Define classes of microgrids, 2) specify the types of generation that can be deployed and 3) clarify the role of utilities and municipalities.

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

[2] Montana Department of Environmental Quality. (2016, January). *Montana energy assurance plan.* Retrieved from https://deq.mt.gov/Portals/112/Energy/EnergizeMT/Energy%20Assurance/MTENERGYASSURANCEPLAN-final.pdf?ver=2017-02-07-112024-230&timestamp=1486491659359

[3] Montana Department of Environmental Quality. (2016, January). *Montana energy assurance plan.* Retrieved from https://deq.mt.gov/Portals/112/Energy/EnergizeMT/Energy%20Assurance/MTENERGYASSURANCEPLAN-final.pdf?ver=2017-02-07-112024-230&timestamp=1486491659359

[4] Oklahoma State Energy Office. (2013, April). *Oklahoma energy assurance plan.* Retrieved from http://www.occeweb.com/pu/PUDVideo/2013%20EAP%20Plan%20FINAL.pdf

[5] National Governors Association. (2017). *Meet the threat: States confront the cyber challenge: 2016–17 NGA Chair's initiative. Memo on state cybersecurity governance bodies.* Retrieved from https://www.nga.org/wp-content/uploads/2019/09/Task-Force-Memo-Final.pdf

[6] Texas, S.B. 475, 86th Legis. (2019–2020).

[7] Texas, S.B. 936, 86th Legis. (2019–2020).

[8] Exec. Order No. 18-17, Vermont Legis., 2nd Sess. (2017, October 10). Retrieved from https://governor.vermont.gov/sites/scott/files/documents/EO%2018-17%20-%20Governor%27s%20Cybersecurity%20Advisory%20Team.pdf

[9] State of Vermont, Office of Governor Phil Scott. (2017, November 20). *Governor Phil Scott announces appointments to Cybersecurity Advisory Team* [Press release]. Retrieved from https://governor.vermont.gov/press-release/governor-phil-scott-announces-appointments-cybersecurity-advisory-team

[10] Rackley, J. (2019, June). *State protection of critical energy infrastructure information (CEII)*. Retrieved from www.nga.org/wp-content/uploads/2019/05/CEII-Paper-June-2019-Revised.pdf

[11] Records Exempt from Disclosure, Idaho Code § 74-105(4)(b) (2017). Retrieved from https://legislature.idaho.gov/statutesrules/idstat/title74/t74ch1/sect74-105

[12] Records Exempt from Disclosure, Idaho Code § 74-105(4)(b) (2017). Retrieved from https://legislature.idaho.gov/statutesrules/idstat/title74/t74ch1/sect74-105

[13] Louisiana Cybersecurity Information Sharing Act, S.B. 46 (2019).

[14] Louisiana Cybersecurity Information Sharing Act, S.B. 46 (2019).

[15] State of Connecticut Public Utilities Regulatory Authority. (2014, April 14). *Cybersecurity and Connecticut's public utilities.* Retrieved from https://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf

[16] State of Connecticut Public Utilities Regulatory Authority. (2016, April 6). *Connecticut public utilities cybersecurity action plan.* Retrieved from https://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf

[17] State of New Jersey Board of Public Utltiies. (2011, October 23). Reliability & security. Docket No. EO11 090575. Retrieved from https://www.state.nj.us/bpu/pdf/boardorders/2011/20111004/10-13-11-6B.pdf

[18] State of New Jersey Board of Public Utilities. (2016, March 18). Reliability & security. Docket No. A016030196. Retrieved from https://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf

[19] North American Electric Reliability Corporation. (n.d.). GridEx V frequently asked questions. Retrieved from https://www.nerc.com/pa/CI/CIPOutreach/Documents/CIP%20Outreach%20Document%20Library/TLP%20WHITE%20E-ISAC%20GridEx%20V%20FAQ.PDF

[20] Indiana Executive Council on Cybersecurity. (2018, September). *Cyber Pre- Thru Post-Incident Working Group strategic plan.* Retrieved from https://www.in.gov/cybersecurity/files/Appendix%20D.11%20Pre-Post%20Incident%20Working%20Group%20Final.pdf

[21] Idaho National Laboratory, Mission Support Center. (2016, August). *Cyber threat and vulnerability analysis of the U.S. electric sector.* Retrieved from https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf; and The Florida Public Service Commission, Office of Auditing and Performance Analysis. (2018, April). *Review of cyber and physical security protection of utility substation and control centers.* Retrieved from http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf

[22] North American Electric Reliability Corporation. (2018, March). *Grid Security Exercise GridEx IV lessons learned* (Atlanta, GA: North American Electric Reliability Corporation.

[23] New York Senate Standing Committee on Veterans, Homeland Security and Military Affairs. (2015). *To address New York State's cyber security infrastructure.*

[24] For more information see https://www.nga.org/wp-content/uploads/2018/12/Idaho-Resiliency-Retreat-Master-Deck.pdf OR https://www.nga.org/wp-content/uploads/2018/12/Master-Deck-Maryland-Resilience-Retreat-NGA-Framework-Powerpoint.pdf OR https://www.nga.org/center/meetings/oregon-retreat-on-prioritizing-and-valuing-local-energy-resilience/

[25] Maloney, P. (2018, June 12). California looks to next steps as utilities near energy storage targets. *Utility Dive.* Retrieved from www.utilitydive.com/news/california-looks-to-next-steps-as-utilities-near-energy-storage-targets/525441

[26] Massachusetts Clean Energy Center. (n.d.). Community Microgrids Program. Retrieved from www.masscec.com/community-microgrids-program

[27] Massachusetts Clean Energy Center. (n.d.). Community Microgrids Program. Retrieved from www.masscec.com/community-microgrids-program

[28] Government of Puerto Rico, Puerto Rico Energy Commission. (2018, May). Adoption of proposed regulation on microgrid development. Retrieved from http://energia.pr.gov/wp-content/uploads/2018/05/Resolution-Adoptation-of-Microgrid-Regulation-Final.pdf